Algebra
Lecture Notes for MTH 818/819
Fall 12/Spring 13

Ulrich Meierfrankenfeld

April 26, 2013

Preface

These are the lecture notes for the classes MTH 818 in Fall 2012 and MTH 819 in Spring 2013. The notes were originally based on Hungerford's Algebra [Hun], but by now the content and proofs have diverged from Hungerford.

The lecture notes will be updated frequently.

Contents

Chapter 1

Group Theory

1.1 Latin Squares

Definition 1.1.1. *Let I, J be sets $\mathcal{C}$ a class. An $I \times J$ matrix in $\mathcal{C}$ is a function $M : I \times J \to \mathcal{C}$.. We will write M_{ij} for the image of (i, j) under M. M_{ij} is called the ij-coefficient of M. We denote M by $[M_{ij}]_{\substack{i\in I\\ j\in J}}$.*

Definition 1.1.2. *Let G be a set and ϕ a function such that $G \times G$ is contained in the domain of G.*

(a) If $a, b \in G$ we write ab or $a\phi b$ for $\phi(a, b)$. ϕ is called a binary operation *on G (or closed on G, if $ab \in G$ for all $a, b \in G$. In this case the pair (G, ϕ) is called a* magma.

(b) $1 \in G$ *is called an* identity element *if $1a = a1 = a$ for all $a \in G$.*

(c) We say that (G, ϕ) is a Latin square *if for all a, b in G there exist unique elements x, y in G so that*

$$ax = b \text{ and } ya = b$$

(d) The multiplication table *of (G, ϕ) is the matrix $G \times G$-matrix $[ab]_{\substack{a\in G\\ b\in G}}$.*

(e) The order *of (G, ϕ) is the cardinality $|G|$ of G.*

We remark that (G, ϕ) is a latin square if and only if each $a \in G$ appears exactly once in each row and in each column of the multiplication table.

If there is no confusion about the binary operation in mind, we will just write G for (G, ϕ) and call G a magma.

If (G, ϕ) is a magma, we can restrict ϕ to a function

$$\tilde{\phi} : G \times G \to G, (a, b) \to ab$$

Then $(G, \tilde{\phi})$ is also a magma

Definition 1.1.3. *Let G and H be magma and $\alpha : G \to H$ a function.*

(a) *α is called a (magma)* homomorphism *if $\alpha(ab) = \alpha(a)\alpha(b)$, for all $a, b \in G$.*

(b) *α is called an* isomorphism *if α is a homomorphism and there exists a homomorphism $\beta : H \to G$ with $\alpha \circ \beta = \mathrm{id}_H$ and $\beta \circ \alpha = \mathrm{id}_G$.*

(c) *α is an* automorphism *if $G = H$ and α is an isomorphism.*

(d) *If G and H are monoid, α is called a monoid-homomorphism if α is magma-homomorphism and $\alpha(1_G) = 1_H$.*

(e) *If G and H are groups, , α is called a group -homomorphism if α is magma-homomorphism.*

Definition 1.1.4. *Let G and H be magmas.*

(a) *The* opposite *magma G^{op} is defined by $G^{\mathrm{op}} = G$ as a set and*

$$g \cdot_{\mathrm{op}} h = hg.$$

(b) *An magma* anti homomorphism*$\alpha : G \to H$ is a magma homomorphism $\alpha : G \to H^{\mathrm{op}}$. So $\alpha(ab) = \alpha(b)\alpha(a)$.*

Lemma 1.1.5. *(a) Let G be a magma. Then G has at most one identity.*

(b) *Let $\alpha : G \to H$ be a magma homomorphism. Then α is an isomorphism if and only if α is a bijection.*

Proof. (a) Let 1 and 1^* be identities. Then

$$1 = 11^* = 1^*.$$

(b) Clearly any isomorphism is a bijection. Conversely, assume α is a bijection and let β be its inverse map. We need to show that β is a homomorphism. For this let $a, b \in H$. Then as α is a homomorphism

$$\alpha(\beta(a)\beta(b)) = \alpha(\beta(a))\alpha(\beta(b)) = ab = \alpha(\beta(ab)).$$

Since α is 1-1 (or by applying β) we get

$$\beta(a)\beta(b) = \beta(ab).$$

So β is an homomorphism. □

1.1.6 (Latin Squares of small order)**.** Below we list (up to isomorphism) all Latin square of order at most 5 which have an identity element 1. It is fairly straightforward to obtain this list, although the case $|G| = 5$ is rather tedious). We leave the details to the reader, but indicate a case division which leads to the various Latin squares.

Order 1,2 and 3:

	1
1	1

	1	a
1	1	a
a	a	1

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Order 4: Here we get two non-isomorphic Latin squares. One for the case that $a^2 \neq 1$ for some $a \in G$ and one for the case that $a^2 = 1$ for all $a \in G$.

(1)

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

(2)

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Order 5: This time we get lots of cases:

Case 1: There exists $1 \neq a \neq b$ with $a^2 = 1 = b^2$.
Case 2 There exists $1 \neq a$ with $a^2 \neq 1$, $aa^2 = 1$ and $(a^2a)^2 = 1$.
Case 3 There exists $1 \neq a$ with $a^2 \neq 1$, $aa^2 = 1$ and $(a^2a)^2 \neq 1$
Case 4 There exists $1 \neq a$ with $a^2 \neq 1$, $a^2a = 1$ and $(aa^2)^2 = 1$.

This Latin square is anti-isomorphic but not isomorphic to the one in case 2. Anti-isomorphic means that is there exists bijection α with $\alpha(ab) = \alpha(b)\alpha(a))$.

Case 5 There exists $1 \neq a$ with $a^2 \neq 1$, $a^2a = 1$ and $(aa^2)^2 \neq 1$.

This Latin square is isomorphic and anti-isomorphic to the one in case 3.

Case 6 There exists $1 \neq a$ with $a^2 \neq 1$, $a^2a = aa^2 \neq 1$
Case 7 There exists $1 \neq a$ with $a^2 \neq 1 = (a^2)^2$.
Case 8 There exists $1 \neq a$ with $(a^2)^2 \neq 1$ and $1 \neq a^2a \neq aa^2 \neq 1$.

In this case put $c = aa^2$. Then $c^2 \neq 1$ and either $cc^2 = 1$ or $c^2c = 1$. Moreover $(c^2c)^2 \neq 1$ respectively $(cc^2)^2 \neq 1$ and the latin square is isomorphic to the one in Case 3.

(1)

	1	a	b	c	d
1	1	a	b	c	d
a	a	1	c	d	b
b	b	d	1	a	c
c	c	b	d	1	a
d	d	c	a	b	e

(2)

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	1	d	c
b	b	c	d	a	1
c	c	d	a	1	b
d	d	1	c	b	a

(3)

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	1	d	c
b	b	c	d	1	a
c	c	d	a	b	1
d	d	1	c	a	b

(4)

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	1
b	b	1	d	a	c
c	c	d	a	1	b
d	d	c	1	b	a

(5)

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	1
b	b	1	d	a	c
c	c	d	1	b	a
d	d	c	a	1	b

(6)

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	1
b	b	c	d	1	a
c	c	d	1	a	b
d	d	1	a	b	c

(7)

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	1
b	b	d	1	a	c
c	c	1	d	b	a
d	d	c	a	1	b

(8)

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	c	d	1
b	b	d	a	1	c
c	c	1	d	x	y
d	d	c	1	y	x

$\{x,y\} = \{a,b\}$

1.2 Semigroups, monoids and groups

Definition 1.2.1. *Let G be a magma.*

(a) The binary operation on G is called associative *if*

$$(ab)c = a(bc)$$

for all $a,b,c \in G$. If this is the case we call G a semigroup.

(b) G is a monoid *if it is a semigroup and has an identity.*

(c) Suppose G is a monoid and let $a,b \in G$ with $ab = 1$. Then a is called a left inverse of b and b is called a right inverse of a.

(d) Suppose that G is a monoid. Then $a \in G$ is called invertible *if there exists $a^{-1} \in G$ with*

$$aa^{-1} = 1 = a^{-1}a.$$

Such an a^{-1} is called an inverse *of a.*

(e) A group *is a monoid in which every element is invertible.*

(f) G is called abelian *(or* commutative*) if*

$$ab = ba$$

for all $a,b \in G$.

Example 1.2.2. Let $\mathbb{Z}^+$ denote the positive integers and $\mathbb{N}$ the non-negative integers. Then $(\mathbb{Z}^+,+)$ is a semigroup, $(\mathbb{N},+)$ is a monoid and $(\mathbb{Z},+)$ is a group. $(\mathbb{Z},\cdot)$ and $(\mathbb{R},\cdot)$ are monoids. Let $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Then $(\mathbb{R}^*,\cdot)$ is a group. The integers modulo n under addition is another example. We denote this group by $(\mathbb{Z}/n\mathbb{Z},+)$. All the examples so far have been abelian.

Note that in a group $a^{-1}b$ is the unique solution of $ax = b$ and ba^{-1} is the unique solution of $ya = b$. So every group is a Latin square with identity. But the converse is not true. Indeed of the

Latin squares listed in section 1.1 all the once of order less than five are groups. But of Latin squares of order five only the one labeled (6) is a group.

Let $\mathbb{K}$ be a field and V a vector space over $\mathbb{K}$. Let $\mathrm{End}_{\mathbb{K}}(V)$ the set of all $\mathbb{K}$-linear maps from V to V. Then $\mathrm{End}_{\mathbb{K}}(V)$ is a monoid under compositions. Let $\mathrm{GL}_{\mathbb{K}}(V)$ be the set of $\mathbb{K}$-linear bijection from V to V. Then $\mathrm{GL}_{\mathbb{K}}(V)$ is a group under composition, called the general linear group of V. It is easy to verify that $GL_{\mathbb{K}}(V)$ is not abelian unless V has dimension 0 or 1.

Let I be a set. Then the set $\mathrm{Sym}(I)$ of all bijection from I to I is a group under composition, called the symmetric group on I. If $I = \{1, \dots, n\}$ we also write $\mathrm{Sym}(n)$ for $\mathrm{Sym}(I)$. $\mathrm{Sym}(n)$ is called the symmetric group of degree n. $\mathrm{Sym}(I)$ is not abelian as long as I has at least three elements.

Above we obtained various examples of groups by starting with a monoid and then considered only the invertible elements. This works in general:

Lemma 1.2.3. *Let G be a monoid.*

(a) Suppose that $a, b, c \in G$, a is a left inverse of b and c is right inverse of b. Then $a = c$ and a is an inverse.

(b) An element in G has an inverse if and only if it has a left inverse and a right inverse.

(c) Each element in G has at most one inverse.

(d) If x and y are invertible, then x^{-1} and xy are invertible. Namely x is an inverse of x^{-1} and $y^{-1}x^{-1}$ is an inverse of xy.

(e) Let $\mathrm{U}(G)$ be the set of invertible elements in G, then $\mathrm{U}(G)$ is a group.

Proof. (a)

$$a = a1 = a(bc) = (ab)c = 1c = c$$

(b) and (c) follow immediately from (a).

(d) Clearly x is an inverse of x^{-1}. Also

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}(xy)) = y^{-1}((x^{-1}x)y) = y^{-1}(1y) = y^{-1}y = e$$

Similarly $(xy)(y^{-1}x^{-1}) = 1$ and so $y^{-1}x^{-1}$ is indeed an inverse for xy.

(e) By (d) $\mathrm{U}(G)$ is closed under multiplication. Since the multiplication is associative on G, its also associative on $\mathrm{U}(G)$. Since $1 \in \mathrm{U}(G)$, $\mathrm{U}(G)$ is a monoid. By (d) $x^{-1} \in \mathrm{U}(G)$ for all $x \in \mathrm{U}(G)$ ad so x has an inverse in $\mathrm{U}(G)$. Hence $\mathrm{U}(G)$ is a group. □

Corollary 1.2.4. *Let G be a group. Then G is isomorphic to its opposite group G^{op}, in fact the map $x \to x^{-1}$ is an anti-automorphism of G and an isomorphism $G \to G^{\mathrm{op}}$.*

Proof. This follows from 1.2.3(d). □

Definition 1.2.5. *Let G be a magma, n a positive integer and $a_1, \dots, a_n \in G$. Let $z \in G$. Inductively, z is called a product of $(a_1, \dots, a_n)$ if either* *(a)* $n = 1$ *and* $z = a_1$*; or*

(b) $n > 1$ *and there exist an integer* k *with* $1 \le k < n$*, a product* x *of* $(a_1 \dots, a_k)$ *and a product* y *of* $(a_{k+1} \dots, a_n)$ *such that* $z = xy$*.*

Also z *is called the standard product of* $(a_1, \dots, a_n)$ *if either*

(a) $n = 1$ *and* $z = a_1$*; or*

(b) $n > 1$ *and* $z = sa_n$ *where* s *is the standard product of* $(a_1, \dots, a_{n-1})$*.*

If G *has an identity* e*, then* e *is called the product and the standard product of the empty tuple* $()$*.*

Example 1.2.6. *Products of tuple of length less or equal to four.*

Let G be magma and $a, b, c, d \in G$.
The only product of (a) is a.
The only product of (a, b) is ab,
The products of (a, b, c) are $a(bc)$ and $(ab)c$.
The products of (a, b, c, d) are $a\big(b(cd)\big)$, $a\big((bc)d\big)$, $(ab)(cd)$, $\big(a(bc)\big)d$ and $\big((ab)c\big)d$.

Theorem 1.2.7 (General Associativity Law)**.** *Let* G *be a semigroup and* $a_1, \dots, a_n \in G$*. Then any product of* $(a_1, \dots, a_n)$ *is equal to the standard product.*

Proof. The proof is by complete induction on n. For $n = 1$ the only product of (a_1) is a_1, which is also the standard product.

So suppose $n \ge 2$ and that any product of a tuple of length less than n is equal to its standard product. Let z be any product of $(a_1, \dots, a_n)$. Then by definition of 'product' there exist an integer $1 \le m < n$, a product x of $(a_1, \dots, a_m)$ and a product y of $(a_{m+1}, \dots, a_n)$ such that $z = xy$.

Suppose first that $m = n - 1$. By induction x is the standard product of $(a_1, \dots, a_{n-1})$. Also $z = xa_n$ and so by definition z is the standard product of $(a_1, \dots, a_n)$.

Suppose next that $m < n - 1$. Again by induction y is the standard product of $(a_{m+1}, \dots, a_n)$ and so $y = sa_n$, where s is the standard product of $(a_{m+1} \dots, a_{n-1})$. Hence

$$z = xy = x(sa_n) = (xs)a_n$$

As xs is a product of $(a_1, \dots a_{n-1})$, we are done by the $m = n - 1$ case. □

One of the most common ways to define a group is as the group of automorphism of some object. For example above we used sets and vector spaces to define the symmetric groups and the general linear group.

If the object is a magma G we get a group which we denote by $\mathrm{Aut}(G)$. So $\mathrm{Aut}(G)$ is the set of all automorphisms of the magma G. The binary operation on $\mathrm{Aut}(G)$ is the composition.

We will determine the automorphism for the Latin squares in 1.1. As the identity element is unique it is fixed by any automorphism. It follows that the Latin square of order 1 or 2, have no non-trivial automorphism (any structure as the trivial automorphism which sends every element to itself).

The Latin square of order three has one non-trivial automorphism. It sends

$$e \to e \quad a \to b \quad b \to a.$$

Consider the first Latin square of order 4. It has two elements with $x^{\neq}2e$, namely a and c. So again we have a unique non- trivial automorphism:

$$e \to e \quad a \to c \quad b \to b \quad c \to a.$$

Consider the second Latin square of order 4. Here is an easy way to describe the multiplication: $ex = x, xx = e$ and $xy = z$ if $\{x, y, z\} = \{a, b, c\}$. It follows that any permutation of $\{e, a, b, c\}$ which fixes e is an automorphism. Hence the group of automorphism is isomorphic to $\mathrm{Sym}(3)$,

Consider the Latin square of order 5 labeled (1). The multiplication table was uniquely determine by any pair $x \neq y$ of non-trivial elements with $x^2 = y^2 = e$. But $x^2 = e$ for all x. So every $e \neq x \neq y \neq e$ there exists a unique automorphism with

$$a \to x \quad b \to y$$

Thus the group of automorphisms has order 12. The reader might convince herself that also the set of bijection which are automorphisms or anti-automorphisms form a group. In this case it has order 24. That is any bijection fixing e is an automorphism or anti-automorphism.

Consider the Latins square of order five labeled (2). This multiplication table is uniquely determine by any element with $x^2 \neq e$, $xx^2 = e$ and $(x^2x)^2 = e$. a, b and d have this property and we get two non-trivial automorphism:

$$e \to e, a \to b \quad b \to d, \quad c \to c \quad d \to a \text{ and } e \to e, a \to d \quad b \to a, \quad c \to c \quad d \to b$$

That is any permutation fixing e and c and cyclicly permuting a, b, d is an automorphism. Consider the Latins square of order five labeled (3). This time only a itself has the defining property. It follows that no non-trivial automorphism exists. But it has an anti-isomorphism fixing a, b and d and interchanging a and c.

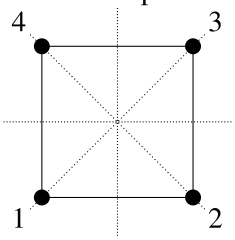
The Latin square (4) and (5) had been (anti-)-isomorphic to (2) and (3). So consider (6). All non-trivial elements have the defining property. So there are 4 automorphisms. They fix e and cyclicly permute (a, b, c, d).

Finally consider the Latin square (7). Here a, c, d have the defining property. So there are 3 automorphism. They fix e and b and cyclicly permuted (a, c, d). Here all bijections fixing a and b are automorphism or anti-automorphism.

It might be interesting to look back and consider the isomorphism types of the groups we found as automorphism of Latin squares. $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3, 4$, $\mathrm{Sym}(3)$ and a group of order 12. We will later see that $\mathrm{Sym}(4)$ has a unique subgroup of order 12 called $\mathrm{Alt}(4)$. So the group of order 12 must be isomorphic to $\mathrm{Alt}(4)$.

Another class of objects one can use are graphs. We define a graph to be a tuple $(\Gamma, -)$, where Γ is a set and " $-$ " is an anti-reflexive, symmetric relation on Γ. The elements are called vertices, If a and b are vertices with $a - b$ we say that a and b are adjacent. An edge is a pair of adjacent vertices. An automorphism of the graph Γ is an bijection $\alpha \in \mathrm{Sym}(\Gamma)$ such that $a - b$ if and only if $\alpha(a) - \alpha(b)$. In other words a bijection which maps edges to edges. $\mathrm{Aut}(\Gamma)$ is the set of all automorphisms of Γ under composition.

As an example let Γ_4 be a square:



The square has the following automorphisms: rotations by $0, 90, 180$ and 270 degrees, and reflections on each of the four dotted lines. So $\mathrm{Aut}(\Gamma_4)$ has order 8.

To describe $\mathrm{Aut}(\Gamma_4)$ as a subset of $\mathrm{Sym}(4)$ we introduce the cycle notation for elements of $\mathrm{Sym}(I)$ for a finite set I. We say that $\pi \in \mathrm{Sym}(I)$ is a cycle of length if the exists $a_1 \dots a_m \in I$ such that

$$\pi(a_1) = a_2, \pi(a_2) = a_3, \dots, \pi(a_{m-1}) = a_m, \pi(a_m) = a_1$$

and $\pi(j) = j$ for all other $j \in I$.

Such a cycle will be denoted by

$$(a_1 a_2 a_3 \dots a_m)$$

The set $\{a_1, \dots a_m\}$ is called the support of the cycle. Two cycles are called disjoint if their supports are disjoint.

It is clear that every permutations can be uniquely written as a product of disjoint cycle.

$$\pi = (a_1^1 a_2^1 \dots a_{m_1}^1)\,(a_1^2 a_2^2 \dots a_{m_2}^2)\,\dots\,(a_1^k a_2^k \dots a_{m_k}^k)$$

One should notice here that disjoint cycles commute and so the order of multiplication is irrelevant. Often we will not list the cycles of length 1.

So $(135)(26)$ is the permutation which sends 1 to 3, 3 to 5,5 to 1, 2 to 6, 6 to 2 and fixes 4 and any number larger than 6.

With this notation we can explicitly list the elements of $\mathrm{Aut}(\Gamma_4)$:

The four rotations: $e, (1234), (13)(24), (1432)$

And the four reflections: $(14)(23), (13), (12)(34), (24)$.

1.3 The projective plane of order 2

In this section we will look at the automorphism group of the projective plane of order two.

Definition 1.3.1. *Let $\mathcal{E} = (\mathcal{P}, \mathcal{L}, \mathcal{R})$ be a triple such that $\mathcal{P}$ and $\mathcal{L}$ are non-empty disjoint sets and $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{L}$. The elements of $\mathcal{P}$ are called points, the elements of $\mathcal{L}$ are called lines and we say a* *point P and a line l are incident if $(P,l) \in \mathcal{R}$. $\mathcal{E}$ is called a projective plane if it has the following three properties*

(PP1) *Any point is incident with at least* 3 *lines and any line is incident with at least three points.*

(PP2) *Any two distinct points are incident with a unique common line.*

(PP3) *Any two distinct lines are incident with a unique common point.*

If P and Q are distinct points in a projective plane, then PQ denotes the unique line incident with P and Q. And if l and k are distinct lines lk denotes the unique point incident with l and k.

Lemma 1.3.2. *Let $\mathcal{E} = (\mathcal{P}, \mathcal{L}, \mathcal{R})$ be a projective plane. Define*

$$\mathcal{R}^* = \{(l,P) \mid (P,l) \in \mathcal{R}\} \text{ and } \mathcal{E}^* = (\mathcal{L}, \mathcal{P}, \mathcal{R}^*).$$

Then $\mathcal{E}^*$ is a projective plane, called the dual plane of $\mathcal{E}$.

Proof. (PP0) for $\mathcal{E}$ implies (PP0) for $\mathcal{E}^*$, (PP1) for $\mathcal{E}$ implies (PP2) for $\mathcal{E}^*$ and (PP2) for $\mathcal{E}$ implies (PP1) for $\mathcal{E}^*$. □

Lemma 1.3.3. *Let $\mathcal{E}$ be a projective plane.*

(a) For each point P there exists a line l not incident with P,

(b) For each line l there exists a point P not incident with l.

(c) There exists three non-collinear points, that is three points which are not incident with a common line.

(d) Let P and Q be points. Then there exists a line l which is neither incident with P nor with Q.

(e) There exists a cardinality q such that each point is incident with exactly $q+1$ lines and each line is incident with exactly $q+1$ points. q is called the order of $\mathcal{E}$.

Proof. (a) By (PP0) there exists a line r incident with P. By (PP0) there exist a point Q incident with r and distinct from P. By (PP0) there exists a line l incident with Q and distinct from r. Suppose that P is incident with l. Then P and Q are both incident with l and with r. But then (PP1) shows that $l = r$, a contradiction. So l is not incident with P.

(b) Follows from (a) applied to the dual plane of $\mathcal{E}$.

(c) Since $\mathcal{L}$ is not empty, there exists a line l. By (PP0) there exists distinct points P and Q incident with l. By (b) there exists a point R not incident with l. Suppose that k is a line incident with P, Q and R. Then both Q and R are incident with r and with l. Hence $r = l$ and P is incident with l, a contradiction. Thus P, Q and R are non-collinear.

(d) If $P = Q$, this is (a). So suppose $P \neq Q$ and let $k = PQ$. By (b) there exists a point R not incident with k. By (PP0), R is incident with at least three lines and so the exists a line l incident with R and distinct from PR and QR. Since R is incident with l we conclude that neither P nor Q is incident with l,

(e) For a point P let $\Delta(P)$ be the set of lines incident with P. For a line l $\Delta(l)$ be the set of points incident with l. We will first show that

1°. *Let P be a point and l a line not incident with P. Then $|\Delta(P)|| = |\Delta(l)|$.*

Let $Q \in \Delta(l)$. Since P is not incident with l, $P \neq Q$ and so PQ is a line incident with P. Hence we obtain a function

$$\alpha : \Delta(l) \to \Delta(P), Q \to QP$$

Applying this result to the dual plane we get a function

$$\beta : \Delta(P) \to \Delta(l), k \to kl$$

Note that Q is a point incident with QP and l and so $Q = (QP)l$. Thus $\beta(\alpha(Q)) = Q$ and $\beta \circ \alpha = \mathrm{id}_{\Delta(l)}$. Thus result applied to the dual plane gives $\alpha \circ \beta = \mathrm{id}_{\Delta(P)}$ and so α is a bijection with inverse β. Thus (1°) holds.

2°. *Let P and Q be points. Then $|\Delta(P)| = |\Delta(Q)|$.*

By (d) there exist a line l neither incident with P nor with Q. Thus using (1°) twice $|\Delta(P)| = |\Delta(l)| = |\Delta(Q)|$.

Now let P be a point and put $c = |\Delta(P)|$. If Q is any point, then (2°) shows $\Delta(Q)| = c$. If l is any line, we can choose a point R not incident with l and so by (1°), $|\Delta(l) = |\Delta(R)| = c$. Thus (e) holds with $q = c - 1$. □

Lemma 1.3.4. *Let $\mathcal{E}$ be a projective plane of order q. Then $\mathcal{E}$ has exactly $q^2 + q + 1$ points and $q^2 + q + 1$ lines.*

Proof. Let P be a point. Any other point lies on exactly one of the $q + 1$ lines incident with P. Each of whose $q + 1$ lines has q points distinct from P and so the number points is $1 + (q + 1) \cdot q = q^2 + q + 1$ points. Note that also the dual of $\mathcal{E}$ is a projective plane of order q. So the dual has $q^2 + q + 1$ points, i.e $\mathcal{E}$ has $q^2 + q + 1$ lines. □

1.3.5 (Projective planes of order 2)**.** Let $\mathcal{E} = (\mathcal{P}, \mathcal{L}, \mathcal{R})$ be a projective plane of order plane. Let A, B, C be any three points which are not collinear. We will show that the whole projective plane can be uniquely described in terms of the tuple (A, B, C). Let P and Q be distinct points. Then PQ is incident with exactly three points and so there exits a unique point incident with PQ distinct from P and Q. We denote this unique point by $P + Q$.

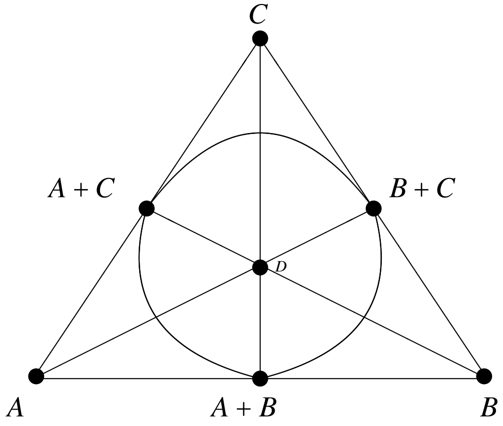
Since A, B and C are non-collinear, AB, BC and AC are three distinct lines. Since two distinct lines have exactly on point in common

$$A, B, C, A + B, A + C, B + C \text{ are six distinct points.}$$

Moreover, these are exactly the points which are incident to of the lines AB, BC and AC. Since $\mathcal{E}$ has seven points there exists exactly one more point D and D is not incident with any of the lines AB, BC and AC. Thus AD is distinct from AB, AC and BC. So none of B and C is incident with AD. Also neither A nor D is incident with BC. So $B+C$ is the only point on BC which can be incident with AD, and $A+D$ is the only point on AD which can be incident with BC. So $A+D = B+C$ and the points incident with AD are A, D and $B+C$. By symmetry the points incident with BD are B, D and $A+C$ and with CD are C, D and $C+D$. In particular,

$$AB, BC, AC, AD, BD, CD \text{ are six distinct lines.}$$

So there exists one more line d. Note that each of A, B, C and D is incident with three of the six lines distinct from d and so cannot be incident with d. Thus the three points incident with d must be $A+B, A+C$ and $B+C$. So we determined all points, all lines and their incidence:



Definition 1.3.6. *Let $\mathcal{E} = (\mathcal{P}, \mathcal{L}, \mathcal{R})$ be a projective plane.*

(a) An automorphism of $\mathcal{E}$ is a bijection $\alpha : \mathcal{P} \cup \mathcal{L} \to \mathcal{P} \cup \mathcal{L}$ such that

- *(i) If P is a point, then $\alpha(P)$ is point.*
- *(ii) If l is a line, then $\alpha(l)$ is a line.*
- *(iii) Let P be a point and l a line. Then P is incident to l if and only if $\alpha(P)$ is incident to $\alpha(l)$.*

(b) $\mathrm{Aut}(\mathcal{E})$ *is the set of automorphisms of $\mathcal{E}$ together with the binary operation defined by composition.*

Note that an automorphism α of $\mathcal{E}$ is uniquely determined by its effect on the points. Namely, if $l = PQ$ is a line, then $\alpha(l)$ is incident with $\alpha(P)$ and $\alpha(Q)$. So $\alpha(l) = \alpha(P)\alpha(Q)$.

If $\alpha, \beta \in \mathrm{Aut}(\mathcal{E})$, then it is easy to see that also $\alpha \circ \beta$ and α^{-1} are also automorphism of $\mathcal{E}$. Moreover, $\mathrm{id}_{\mathcal{P}\cup\mathcal{L}} \in \mathrm{Aut}(\mathcal{E})$ and composition of function is associative. Hence $(\mathrm{Aut}(\mathcal{E}), \circ)$ is a group.

Lemma 1.3.7. *Let $\mathcal{E}$ be a projective plane of order two and (A,B,C) and $(\tilde{A},\tilde{B},\tilde{C})$ be triples of non-collinear points. Then there exists a unique automorphism α of $\mathcal{E}$ with*

$$\alpha(A)=\tilde{A},\ \alpha(B)=\tilde{B} \text{ and } \alpha(C)=\tilde{C}$$

Proof. It is readily verified that the unique automorphism $\alpha:\mathcal{P}\cup\mathcal{L}\to\mathcal{P}\cap\mathcal{L}$ is given by

$$\begin{array}{ccccc}
A\to\tilde{A} & B\to\tilde{B} & C\to\tilde{C} & A+B\to\tilde{A}+\tilde{B} & B+C\to\tilde{B}+\tilde{C} \\
A+C\to\tilde{A}+\tilde{C} & D\to\tilde{D} & & AB\to\tilde{A}\tilde{B} & BC\to\tilde{B}\tilde{C} \\
AC\to\tilde{A}\tilde{C} & AD\to\tilde{A}\tilde{D} & BD\to\tilde{B}\tilde{D} & CD\to\tilde{C}\tilde{D} & d\to\tilde{d}
\end{array}\ .$$

Here D is the point not incident with any of lines AB, AC, BC. d is the line not incident with any of the points A, B and C. $\tilde{D}$ and $\tilde{d}$ are defined similarly (replacing each symbol X by $\tilde{X}$.) □

Corollary 1.3.8. *Let $\mathcal{E}$ be a projective plane of order two. Then* $|\mathrm{Aut}(\mathcal{E})|=168$.

Proof. Fix a triple (A,B,C) of non-collinear points. 1.3.7 show that there exists a bijection between $|\mathrm{Aut}(\mathcal{E})$ and the set of triples $(\tilde{A},\tilde{B},\tilde{C})$ of non-collinear points.

Now $\tilde{A}$ can be any one of the seven points, $\tilde{B}$ is any of the six points different from $\tilde{A}$, and $\tilde{C}$ is any of the four points not incident to $\tilde{A}\tilde{B}$. So there are $7\cdot 6\cdot 4=168$ triples of non-collinear points. Hence

$$|\mathrm{Aut}(\mathcal{E})|=7\cdot 6\cdot 4=168.$$

□

1.3.9 (The group associated to the projective plane of order 2)**.** Let $\mathcal{E}=(\mathcal{P},\mathcal{L},\mathcal{R})$ be a projective plane of order 2. We will construct a group of order 8 associated to $\mathcal{E}$. Let $G=\{0\}\cup\mathcal{P}$, where 0 is an arbitrary element not in $\mathcal{P}$. Define a binary operation + on G as follows:

- $0+g=g=g+0$ if $g\in G$.
- $P+P=e$ if P is a point
- $P+Q$ is the third point on PQ if P and Q are distinct points.

Then G is an abelian group. Indeed, 0 is the identity, each elements is its own inverse and the operation is clearly commutative. Checking that the operation is associative takes a little bit of effort: Let $P,Q,R\in G$.

If one of P,Q,R is equal to 0, then $P+(Q+R)$ and $(P+Q)+R$ both are equal to the sum of the other two.

So suppose that P,Q and R are points. If two of the points are equal, we will show that both $(P+Q)+R$ and $P+(Q+R)$ are equal to third point. So let S and T be points. Then

$$T+(S+S)=(S+S)+T=0+T=T$$

Also

$$S + (S + T) = S + (T + S) = (T + S) + S = (S + T) + S$$

If $S = T$, this is equal to S and so to T as required. So suppose $S \neq T$. Note $(S + T)T = ST$ and T is the point on ST distinct from S and $S + T$. Thus again $(S + T) + S = T$.

It remains to consider the case where P, Q and R are three distinct points.

If P, Q, R are collinear, then $P + Q = R$ and so $(P + Q) + R = R + R = 0$. Similarly $P + (Q + R) = P + P = 0$.

Suppose that P, Q, R are non-collinear. Then $(P + Q) + R$ and $P + (Q + R)$ both are equal to the unique point not incident with any of the lines PQ, PR and QR.

1.4 Subgroups, cosets and counting

Definition 1.4.1. *Let $(G, *)$ and $(H, \cdot)$ be groups. Then $(H, \cdot)$ is called a* subgroup *of $(G, *)$ provided that:*

(i) $H \subseteq G$.

(ii) $a * b = a \cdot b$ for all $a, b \in H$.

Note that, if $(H, \cdot)$ is a subgroup of $(G, *)$, then also $(H, *)$ is a subgroup of $(G, *)$.

Lemma 1.4.2. *Let $(G, *)$ be a group and $(H, \cdot)$ a subgroup of $(G, *)$. Then*

(a) $1_H = 1_G$ where 1_H is the identity of H with respect to $\cdot$ and 1_G is the identity of G with respect to $*$. In particular, $1_G \in H$.

(b) $a * b \in H$ for all $a, b \in H$.

(c) Let $a \in H$. Then the inverse of a in H with respect to $\cdot$ is the same as the inverse of a in G with respect to $*$. In particular, $a^{-1} \in H$.

Proof. (a)

$$1_H * 1_H = 1_H \cdot 1_H = 1_H = 1_H * 1_G$$

Multiplying with the inverse of 1_H in G from the left gives that $1_H = 1_G$.

(b) Let $a, b \in H$. Then by definition of a subgroup $a * b = a \cdot b$. Since $*$ is a binary operation of H, $a \cdot b \in G$ and $a * b \in H$.

(c) Let b be the inverse of a in H with respect to $\cdot$ and c the inverse of a in G with respect to $*$. Then

$$a * b = a \cdot b = 1_H = 1_G = a * c$$

Multiplying with the inverse of a in G from the left gives $b = c$. □

Lemma 1.4.3. *Let $(G, *)$ be a group and $H \subseteq G$. Then $(H, *)$ is a subgroup of $(G, *)$ if and only if* *(i)* $1_G \in H$;

(ii) *H is closed under multiplication, that is for all* $a, b \in H$, $ab \in H$; *and*

(iii) *H is closed under inverses, that is for all* $a \in H$, $a^{-1} \in H$.

Proof. Suppose first that (i), (ii) and (iii) hold. We will first verify that $(H, *)$ is a group.

By (ii), $*$ is a binary operation on H. Since $*$ is associative on G, it associative on H. Since $1_G \in H$ and 1_G is an identity for $*$ on G, its also an identity for $*$ on H.

Let $h \in H$. Then by (iii), $h^{-1} \in H$ and so h^{-1} is an inverse for h with respect to $*$ in H.

So $(H, *)$ is a group. Since $H \subseteq G$ and the same operation is used for H and G, conditions (i) and (ii) of a subgroup are fulfilled. So indeed, $(H, *)$ is a subgroup of $(G, *)$.

Suppose now that $(H, *)$ is a subgroup of $(G, *)$. Then 1.4.2 shows that (i), (ii) and (iii) hold. □

Let $(G, *)$ be a group and $(H, \cdot)$ a subgroup of G. Slightly abusing notation we will often just say that H is a subgroup of G. We also write $H \leq G$ if H is a subgroup of G.

Lemma 1.4.4. *Let G be a group and H a subset of G. Define the relation* $\sim_H$ *on G by*

$$a \sim_H b \quad \text{if and only if } a^{-1}b \in H$$

Then

(a) $e \in H$ *if and only* $\sim_H$ *is reflexive.*

(b) *H is closed under inverses if and only if* $\sim_H$ *is symmetric.*

(c) *H is closed under multiplication if and only if* $\sim_H$ *is transitive.*

In particular, H is a subgroup of G if and only $\sim_H$ *is an equivalence relation.*

Proof. (a) Suppose that $e \in H$. Let $a \in G$. Then $a^{-1}a = e \in H$. So $a \sim_H a$ and $\sim$ is reflexive.

Suppose $\sim_H$ is reflexive. Then $e \sim_H e$ and so $e = e^{-1}e \in H$.

(b) Suppose H is closed under inverses. Let $a, b \in G$ with $a \sim_H b$. Then $a^{-1}b \in H$ and so also $b^{-1}a = (a^{-1}b)^{-1} \in H$. Thus $b \sim_H a$. Hence $\sim_H$ is symmetric.

Suppose that $\sim_H$ is symmetric. Let $h \in H$. Then $e^{-1}h = h \in H$ and so $e \sim_H h$. Since $\sim H$ is symmetric, $h \sim_H e$ and so $h^{-1} = h^{-1}e \in H$.

(c) Suppose H is closed under multiplication. Let $a, b, c \in G$ with $a \sim_H b$ and $b \sim_H c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$ and so, since H is closed under multiplication,

$$a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$$

Thus $a \sim_H c$ and $\sim_H$ is transitive.

Suppose $\sim H$ is transitive. Let $a, b \in H$. Then $(a^{-1})^{-1}e = ae = a \in H$ and $e^{-1}b = b \in H$. So $a^{-1} \sim_H e$ and $e \sim_H b$. Since $\sim_H$ is transitive, this gives $a^{-1} \sim_H b$. Thus $ab = (a^{-1})^{-1}b \in H$ and H is closed under multiplication □

Definition 1.4.5. *Let I be a set and $\sim$ a relation on I.*

For $a \in I$ put

$$[a]_\sim := \{b \in I \mid a \sim b$$

$[a]_\sim$ is called the class *of $\sim$ associated to a.*

$$I/\sim = \{[a]_\sim \mid a \in I\}$$

is set of classes of I.

If $\sim$ is a an equivalence relation, the classes of $\sim$ is also called the equivalence class of $\sim$ containing a.

We will often write $[a]$ for $[a]_\sim$.

Lemma 1.4.6. *Let $\sim$ be a equivalence relation on the set I.*

(a) Each $i \in i$ lies in a unique equivalence class of $\sim$, namely $[i]_\sim$.

(b) $|i| = \sum_{c \in i/\sim} |c|$.

Proof. (a) Let $a \in i$. since $\sim$ is reflexive, $a \sim a$. So $a \in [a]$ and a is contained in an equivalence class of i. Now let c be any equivalence class of $\sim$ with $a \in C$. We need to show that $C = [a]$. By definition of an equivalence class, $C = [b]$ for some $b \in I$. Since $a \in C = [b]$ we have $b \sim a$

Let $c \in [a]$. Then $a \sim c$. Since $\sim$ is transitive, $b \sim c$ and so $c \in [b]$. Hence $[a] \subseteq [b]$.

We proved that if $a \in [b]$ then $[a] \subseteq [b]$. Since $b \sim a$ and $\sim$ is symmetric we have $a \sim b$ and $b \in [a]$. Thus $[b] \subseteq [a]$.

Hence $[b] = [a]$ and (a) holds.

(b) follows immediately from (a). □

Definition 1.4.7. *Let G be a magma, $g \in G$ and $A, B \subseteq G$.*

(a) $gA = \{ga \mid a \mid a \in A$ and $Ag = \{ag \mid a \in A\}$.

(b) $B/A = \{bA \mid b \in B\}$.

(c) Suppose G is a group and A a subgroup of G. Then

   (a) gA is called the (left) coset *of A in G containing g.*

   (b) Ag is called a right coset of A in G.

   (c) $|G/A|$ is called the index *of A in G.*

Proposition 1.4.8. *Let H be a subgroup of G and $g \in G$.*

(a) gH is the equivalence class of $\sim_H$ containing g.

(b) g lies in a unique coset of H in G, namely in gH.

(c) $|gH| = |H|$.

Proof. (a) We have

$$\begin{aligned} a \in gH \quad &\Longleftrightarrow \quad a = gh \text{ for some } h \in H \quad \Longleftrightarrow \quad g^{-1}a = h \text{ for some } h \in H \\ &\Longleftrightarrow \quad g^{-1}a \in H \Longleftrightarrow g \sim_H a \quad \Longleftrightarrow \quad a \in [g] \end{aligned}$$

So $gH = [g]$.

(b) This follows from (a) and 1.4.6.

(c) Define $f : H \to gH, h \to gh$. Then by definition of gH, f is onto. If $gh = gh'$ for some h, h', then $h = h'$. Hence f is 1-1. This gives (c). □

Theorem 1.4.9 (Lagrange)**.** *Let H be a subgroup of G. Then* $|G| = |G/H| \cdot |H|$*. In particular if G is finite, the order of H divides the order of G.*

Proof.

$$|G| \overset{1.4.6(b)}{=} \sum_{C \in G/\sim_H} |C| \overset{1.4.8(c)}{=} \sum_{C \in G/H} |C| \overset{1.4.8(c)}{=} \sum_{C \in G/H} |H| = |G/H| \cdot |H|$$

□

1.4.10 (Cycle Notation)**.** We will often use cycle notation to denoted elements of $\mathrm{Sym}(n)$:

For $1 \le j \le l$ and $1 \le i \le k_j$ let $1 \le a_{i,j} \le n$ such that for each $1 \le m \le n$ there exists a unique $1 \le j \le l$ and $1 \le i \le k_l$ with $m = a_{i,j}$. Then

$$(a_{1,1}, a_{2,1}, a_{3,1}, \ldots a_{k_1,1})(a_{1,2}, a_{2,2} \ldots a_{k_2,2}) \ldots (a_{1,l}, a_{2,l} \ldots a_{k_l,l})$$

denotes the element $\pi \in \mathrm{Sym}(n)$ with

$$\pi(a_{i,j}) = a_{i+1,j} \text{ and } \pi(a_{k_j,j}) = a_{1,j}$$

for all $1 \le i < k_j$ and $1 \le j \le l$.

$(a_{1,j}, a_{2,j}, \ldots, a_{k_j,j})$ is called a cycle of length k_j of π. If n is understood, we will not bother to list the cycles of length 1. Also we will often drop the separating comas in the cycle. For example in $\mathrm{Sym}(9)$,

$$(2975)(13)(48)$$

denotes the permutation with

$$1 \to 3, 2 \to 9, 3 \to 1, 4 \to 8, 5 \to 2, 6 \to 6, 7 \to 5, 8 \to 4, 9 \to 7$$

Example 1.4.11. Let $G = \mathrm{Sym}(3)$ and $H = \{(1), (12)\}$. Then

$$(1) \circ H = H = \{(1), (12)\} = (12) \circ H$$

$$(123) \circ H = \{(123) \circ (1), (123) \circ (12)\} = \{(123), (13)\} = (13) \circ H$$

$$(132) \circ H = \{((132) \circ (1), (132) \circ (12)\} = \{(132), (23)\} = (23) \circ H$$

Hence

$$|G| = 6, |G/H| = 3 \text{ and } |H| = 2$$

So by Lagrange's

$$6 = 3 \cdot 2$$

Definition 1.4.12. *(a) Let I be set, then $\mathcal{P}(I)$ denotes the* power set *of G, that is the set of subsets of I.*

(b) Let G be a magma. For $H, K \subseteq G$ put

$$HK = \{hk \mid h \in H, k \in K\}.$$

(c) Let G be a group. For $H \subseteq G$ define $H^{-1} = \{h^{-1} \mid h \in H\}$.

Lemma 1.4.13. *Let G be a magma.*

(a) $\mathcal{P}(G)$ is magma under the operation $(A, B) \to AB$.

(b) If G is associative, so is $\mathcal{P}(G)$.

(c) If e is an identity for G, then $\{e\}$ is an identity for $\mathcal{P}(G)$.

(d) If G is a monoid, so is $\mathcal{P}(G)$.

(e) If G is a group and $A, B \subseteq G$, then $(AB)^{-1} = B^{-1}A^{-1}$.

Proof. Let $A, B, C \subseteq G$.

(a) By definition, AB is a subset if G and so the $\mathcal{P}(G)$ is closed under the operation $(A, B) \to (A, B)$.

(b) We have

$$(AB)C = \{(ab)c \mid a \in A, b \in B, c \in C\} = \{a(bc) \mid a \in A, b \in B, c \in C\} = A(BC)$$

(c) Obvious.

(d) follows from (a), (b), (c)

(e) $(AB)^{-1} = \{(ab)^{-1} \mid a \in A, b \in B\} = \{b^{-1}a^{-1} \mid b \in B, a \in A\} = B^{-1}A^{-1}$. □

Lemma 1.4.14. *Let G be a group, H a subset of G and K a subgroup of G.*

(a) $(gk)K = gK$ for all $g \in G, k \in K$.

(b) $KK = K$ and $K^{-1} = K$.

(c) $H/K = HK/K$

(d) The map $\alpha : H/H\cap K \to H/K, h(H\cap K) \to hK$ is a well defined bijection. Moreover, $\alpha(C) = CK$ for all $C \in H/H \cap K$.

(e) $|HK| = |HK/K| \cdot |K| = |H/H \cap K| \cdot |K|$.

(f) If G is finite and H is a subgroup of K, then $|HK| = \frac{|H||K|}{|H\cap K|}$

Proof. (a) Since K is closed under multiplication $kK \subseteq K$. Let $l \in K$. Then $l = k(k^{-1}l) \in kK$ and so $K \subseteq kK$. Thus $K = kK$ and so also $(gk)K = g(kK) = gK$.

(b) By (a), $kK = K$ for all $k \in K$ and so $KK = K$. Since K is closed under inverse $K^{-1} \subseteq K$. Since $k = (k^{-1})^{-1}$ and $k^{-1} \in K$, $K \subseteq K^{-1}$. Hence $K = K^{-1}$.

(c) Since $e \in K$, $H \subset HK$ and so $H/K \subseteq HK/K$. Let $h \in H$ and $k \in K$. Then by (d) $(hk)K = hK \in H/K$ and so $HK/K \subseteq H/K$.

(d) Let $C \in H/H \cap K$. Then $C = h(H \cap K)$ for some $h \in H$. We compute

$$CK = \big(h(H \cap K)\big)K = h\big((H \cap K)K\big) = hK$$

so $\alpha(C) = CK$ and the definition of α is independent of the choice of h. Clearly α is onto.

Finally if $hK = jK$ for some $h, j \in H$, then $h^{-1}jK = K$, $h^{-1}j \in K$ and so $h^{-1}j \in H \cap K$ and $h(H \cap K) = j(H \cap K)$. Thus α is 1-1.

(e) Note that $HK = \bigcup_{h\in H} hK$. Hence

$$|HK| = \sum_{C\in H/K} |C| = |H/K| \cdot |K| \overset{(d)}{=} |H/H \cap K| \cdot |K|.$$

(f) By Lagrange's $|H| = |H/H \cap K| \cdot |H \cap K|$. So if G is finite, $|H/H \cap K| = \frac{|H|}{|H\cap K|}$ and thus (f) follows from (e). □

1.5 Equivalence Relations

Definition 1.5.1. *Let $\sim$ be a relation on the set J and let $f : I \to J$ be a function. Then $\sim_f$ is the relation on I defined by*

$$i \sim_f k \quad \Longleftrightarrow \quad fi \sim fk$$

for all $i, k \in I$.

Lemma 1.5.2. *Let $\sim$ be a relation on the set J and let $f : I \to J$ be a function.*

(a) If $\sim$ is reflexive, so is $\sim_f$.

(b) If $\sim$ is symmetric, so is $\sim_f$.

(c) If $\sim$ is transitive, so is $\sim_f$.

(d) If $\sim$ is equivalence relation so is $\sim_f$.

Proof. (c) Suppose $\sim$ is transitive and le $a, b, c \in I$ with $a \sim_f b$ and $b \sim_f c$. Then $fa \sim fb$ and $fb \sim fa$. Since $\sim$ is transitive, $fa \sim fc$ and so $a \sim_f c$. Thus $\sim_f$ is transitive.

The proofs for (a) and (b) are similar and somewhat easier. (d) follows from (a)-(c). □

Lemma 1.5.3. *Let I be a set and $\sim$ a relation on I. Define*

$$\approx = \bigcap \{ \approxeq \mid \approxeq \text{ an equivalence relation on } I \text{ with } \sim \subseteq \approxeq \}$$

Then

(a) $\approx$ is an equivalence relation on I, called the equivalence relation *generated by $\sim$.*

(b) Let $a, b \in I$. Then $a \approx b$ if and only if there exists $n \in \mathbb{N}$ and a sequence of elements $(x_0, x_1, \ldots x_n)$ in I such that $x_0 = a$, $x_n = b$ and for each $1 \leq i \leq n$ either $x_{i-1} \sim x_i$ or $x_i \sim x_{i-1}$.

Proof. Straightforward. □

Definition 1.5.4. *Let $f : I \to J$ be a function, $\sim$ a relation on I and $\approxeq$ a relation J.*

$(\sim, \approxeq)$ is called f-invariant if for all $a, b \in I$:

$$a \sim b \qquad \Longrightarrow \qquad f(a) \approxeq f(b)$$

Lemma 1.5.5. *Let $\sim$ a relation on the set I and $\approx$ the equivalence relation generated by $\sim$. Let $\approxeq$ be a equivalence relation on the set J and $f : I \to J$ a function.*

(a) If $(\sim, \approxeq)$ is f-invariant, then also $(\approx, \approxeq)$ is f-invariant.

(b) If $f(a) = f(b)$ for all $a, b \in I$ with $a \sim b$, then $f(a) = f(b)$ for all $a, b \in I$ with $a \approx b$.

Proof. (a) Let $a, b \in I$ with $a \sim b$. Then $fa \approxeq fb$ and so $a \approxeq_f b$. Thus $\sim \subseteq \approxeq_f$. By 1.5.2 $\approxeq_f$ is an equivalence relation on I and so by definition of $\approx$, $\approx \subseteq \approxeq_f$. Thus $a \approx b$ implies $a \approxeq_f b$, that is $fa \approxeq fb$.

(b) Just apply (a) with $\approxeq$ the equality relation. □

Lemma 1.5.6. *Let $f : I \to J$ be a function, $\sim$ a relation on I and $\approxeq$ a relation on J.*

(a) $(\sim, \approxeq)$ is f-invariant if and only $\sim \subseteq \approxeq_f$.

(b) $(\approxeq_f, \approxeq)$ is f-invariant.

(c) $(\sim, =)$ is f-invariant if and only if $\sim \subseteq =_f$.

(d) $(=_f, =)$ is f-invariant.

Proof. (a) $(\sim, \approxeq)$ is f invariant if and only if

$$a \sim b \qquad \Longrightarrow \qquad f(a) \approxeq f(b)$$

and so if and only if

$$a \sim b \qquad \Longrightarrow \qquad a \approxeq_f b$$

(b) follows from (a).

(c) and (d): Just apply (a) and (b) with $\approxeq$ the equality relation. □

Lemma 1.5.7. *Let $f : I \to J$ be a function, $\sim$ a relation on f and $\approx$ a relation on J. Suppose $(\sim, \approx)$ is f-invariant. Then*

(a) $f\big([a]_\sim\big) \subseteq [fa]_\approx$ for all $a \in I$.

(b) Suppose $I \subseteq \mathrm{Dom}(\sim)$ and $\approx$ is an equivalence relation on J. Then

$$\overline{f} : I/\sim \to J/\approx, \ [a]_\sim \to [fa]_\approx$$

is a well-defined function.

Proof. (a) Let $x \in f\left([a]_\sim\right)$. Then $x = fb$ for some $b \in I$ with $a \sim b$. Since $a \sim b$ we have $fa \approx fb$ and so $x = fb \in [fa]_\approx$.

(b) Let $a, b \in I$ with $[a]_\sim = [b]_\sim$. Since $I \subseteq \mathrm{Dom}(\sim)$, there exists $c \in I$ with $a \sim c$. Then $c \in [a]_\sim = [b]_\sim$ and so $b \sim c$. Hence $fa \approx fc$ and $fb \approx fc$. Since $\approx$ is an equivalence relation, this gives $fa \approx fb$ and $[fa]_\approx = [fb]_\approx$. □

Lemma 1.5.8 (Isomorphism Theorem for Sets)**.** *Let $f : I \to J$ be a function. Then the function*

$$\overline{f} : I/=_f \to \mathrm{Im} f, \ [a]_{=_f} \to fa$$

is a well-defined bijection.

Proof. Let $a, b \in I$. Then

$$f(a) = f(b) \quad \Longleftrightarrow \quad a =_f b \quad \Longleftrightarrow \quad [a]_{=_f} = [b]_{=_f}$$

and so $\overline{f}$ is well-defined and 1-1. $\overline{f}$ is clearly onto and so the lemma holds. □

1.6 Normal subgroups and the isomorphism theorem

Example 1.6.1. Let $G = \mathrm{Sym}(3)$ and $H = \{(1), (12)\}$. Then

$$(23) \circ H = \{(23), (132)\} \text{ and } H \circ (23) = \{(23), (123)\}$$

So $(23) \circ H \neq H \circ (23)$.

Note that $gH = Hg$ if and only if $gHg^{-1} = H$. We therefore introduce the following notation:

Definition 1.6.2. *Let G be a group, $a, b \in G$ and $D \subseteq G$.*

(a) ${}^a b = aba^{-1}$. ${}^a b$ is called the conjugate of b under a.

(b) ${}^a D = aDa^{-1} = \{ada^{-1} \mid d \in D\} = \{{}^a d \mid d \in D\}$.

(c) The function $\mathrm{i}_a : G \to G, g \to {}^a g$ is called the inner automorphism *of G induced by a. i_a is also called* conjugation *by a*

Lemma 1.6.3. *Let $N \leq G$. Then the following statements are equivalent:*

(a) $^{g}N = N$ *for all* $g \in G$.

(b) $gN = Ng$ *for all* $g \in G$.

(c) Every left coset is a right coset.

(d) Every left coset is contained in a right coset.

(e) $^{g}N \subseteq N$ *for all* $g \in G$.

(f) $^{g}n \in N$ *for all* $g \in G$, $n \in N$.

Proof. Suppose (a) holds. Then $gNg^{-1} = N$ for all $g \in G$. Multiplying with g from the right we get $gN = Ng$.

Suppose (b) holds. Then the left cosets gN equals the right coset Ng. so (c) holds.

Clearly (c) implies (d)

Suppose that (d) holds. Let $g \in G$. Then $gN \subseteq Nh$ for some $h \in G$. Since $g \in gN$ we conclude $g \in Nh$. By 1.4.8(b), Ng is the unique right coset of N containing g and so and $Ng = Nh$ Thus $gN \subseteq Ng$. Multiplying with g^{-1} from the right we get $gNg^{-1} \subseteq N$. Thus (e) holds.

Clearly (e) implies (f).

Finally suppose that (f) holds. Then $gNg^{-1} \subseteq N$ for all $g \in G$. This statement applied to g^{-1} in place of g gives $g^{-1}Ng \subseteq N$. Multiplying with g from the left and g^{-1} from the right we obtain $N \subseteq gNg^{-1}$. Hence $N \subseteq {}^{g}N$ and $^{g}N \subseteq N$. So $N = {}^{g}N$ and (a) holds. □

Definition 1.6.4. *Let G be a group and $N \leq G$. We say that N is* normal *in G and write $N \trianglelefteq G$ if N fulfills one (and so all) of the equivalent conditions in 1.6.3.*

Example 1.6.5. 1. From 1.6.1 we have $(2,3)\mathrm{Sym}(2) \neq \mathrm{Sym}(2)(2,3)$ and so $\mathrm{Sym}(2)$ is not a normal subgroup of $\mathrm{Sym}(3)$.

2. Let $H = \{(1), (123), (132)\}$. Then H is a subgroup of $\mathrm{Sym}(3)$. By Lagrange's

$$|\mathrm{Sym}(3)/H| = \frac{|\mathrm{Sym}(3)|}{|H|} = \frac{6}{3} = 2$$

Hence H has exactly two cosets in H. One of them is

$$H = \{(1), (123), (132)\}$$

Since each element of $\mathrm{Sym}(3)$ lies in a unique coset of H, the other coset must be

$$\mathrm{Sym}(3) \setminus H = \{(12), (13), (23)\}$$

The same argument shows that H and $\mathrm{Sym}(3) \setminus H$ are the only right cosets of $\mathrm{Sym}(3)$. Thus every coset is a right coset and so H is normal in $\mathrm{Sym}(3)$.

3. Let n be a positive integer, let $\mathrm{GL}_n(\mathbb{R})$ the set of invertible $n\times n$-matrices with coefficients in $\mathbb{R}$ and let $\mathrm{SL}_n(\mathbb{R})$ the set of $n \times n$-matrices with coefficients in $\mathbb{R}$ and determinant 1. Note that $GL_n(\mathbb{R})$ is a group under matrix multiplication and $\mathrm{SL}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. $\mathrm{GL}_n(\mathbb{R})$ is called a *general linear group* and $\mathrm{SL}_n(\mathbb{R})$ a *special linear group*. Let $A \in \mathrm{GL}_n(\mathbb{R})$ and $B \in \mathrm{SL}_n(\mathbb{R})$. Then

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det B = 1$$

and so $ABA^{-1} \in \mathrm{SL}_n(\mathbb{R})$. Thus $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Lemma 1.6.6. *Let G and H be monoid and $\phi : G \to H$ a magma-homomorphism. Then the following are equivalent.*

(a) $\phi(1) = 1$, that is ϕ is a monoid-homomorphism.

(b) $\phi(1)$ is (left,right,) invertible

(c) There exists g in G such that $\phi(g)$ is (left,right,) invertible.

Proof. (a) $\Longrightarrow$ (b): Suppose that $\phi(1) = 1$. Then $\phi(1)\phi(1) = \phi(1 \cdot 1) = \phi(1) = 1$ and $\phi(1)$ is invertible.

(b) $\Longrightarrow$ (c): Obvious.

(c) $\Longrightarrow$ (a): Suppose $g \in G$ such that $\phi(g)$ is left-invertible in H and choose $h \in H$ with $h\phi(g) = 1$. Then

$$\phi(1) = 1\phi(1) = (h\phi(g))\phi(1) = h(\phi(g)\phi(1)) = h\phi(g) = 1$$

□

Lemma 1.6.7. *Let $\phi : G \to H$ be a monoid homomorphism. Suppose $g \in G$ and g' is (left,right,) inverse of g in G. Then $\phi(g')$ is a (left,right,) inverse of $\phi(g)$ in G.*

Proof. By symmetry it suffices to tread the case where g' is left inverse of g. Then

$$\phi(g')\phi(g) = \phi(g'g) = \phi(1) = 1$$

□

We will now start to establish a connection between normal subgroups and homomorphism.

Lemma 1.6.8. *Let $\phi : G \to H$ be a group homomorphism.*

(a) $\phi(1_G) = 1_H$, that is ϕ is a monoid-homomorphism.

(b) $\phi(a^{-1}) = \phi(a)^{-1}$.

(c) $\phi({}^g a) = {}^{\phi(g)}\phi(a)$.

(d) If $A \leq G$ then $\phi(A) \leq H$.

(e) If $B \leq H$ then $\phi^{-1}(B) \leq G$.

(f) Put $\ker\phi := \{g \in G \mid \phi(g) = 1_H\}$. Then $\ker\phi$ is a normal subgroup of G.

(g) If $N \trianglelefteq G$, and ϕ is onto, $\phi(N) \trianglelefteq H$.

(h) If $M \trianglelefteq H$, $\phi^{-1}(M) \trianglelefteq G$.

Proof. Except for (c), (f) and (**??**) this is Exercise 2 on Homework 2.

(c) $\phi({}^{g}a) = \phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) \overset{\text{(b)}}{=} \phi(g)\phi(a)\phi(g)^{-1} = {}^{\phi(g)}\phi(a)$.

(f) This follows from (h) applied to the normal subgroup $M = \{1_H\}$ of H.

□

Lemma 1.6.9. *Let $\phi : G \to H$ be a homomorphism of groups.*

(a) Let $a, b \in G$. Then $\phi(a) = \phi(b)$ if and only if $a\ker\phi = b\ker\phi$.

(b) The relations $=_\phi$ on G is the same as the relation $\sim_{\ker\phi}$.

(c) ϕ is 1-1 if and only if $\ker\phi = \{1_G\}$.

Proof. Let $a, b \in G$. Then

$$\begin{array}{cccc}
 & a & =_\phi & b \\
\Longleftrightarrow & \phi(a) & = & \phi(b) \\
\Longleftrightarrow & \phi(a)^{-1}\phi(b) & = & 1_H \\
\Longleftrightarrow & \phi(a^{-1}b) & = & 1_H \\
\Longleftrightarrow & a^{-1}b & \in & \ker\phi \\
\Longleftrightarrow & a & \sim_{\ker\phi} & b \\
\Longleftrightarrow & g\ker\phi & = & k\ker\phi
\end{array}$$

Thus (a) and (b) hold.

(c) By (a) ϕ is 1-1 if and only if $\{a\} = a\{\ker\phi\}$ for all $a \in A$ and so if and only f $\ker phi = \{1_G\}$. □

Lemma 1.6.10. *Let G be a group and $N \trianglelefteq G$. Let $T, S \in G/N$ and $a, b \in G$ with $T = aN$ and $S = bN$.*

(a) $TS \in G/N$, namely $(aN)(bN) = (ab)N$.

(b) $T^{-1} \in G/N$, namely $(aN)^{-1} = a^{-1}N$.

(c) $TN = T = NT$.

(d) $TT^{-1} = N = T^{-1}T$.

(e) G/N is a group under the binary operation $G/N \times G/N \to G/N, (T, S) \to TS$.

(f) The map $\pi_N : G \to G/N, \quad g \to gN$ is an onto homomorphism with kernel N.

Proof. (a) $(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN$.

(b) $(aN)^{-1} = N^{-1}a^{-1} = Na^{-1} = a^{-1}N$.

(c) We have $N = eN$ and so by (a) $TN = (aN)(eN) = (ae)N = aN = T$. Similarly $NT = T$.

(d) By (a) and (b) $TT^{-1} = (aN)(a^{-1})N = (aa^{-1})N = eN = N$. Similarly $T^{-1}T = N$.

(f) By (a) the map $G/N \times G/N \to G/N, (T, S) \to TS$ is a well-defined binary operation on G/N. By 1.4.13 multiplication of subsets is associative. By (c) N is an identity element and by (f), T^{-1} is an inverse of T. Thus (e) holds.

(f) We have

$$\pi_N(ab) = abN = (aN)(bN) = \pi_N(a)\pi_N(b)$$

So π_N is a homomorphism. Clearly π_N is onto. We have

$$\ker \pi_N = \{a \in G \mid \pi_N(a) = 1_{G/N}\} = \{a \in G \mid aN = N\} = \{a \in G \mid a \in N\} = N$$

□

Theorem 1.6.11 (The Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism of groups. The map*

$$\overline{\phi} : G/\ker\phi \to \phi(H), \quad g\ker\phi \to \phi(g)$$

is a well-defined isomorphism. Moreover, $\phi = \overline{\phi} \circ \pi_{\ker\phi}$.

Proof. Since $a\ker\phi = b\ker\phi$ if and only of $a =_\phi b$, 1.5.8 shows that $\overline{\phi}$ is a well-defined bijection.

We have

$$\overline{\phi}\big(((g\ker\phi)(k\ker\phi)\big) = \overline{\phi}\big(gk\ker\phi\big) = \phi(gk) = \phi(g)\phi(k) = \overline{\phi}\big(g\ker\phi\big)\overline{\phi}\big(k\ker\phi\big)$$

and so $\overline{\phi}$ is a homomorphism.

Also

$$(\phi \circ \pi_{\ker\phi})(g) = \overline{\phi}\big(\pi_{\ker\phi}(g)\big) = \overline{\phi}\big(g\ker\phi\big) = \phi(a)$$

and so $\phi = \overline{\phi} \circ \pi_{\ker\phi}$ □

The Isomomorphism Theorem can be summarized in the following diagram:

$$\begin{tikzcd}
 & & G \arrow[dddll, "\phi"'] \arrow[dddrr, "\pi_{\ker\phi}"] & & \\
 & & g \arrow[dl] \arrow[dr] & & \\
 & \phi(g) & & g\ker\phi \arrow[ll] & \\
\mathrm{Im}\,\phi & & & & G/\ker\phi \arrow[llll, "\cong", "\overline{\phi}"']
\end{tikzcd}$$

Example 1.6.12. Define $\det : GL_n(\mathbb{R}) \to (\mathbb{R} \smallsetminus \{0\}, \cdot), A \to \det(A)$. Since $\det(AB) = \det(A)\det(B)$, det is a homomorphism. It is easy to see that det is onto. Also $\ker\det = \mathrm{SL}_n(\mathbb{R})$. So 1.6.8(f) gives a new proof that $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$. Moreover the Isomorphism Theorem implies

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(R) \cong (\mathbb{R} \smallsetminus \{0\}, \cdot)$$

1.7 Group Actions

Definition 1.7.1. *Let $(G, \cdot)$ be a magma and S a set. Let $*$ be a function such that $G \times S$ is contained in the domain of $*$. For $g \in G$ and $s \in S$, write $g * s$ for $*(g, s)$. $*$ is called an magma* action *of G on S if*

(A0) *$g * s \in S$ for all $g \in G, s \in S$.*

(A1) *$(a \cdot b) * s = a * (b * s)$ for all $a, b \in G$, $s \in S$.*

*A G-*set *is a set S together with a magma-action of G on S.*

Definition 1.7.2. *Let $(G, \cdot)$ be a monoid and S a set. A magma action $*$ of $(G, \cdot)$ on S is called a monoid-action if*

(A2) *$1_G * s = s$ for all $s \in S$.*

In the case that $(G, \cdot)$ is group, a monoid-action of $(G, cdot)$ is also called a group-action.

We will often just write as for $a * s$. The three axioms of a monoid action then read $as \in S$, $1s = s$ and $(ab)s = a(bs)$.

Example 1.7.3. Let $(G, \cdot)$ be a group,

1. Note the similarity between the definition of a group action and the definition of a group. In particular, we see that the operation $\cdot$ of group G defines an action of G on G, called the action by *left multiplication.* Indeed, since $\cdot$ is a closed operation (A0)- holds. Since 1_G is an identity, (A2) holds and since $\cdot$ is associative (A1) holds.

2. The function
$$\cdot_{\mathrm{op}} : G \times G \to G, (a, s) \to s \cdot a$$
is not an action (unless G is abelian). Indeed
$$(a \cdot b) \cdot_{\mathrm{op}} s = s \cdot (a \cdot b) = (s \cdot a) \cdot b = b \cdot_{\mathrm{op}} (a \cdot_{\mathrm{op}} s)$$
But observe that $\cdot_{\mathrm{op}}$ is an action of G^{op} on G.

   To obtain an action of G on G define
$$\cdot_{\mathrm{r}} : \quad G \times G, (a, s) \to sa^{-1}.$$
Then $(ab) \cdot_{\mathrm{r}} s = s(ab)^{-1} = sb^{-1}a^{-1} = a \cdot_{\mathrm{r}} (b \cdot_{\mathrm{r}} s)$ and $\cdot_{\mathrm{r}}$ is indeed an action. This action is called the action of G on G by *right multiplication*.

3. G acts on G via conjugation:
$$\mathrm{c} : G \times G \to G, (a, g) \to {}^{a}g$$
Indeed ${}^{1}g = g$ and ${}^{(ab)}g = {}^{a}({}^{b}g)$.

4. Let $*$ be an action of G on the set I and let $H \leq G$. Then $*$ is also an action of H on I. In particular, we obtain actions of H on G by left multiplication, right multiplication and by conjugation.

5. Let I be a set. Then $\mathrm{Sym}(I)$ acts on I via
$$\mathrm{Sym}(I) \times I \to I, (\pi, i) \to \pi(i)$$
Indeed, $\mathrm{id}_I(i) = i$ for all i in I and $\alpha(\beta(i)) = (\alpha\beta)(i)$ for all $\alpha, \beta \in \mathrm{Sym}(I), i \in I$.

6. Let G be a group. Then $\mathrm{Aut}(G)$ acts on G via
$$\mathrm{Aut}(G) \times G \to G, (\alpha, g) \to \alpha(g)$$
Indeed by (3), $\mathrm{Sym}(G)$ acts on G and so by (4) also the subgroup $\mathrm{Aut}(G)$ of $\mathrm{Sym}(G)$ acts on G.

Notation 1.7.4. *Let $*$ and $\diamond$ be actions of the magma G on the set S. We will write $* \equiv \diamond$ if $g * s = g \diamond s$ for all g and $s \in S$.*

Note that $*\equiv\diamond$ if and only if the restrictions of $*$ and $\diamond$ to $G\times S, S$ are equal. Often we will be sloppy and consider two action with $*\equiv\diamond$ to be equal.

We will now show that an action of magma G on S can also by thought of as an homomorphism from G to $Fun(S,S)$.

Definition 1.7.5. *Let A,B be sets.*

(a) $\mathrm{Fun}(A)$ *is the class of function with domain A.* $\mathrm{Fun}(A,B)$ *is the set of function from A to B.*

(b) Let $f\in\mathrm{Fun}(A\times B)$. For $a\in A$ define $f_a\in\mathrm{Fun}(B)$ by

$$f_a(b)=f(a,b)$$

for all $b\in B$. Define $f_A: A\to\mathrm{Fun}(B), a\to f_a$. f_A is called the function on A associated to f.

Then we view f as binary operation and use the notion $a*b$ for $f(a,b)$, we will use the notation a^* for f_a, so $a^*(b)=a*b$.

(c) Let $g: A\to\mathrm{Fun}(B)$ a function. Define $g_{A\times B}\in\mathrm{Fun}(A\times B)$ by

$$g_{A\times B}(a,b)\to g(a)(b)$$

for all $(a,b)\in A\times B$. $g_{A\times B}$ is called the function on $A\times B$ associated to g.

Lemma 1.7.6. *Let A,B be sets.*

(a) Let $f\in\mathrm{Fun}(A\times B)$, Then $(f_A)_{A\times B}=f$.

(b) Let $g: A\to\mathrm{Fun}(B)$ be a function. Then $(g_{A\times B})_A=f$.

Proof. Let $a\in A$ and $b\in B$.

(a)

$$(f_A)_{A\times B}(a,b)=f_A(a)(b)=f_a(b)=f(a,b)$$

and so $(f_A)_{A\times B}=f$.

(b)

$$(g_{A\times B})_A(a)(b)=(g_{A\times B})_a(b)=g_{A\times B}(a,b)=g(a)(b)$$

and so $(g_{A\times B})_A=g$. □

Lemma 1.7.7. *Let G be a magma, S a set, $*\in Fun(G\times S)$ and $*_G: G\to\mathrm{Fun}(S)$ the function on G associated to $*$.*

(a) $*$ is an magma-action of G on S if and only if Φ is a magma-homomorphism from G to $\mathrm{Fun}(S,S)$.

(b) Suppose G is monoid. Then $*$ is a monoid-action if and only if Φ is a monoid-homomorphism from G to $\mathrm{Fun}(S,S)$.

(c) *Suppose G is a group. Then $*$ is a group-action if and only if Φ is a homomorphism from G to* $\mathrm{Sym}(S)$.

Proof. Let $g, h \in G$ and $s \in S$.

(a) Since $g^*(s) = g * s$, (A0) holds if and only if g^* is a function from S to S for all $g \in G$ and if and only if $*_G$ is a function from G to $\mathrm{Fun}(S, S)$.

So we may assume that:

1°. *(A0) holds and $*_G$ is a function from G to* $\mathrm{Fun}(S, S)$.

Since

$$(g^* \circ h^*)(s) = g * (h * s)\text{and } (gh)^*(s) = (gh) * s$$

we see that (A1) holds if and only if $*_G$ is a homomorphism from G to $\mathrm{Fun}(S, S)$. Thus (a) holds.

(b) Suppose G is a monoid. Since $1^*(s) = 1 * s$, (A2) holds if and only if $*_G(1) = \mathrm{id}_S$. Together with (a) this gives (b).

(c) Suppose that now that G is a group. Recall that a group-action for G is the same as monoid action for G.

Assume first that $*$ is an monoid-action of G on S. Then by (b) $*_G$ is a monoid- homomorphism from G to $\mathrm{Fun}(S, S)$. Since each element in G is invertible, 1.6.7 shows that $*_G(g)$ is invertible for all $g \in G$. Thus $*_G(g) \in \mathrm{Sym}(S)$ and $*_G$ is homomorphism from G to $\mathrm{Sym}(S)$.

Assume next that $*_G$ is a homomorphism from $G \to \mathrm{Sym}(G)$. Then by 1.6.8(a) $*_G$ is a monoid-homomorphism and so (b) $*$ is an monoid-action of G on S.

□

Example 1.7.8. 1. Let $(G, \cdot)$ be a group. For $a \in G$, define $g^{\cdot} : G \to G, g \to ag$. Then by 1.7.3(1) and 1.7.7 the map

$$\Phi : \; G \to \mathrm{Sym}(G), \; g \to g^{\cdot}$$

is a homomorphism. If $\Phi(a) = \mathrm{id}_G$, then $a = a1 = \Phi(a)(1) = \mathrm{id}_G(1) = 1$ and so Φ is 1-1. Thus $G \cong \Phi(G)$. In particular, G is isomorphic to a subgroup of a symmetric group. This is known as *Cayley's Theorem.*

2. Let G be group. Recall that for $g \in G$, i_g is the map

$$\mathrm{i}_g : G \to G, a \to {}^g a$$

By 1.7.3(1) G acts G by conjugation, the corresponding homomorphism is

$$\mathrm{i}_G : G \to \mathrm{Sym}(G), g \to \mathrm{i}_g$$

3. The homomorphism corresponding to the action of $\mathrm{Sym}(I)$ on I is $\mathrm{id}_{\mathrm{Sym}(I)}$. Indeed $*_\pi(i) = \pi * i = \pi(i)$ and so $*_\pi = \pi$ for all $\pi \in \mathrm{Sym}(I)$.

Definition 1.7.9. *Let $*$ by an action of the group G on the set S, $H \subseteq G$,$g \in G$, $s \in S$ and $T \subseteq S$. Then*

(a) $\mathrm{Stab}^*_H(T) = \{h \in H \mid g * t = t \text{ for all } t \in T\}$ *and* $\mathrm{Stab}^*_H(s) = \{h \in H \mid h * s = s\}$. $\mathrm{Stab}^*_H(T)$ *is called the* stabilizer *of T in H.*

(b) We $g * s = s$ we say that g fixes s or that s is a fixed-point of g. If $h * s = s$ for all $h \in H$ we say H fixes s or that s is a fixed-point H of G.

(c) $\mathrm{Fix}^*_T(H) = \{t \in T \mid h * t = t \text{ for all } t \in T\}$ *and* $\mathrm{Fix}_T(g)) = \{t \in T \mid g * t = t\}$. *So* $\mathrm{Fix}_T(H)$ *is the set of fixed-points of H in T.*

(d) $g * T = \{g * t \mid t \in T\}$, $H * s = \{h * s \mid h \in H\}$, $H * T = \{h * t \mid h \in H, t \in T$

(e) $*$ is called a faithful action *of G on S if* $\mathrm{Stab}^*_G(S) = \{e\}$. *In this case we also say that S is a faithful G-set.*

*(f) T is called H-*invariant *with respect to $*$ if $h * T = T$ for all $h \in H$. T is called g-invariant if $g * T = T$.*

(g) $\mathrm{N}^*_H(T) = \{h \in H \mid hT = T\}$. $\mathrm{N}^*_H(T)$ *is called the* normalizer *of T in H with respect to $*$.*

(h) $H^{*S} = \{h^* \mid h \in H\}$. *Note that* $G^{*S} = \mathrm{Im} *_G$.

We will often just write $\mathrm{Stab}_H(S)$ in place of $\mathrm{Stab}^*_H(S)$, but of course only if its clear from the context what the underlying action $*$ is. We will also sometimes use H^S or H^* for H^{*S}.

Lemma 1.7.10. *(a)* $\mathrm{Stab}_G(S) = \ker *_G \trianglelefteq G$.

(b) $G/\mathrm{Stab}_G(S) \cong G^{*S} \leq \mathrm{Sym}(S)$.

(c) S is a faithful G-set if and only if Φ_* is 1-1. So if S is faithful, G is isomorphic to the subgroup G^{*S} of $\mathrm{Sym}(S)$.

(d) Let $H \leq G$ and T an H-invariant subset of S, $*$ is also an action of H on T.

(e) The map

$$*_{\mathcal{P}} : G \times \mathcal{P}(S) \to \mathcal{P}(S), (g, T) \to g * T$$

is an action of H on $\mathcal{P}(S)$.

(f) Let $T \subseteq S$. Then $\mathrm{Stab}_G(T)^{*S} = \mathrm{Stab}_{G^{*S}}(T)$.

(g) Let $s \in S$, then $\mathrm{Stab}_G(T)^{*S} = \mathrm{Stab}_{G^{*S}}(T)$.

Proof. (a) Let $g \in G$, then

$$\begin{aligned} & g \in \mathrm{Stab}_G(S) \\ \Longleftrightarrow\quad & gs = s \text{ for all } g \in G \\ \Longleftrightarrow\quad & g^*(s) = s \text{ for all } g \in G \\ \Longleftrightarrow\quad & g^* = \mathrm{id}_S \\ \Longleftrightarrow\quad & \Phi^*(g) = \mathrm{id}_S \\ \Longleftrightarrow\quad & g \in \ker \Phi^* \end{aligned}$$

(b) Since $G^* = \mathrm{Im}\,\Phi^*$, this follows from (a) and the First Isomorphism Theorem.
(c) - (e) are readily verified.
(f) Let $g \in G$ and $t \in T$ then $g * t = t$ if and only if $g^*(t) = t$. So (f) holds.
(g) follows from (f) applied with $T = \{s\}$. □

Lemma 1.7.11. *Let $*$ be an action of the group G on the set S. Let $H \subseteq G$, $T \subseteq S$, $g, h \in G$ and $s, t \in S$.*

(a) $g * s = g * t$ *if and only if* $s = t$.

(b) h *fixes* t *if and only if* ${}^g h$ *fixes* $g * t$.

(c) H *fixes* t *if and only if* ${}^g H$ *fixes* $g * t$.

(d) $\mathrm{Stab}_G(g * t) = {}^g\mathrm{Stab}_G(t)$.

(e) $\mathrm{Stab}_G(g * T) = {}^g\mathrm{Stab}_G(T)$.

(f) $\mathrm{Fix}_S({}^g H) = g * \mathrm{Fix}_S(H)$.

(g) $\mathrm{Fix}_S({}^g h) = g * \mathrm{Fix}_S(h)$.

Proof. (a) This holds since by 1.7.7(c), g^* is a bijection.
(b)

$$\begin{aligned} & {}^g h \text{ fixes } {}^g t \\ \Longleftrightarrow\quad & (ghg^{-1}) * (g * t) = g * t \\ \Longleftrightarrow\quad & ((ghg^{-1})g) * t = g * t \\ \Longleftrightarrow\quad & (gh) * t = g * \\ \Longleftrightarrow\quad & g * (h * t) = g * t \\ \Longleftrightarrow\quad & h * t = t \\ \Longleftrightarrow\quad & h \text{ fixes } t \end{aligned}$$

Since g^* is bijection for each $s \in S$ there exists a unique $t \in S$ with $s = g * t$. Thus the remaining statement now follow from (b). □

Lemma 1.7.12. *Let G be a group acting on the set S. Let $s \in S$ and $T \subseteq S$.*

(a) $\mathrm{Stab}_G(T)$ *is a subgroup of* G.

(b) $\mathrm{Stab}_G(s)$ *is a subgroup of* G.

(c) $\mathrm{N}_G(T)$ *is a subgroup of* G.

Proof. (a) $1t = t$ for all $t \in T$ and so $1 \in \mathrm{Stab}_G(T)$. Let $g, h \in \mathrm{Stab}_G(T)$. Then $gt = t$ and $ht = t$ for all $t \in T$. Thus

$$(gh)t \overset{\text{(GA2}}{=} g(ht) = gt = t$$

and so $gh \in \mathrm{Stab}_G(T)$.

From $gt = t$ we get $g^{-1}(gt) = g^{-1}t$. So by (GA2), $(g^{-1}g)t = g^{-1}t$ and $et = g^{-1}t$. Thus by (GA1), $t = g^{-1}t$. Hence $g^{-1} \in \mathrm{Stab}_G(T)$. 1.4.3 now implies that $\mathrm{Stab}_G(T)$ is a subgroup of G.

Note that $\mathrm{Stab}_G(s) = \mathrm{Stab}_G(\{s\})$. Thus (b) follows from (c).

(c) We have

$$\mathrm{N}^*_G(T) = \{g \in G \mid gT = T\} = \mathrm{Stab}^{*\mathcal{P}}_G(T).$$

(Note that on the left hand side T is treated as a subset of the G-set S, and in the right hand side, T is treated as an element of the G-set $\mathcal{P}(S)$.) Thus (c) follows from (b). □

Example 1.7.13. Consider the action c of a group G on itself. be conjugation and let $A \subseteq G$. Let $g \in G$. Then

$$\begin{aligned}
& g \in \mathrm{Stab}^{\mathrm{c}}_G(A) \\
\iff\quad & g\,\mathrm{c}\,a = a \text{ for all } a \in A \\
\iff\quad & {}^{g}a = a \text{ for all } a \in A \\
\iff\quad & gag^{-1} = a \text{ for all } a \in A \\
\iff\quad & ga = ag \text{ for all } a \in A
\end{aligned}$$

Define

$$\mathrm{C}_G(A) := \{g \in G \mid ga = ag \text{ for all } a \in A\}$$

Then we proved $\mathrm{C}_G(A) = \mathrm{Stab}^*(A)$ and so by 1.7.12(a), $\mathrm{C}_G(A) \le G$.

The center $\mathrm{Z}(G)$ if G is defined as

$$\{g \in G \mid ga = ga \text{ for all } a \in A\}$$

So

$$\mathrm{Z}(G) = \mathrm{C}_G(G) = \mathrm{Stab}^{\mathrm{c}}_G(G)$$

and so by 1.7.10(a)

$$\mathrm{Z}(G) \trianglelefteq G \quad \text{and } G/\mathrm{Z}(G) \cong G^{\mathrm{c}} \le \mathrm{Sym}(G)$$

Definition 1.7.14. *Let $* : G \times S \to S$ be a magma action.*

(a) $\sim_*$ is the equivalence relation on S generated by $\{(s, gs) \mid s \in S, g \in G\}$.

(b) The equivalence classes of $\sim_*$ are called the orbits *of G on S with respect to $*$.*

(c) The set of orbits of G on S is denoted by $S/^*G$.

(d) We say that G acts transitive*ly on S if G has exactly one orbit on S.*

Lemma 1.7.15. *Let $*$ be an magma-action of the non-empty magma G on the set S. Let $s, t \in S$.*

(a) Suppose $*$ is a group-action. Then

$$s \sim_* t \qquad \Longleftrightarrow \qquad gs = t \text{ for some } g \in G$$

(b) Suppose G is abelian. Then

$$s \sim_* t \qquad \Longleftrightarrow \qquad gs = ht \text{ for some } g, h \in G$$

Proof. Le $\sim$ be the relation $\{(s, gs) \mid s \in S, g \in G\}$ on G. By definition $\sim_*$ is the equivalence relation generated by $\sim$.

(a) Suppose $*$ is a group action. We just need need to show that $\sim$ is an equivalence relation.

Since $s = es$, $s \sim s$ and $\sim$ is reflexive.

If $t = as$, then

$$a^{-1}t = a^{-1}(as) = (a^{-1}a)s = es = s$$

Thus $s \sim t$ implies $t \sim s$ and $\sim$ is symmetric.

Finally if $s = at$ and $t = br$ then $s = at = a(br) = (ab)r$. Thus $s \sim t$ and $t \sim r$ implies $s \sim r$ and $\sim$ is reflexive.

(b) Define the relation $\approx$ on S by

$$s \approx t \qquad \text{if} \qquad gs = ht \text{ for some } g, h \in G$$

Suppose $gs = ht$ for some $g, h \in G$. Since $s \sim gs$ and $t \sim ht = gs$ we conclude that $s \sim_* t$ and so $\approx \subseteq \sim_*$. So we just need to show $\approx$ is an equivalence relation. Let $s \in S$. Since G is not-empty there exists $g \in G$ and so $gs = gs$ and $s \approx s$. $\approx$ is clearly symmetric. Suppose that $r, s, t \in G$ with $r \approx s$ and $s \approx t$. Then $gr = hs$ and $ks = lt$ for some $g, h, k, l \in H$. Thus

$$(kg)r = k(gr) = k(hs) = (kh)s = (hk)s = h(ks) = h(lt) = (hl)t$$

and so $r \approx t$.

□

Lemma 1.7.16. *Let G be a group acting on the non-empty set S. Let $s \in S$. Then the orbit of G on S containing s is $Gs = \{gs \mid g \in G\}$.*

Proof. Let O be the orbit of G on T containing s and let $t \in S$. Then

$$\begin{array}{cc} & t \in O \\ \Longleftrightarrow & t \sim_* s \\ \Longleftrightarrow & t = gs \text{ for some } g \in G \\ \Longleftrightarrow & t \in Gs \end{array}$$

□

Lemma 1.7.17. *Let G be a group acting on the non-empty set S. Then following are equivalent:*

(a) For each $s, t \in S$ there exists $g \in G$ with $t = gs$.

(b) There exists $s \in S$ with $S = Gs$.

(c) S is an orbit for G on S.

(d) G acts transitively on S.

Proof. (a) $\Longrightarrow$ (b): Suppose (a) holds. Since S is not empty there exists $s \in S$. Let $t \in T$. By (a) there exists $g \in G$ with $t = gs$. So $t \in Gs$ and $S = Gs$.

(b) $\Longrightarrow$ (c): By 1.7.16 Gs is an orbit for G on S. So if $S = Gs$, S is an orbit for G on S.

(c) $\Longrightarrow$ (d): Suppose S is an orbit for G on S. Since distinct orbits are disjoint we conclude that S is the only orbit for G on S. Thus G acts transitively on S.

(d) $\Longrightarrow$ (a): Suppose that G acts transitively on S and let $s, t \in G$. By 1.7.16 Gs is an orbit for G in S and since G acts transitively, Gs is the only orbit. Since t lies is some orbit, this means that $t \in Gs$ and so $t = gs$ for some $g \in G$. □

Example 1.7.18. Let G be group and $H \leq G$.

1. The right cosets of H are the orbits for the action of H on G by left multiplication. So H acts transitively on G by left multiplication if and only if H is the only coset of H in G and so if and only if $G = H$.

2. The left cosets of H are the orbits for the action of H on G by the right multiplication. (Note here that since $H = H^{-1}$, $gH^{-1} = gH$.) Again this action is transitive if and only if $G = H$.

3. The orbit of G on G containing h with respect to the action by conjugation id ${}^{G}h = \{cgh \mid g \in H\}$. This orbit is called the conjugacy class of G containing h. Note that ${}^{G}e = \{e\}$ and so the action by conjugation is transitive if and only if $G = \{e\}$.

4. Let I be a non-empty set. Then $\mathrm{Sym}(I)$ acts transitively on I.

5.
$$*_{G/H} : G \times G/H \to G/H, (g,T) \to gT$$

is a well -defined transitive action of G on G/H.

Indeed, if $T = tH$, then $g(tH) = (gT) \in G/H$. So $*_{G/H}$ is well-defined. Its straightforward to verify that $*_{G/H}$ is indeed an action. Also

$$G *_{G/H} H = \{gH \mid g \in G\} = G/H,$$

and so G acts transitively on G/H. This action is called the action of G on G/H by left multiplication.

We will show that any transitive action of G is isomorphic to the action on the coset of a suitable subgroup. But first we need to define isomorphism for G-sets.

Definition 1.7.19. *Let G be a group, $*$ an action of G on the set S, $\triangle$ an action of G on the set T and $\alpha : S \to T$ a function.*

*(a) α is called G-*equivariant* with respect to $*$ and $\triangle$ if*

$$\alpha(g * s) = g \triangle \alpha(s)$$

for all $g \in G$ and $s \in S$.

*(b) α is called a G-*isomorphism* from $(S, *)$ to $(T, \triangle)$ if α is a bijection and α is G-equivariant with respect to $*$ and $\triangle$.*

(c) We say that $(S, *)$ and $(T, \triangle)$ are G-isomorphic and write

$$(S, *) \cong (T, \triangle), \qquad \text{or } S \cong_G T$$

*if there exists a G-*isomorphism* from $(S, *)$ to $(T, \triangle)$.*

Lemma 1.7.20. *Let S be a G-set, $s \in S$ and put $H = \mathrm{Stab}_G(s)$.*

(a) The map
$$\alpha : G/H \to S, \; aH \to as$$

is well defined, G-equivariant and one 1-1

(b) α is an G-isomorphism if and only if G acts transitively on S

(c) $|Gs| = |G/\mathrm{Stab}_G(s)|$.

Proof. (a) Let $a, b \in G$. Then

$$\begin{aligned}
& aH = bH \\
\Longleftrightarrow\quad & a^{-1}b \in H \\
\Longleftrightarrow\quad & a^{-1}b \in \mathrm{Stab}_G(s) \\
\Longleftrightarrow\quad & (a^{-1}b)s = s \\
\Longleftrightarrow\quad & a\big((a^{-1}b)s\big) = as \\
\Longleftrightarrow\quad & bs = as
\end{aligned}$$

The forward direct shows that α is well-defined and the backward direction shows that α is 1-1. Also

$$\alpha(a(bH)) = \alpha((ab)H) = (ab)s = a(bs) = a\alpha(bH)$$

So α is G-equivariant.

(b) By (a) α is a G-isomorphism if and only if α is onto. We have

$$\operatorname{Im}\alpha = \{\alpha(gH) \mid g \in G\} = \{gs \mid g \in G\} = Gs$$

So α is onto if and only if $S = Gs$ and so if and only if G is transitive on S.

(c) Since α is 1-1, $|G/H| = |\operatorname{Im}\alpha| = |Gs|$. □

Lemma 1.7.21. *Suppose that G acts transitively on the sets S and T. Let $s \in S$ and $t \in T$. Then S and T are G-isomorphic if only if* $\mathrm{Stab}_G(s)$ *and* $\mathrm{Stab}_G(t)$ *are conjugate in G.*

Proof. Suppose first that $\alpha : S \to T$ is a G-isomorphism. Let $g \in G$. Since α is 1-1 and G-equivariant:

$$gs = s \Longleftrightarrow \alpha(gs) = \alpha(s) \Longleftrightarrow g\alpha(s) = \alpha(s)$$

So $\mathrm{Stab}_G(s) = \mathrm{Stab}_G(\alpha(s))$. Since G is transitive on T, there exists $g \in G$ with $g\alpha(s) = t$. Thus

$$\mathrm{Stab}_G(t) = \mathrm{Stab}_G(g\alpha(s)) = {}^g\mathrm{Stab}_G(\alpha(s)) = {}^g\mathrm{Stab}_G(s).$$

Conversely suppose that ${}^g\mathrm{Stab}_G(s) = \mathrm{Stab}_G(t)$ for some $g \in G$. Then $\mathrm{Stab}_G(gs) = {}^g\mathrm{Stab}_G(s) = \mathrm{Stab}_G(t)$ and so by 1.7.20(b) applied to S and to T:

$$S \cong_G G/\mathrm{Stab}_G(gs) = G/\mathrm{Stab}_G(t) \cong_G T.$$

□

Definition 1.7.22. *Let G be a group and S a G-set. A subset $R \subseteq S$ is called a set of* representatives *for the orbits of G on S, provided that R contains exactly one element from each G-orbit. In other words if the map $R \to S/G, r \to Gr$ is a bijection.*

An orbit O of G on S is called trivial *if* $|O| = 1$.

Let R be an set of representatives for the orbits of G on S and any trivial orbit $\{s\}$. Then s must be in R. Thus $\mathrm{Fix}_S(G) \subseteq R$ and $R \smallsetminus \mathrm{Fix}_G(R)$ is a set of representatives for the non-trivial G-orbits.

Proposition 1.7.23 (Orbit Equation)**.** *Let G be a group acting on the set S and let $R \subseteq S$ be a set of representatives for S/G. Then*

$$|S| = \sum_{r\in R} |G/\mathrm{Stab}_G(r)| = |\mathrm{Fix}_S(G)| + \sum_{r\in R\smallsetminus \mathrm{Fix}_S(G)} |G/\mathrm{Stab}_G(r)|.$$

Proof. Since the orbits are the equivalemce classes of an equivalence relation S is the disjoint union of its orbit. Thus

$$|S| = \sum_{O\in S/G} |O| = \sum_{r\in R} |Gr|$$

By 1.7.20d, $|Gr| = |G/\mathrm{Stab}_G(r)|$ and so

$$|S| = \sum_{r\in R} |G/\mathrm{Stab}_G(r)|$$

Also

$$S = \sum_{r\in \mathrm{Fix}_S(G)} |Gr| + \sum_{r\in R\smallsetminus \mathrm{Fix}_S(G)} |Gr| = |\mathrm{Fix}_S(G)| + \sum_{r\in R\smallsetminus \mathrm{Fix}_S(G)} |G/\mathrm{Stab}_G(r)|$$

□

Corollary 1.7.24 (Class Equation)**.** *Let G be a group and R be a set of representatives for the conjugacy classes of G. Then*

$$G = \sum_{r\in R} |G/\,\mathrm{C}_G(r)| = |\mathrm{Z}(G))| + \sum_{r\in R\smallsetminus \mathrm{Z}(G)} |G/\,\mathrm{C}_G(r)|$$

Proof. Let c be the action of G on G be conjugation. Then

$$\mathrm{Fix}^{\mathrm{c}}_G(G) = \{g \in G \mid {}^h g = g \text{ for all } h \in G\} = \{g \in G \mid hg = gh \text{ for all } h \in G\} = \mathrm{Z}(G)$$

and by 1.7.13 $\mathrm{Stab}^{\mathrm{c}}_G(a) = \mathrm{C}_G(a)$. So the Class Equation follows from the orbit equation. □

To illustrate the class equation we will determine the conjugacy classes in $\mathrm{Sym}(n)$.

Definition 1.7.25. *Let $\pi \in \mathrm{Sym}(n)$. For $i \in \mathbb{Z}^+$ let λ_i be the number of cycle of length i of π. Then the* cycle type *of π to be sequence $(\lambda_i)_{i=1}^{\infty}$. Alternatively we will write the cycle type as $1^{\lambda_1}2^{\lambda_2}3^{\lambda_3}\dots$ and often will not list terms i^{λ_i} for which $\lambda_i = 0$.*

For example the cycle type of

$$(1,7,3)(2,6)(4)(5,8,10)(9,13,16)(11)(14,15)(16,17)$$

in $\mathrm{Sym}(17)$ is $(2,3,3,0,0,\dots) = 1^2 2^3 3^3$.

Proposition 1.7.26. *(a) Let $\mu, \pi \in \mathrm{Sym}(n)$ and suppose that μ has cycle notation*

$$(a_{11}, a_{12}, \dots, a_{1k_1})(a_{21}, a_{22}, \dots, a_{2k_2}) \dots (a_{l1}, a_{l2}, \dots, a_{lk_l})$$

Then the cycle notation for ${}^{\pi}\mu$ is

$$(\pi(a_{11}), \pi(a_{12}), \dots, \pi(a_{1k_1}))(\pi(a_{21}), \pi(a_{22}), \dots, \pi(a_{2k_2})) \dots (\pi(a_{l1}), \pi(a_{l2}), \dots \pi(a_{lk_l}))$$

(b) Two elements in $\mathrm{Sym}(n)$ are conjugate if and only if they have the same cycle type.

Proof. (a) We have

$$\big({}^{\pi}\mu\big)\big(\pi(a_{ij})\big) = \big(\pi \circ \mu \circ \pi^{-1}\big)\big(\pi(a_{ij})\big) = \pi(\mu(a_{ij})) = \begin{cases} \pi((a_{i,j+1})) & \text{if} j \neq k_i \\ \pi(a_{i,1}) & \text{if} j = k_i \end{cases}$$

So (a) holds.

(b) By (a) μ and ${}^{\pi}\mu$ have the same cycle type. Conversely suppose that μ and σ in $\mathrm{Sym}(n)$ have the same cycle type. Then σ has cycle notation

$$\sigma = (b_{11}, b_{12}, \dots b_{1k_1})(b_{21}, b_{22}, \dots b_{2k_2}) \dots (b_{l1}, b_{l2}, \dots b_{lk_l})$$

Note that for each $1 \leq k \leq n$ there exist unique i, j with $k = a_{i,j}$ and unique s, t with $k = b_{s,t}$. So we can define $\pi \in \mathrm{Sym}(n)$ by $\pi(a_{ij}) = b_{ij}$. Then by (a) ${}^{\pi}\mu = \sigma$ and so elements of the same cycle type are conjugate. □

Example 1.7.27. 1. ${}^{(1,3,5)(2,7)}(1,4,3)(2,6,7)(5,8) = (3,4,5)(7,6,2)(1,8)$

2. Let $\mu = (1,3)(2)(4,7)(5,6,8)$ and $\sigma = (3,5)(8)(1,7)(2,4,6)$

Define $\pi \in \mathrm{Sym}(8)$ by

$$\pi(1) = 3, \pi(3) = 5, \pi(2) = 8, \pi(4) = 1, \pi(7) = 7, \pi(5) = 2, \pi(6) = 4 \text{ and } \pi(8) = 6$$

Then ${}^{\pi}\mu = \sigma$.

Example 1.7.28. By 1.7.26 has three conjugacy classes corresponding to the cyles types 1^3, $1^1 2^1$ and 3^1. So $R = \{(1), (13), (123)\}$ is a set of representatives for the conjugacy class of $\mathrm{Sym}(3)$. A straight forward calculation shows that

$$\mathrm{C}_{\mathrm{Sym}(3)}((1)) = \mathrm{Sym}(3), \quad \mathrm{C}_{\mathrm{Sym}(3)}((13)) = \{(1), (13)\}, \quad C_{\mathrm{Sym}(3)}((123)) = \{(1), (123), (132)\}$$

The orders of these centralizers are

$$6, 2, 3.$$

$\mathrm{Sym}(3)$ has order 6 and since $|G/C_G(r)| = \frac{|G|}{|C_G(r)|}$ the class equation now says

$$6 = \frac{6}{6} + \frac{6}{2} + \frac{6}{3} = 1 + 2 + 3$$

Example 1.7.29. *The conjugacy classes of* $\mathrm{Sym}(4)$ *are:*

Cycle type	*elements*	*number of elements*
1^4	(1)	1
$1^2 2^1$	$(12), (13), (14), (23), (24), (34)$	6
$1^1 3^1$	$(123), (132), (124), (142), (134), (143), (234), (243)$	8
2^2	$(12)(34), (13)(24), (14)(23)$	3
4^1	$(1234), (1243), (1324), (1342), (1423), (1432)$	6

A set of representatives for the conjugacy classes

$$\{(1), (12), (123), (12)(34, (1234)\}$$

and their centralizers:

r	$C_{\mathrm{Sym}(4)}(r)$	$\lvert C_{\mathrm{Sym}(4)}(r)\rvert$
(1)	$\mathrm{Sym}(4)$	24
(12)	$(1), (12), (34), (12)(34)$	4
(123)	$(1)(123), (132)$	3
$(12)(34)$	$(1), (12), (34), (12)(34), (1324), (13)(24), (1423), (14)(23)$	8
(1234)	$(1), (1234), (13)(24), (1432))$	4

So the orbit equation says

$$24 = \frac{24}{24} + \frac{24}{4} + \frac{24}{3} + \frac{24}{8} + \frac{24}{4}$$

and so

$$24 = 1 + 6 + 8 + 3 + 6$$

The Orbit Equations become particular powerful if G is a finite *p-group*:

Definition 1.7.30. *Let G be finite group and p a prime. Then G is called a* p-group *provided that that is* $|G| = p^k$ *for some* $k \in \mathbb{N}$.

Proposition 1.7.31 (Fixed-Point Equation)**.** *Let p be a prime and P a p-group acting on a finite set* S. *Then*

$$|S| \equiv |\mathrm{Fix}_S(P)| \pmod{p}.$$

Proof. Let R be a set of representatives for S/P and let $r \in R \setminus \mathrm{Fix}_S(P)$. Then $\mathrm{Stab}_P(r) \nleq P$. By Lagrange's Theorem $|P/\mathrm{Stab}_P(r)|$ divides $|P|$. Since $|P|$ is a power of p and $|P/\mathrm{Stab}_P(r)| \neq 1$ we get

$$|P/\mathrm{Stab}_P(r)| \equiv 0 \pmod{p}.$$

So by the Orbit Equation 1.7.23

$$|S| = |\mathrm{Fix}_S(P)| + \sum_{r \in R \setminus \mathrm{Fix}_S(P)} |P/\mathrm{Stab}_P(r)| \equiv |\mathrm{Fix}_S(P)| \pmod{p}$$

□

Corollary 1.7.32. *Let P be a prime and P a finite p-group acting on finite set S.*

(a) If p does not divide S, then $\mathrm{Fix}_S(P) \neq \varnothing$.

(b) If p divides $|S|$ and P has at least one fixed-point on S, than P has more than one fixed point on S.

Proof. This follows immediately from $|S| \equiv \mathrm{Fix}_S(P) \pmod{p}$. □

Example 1.7.33. Let G be a finite group and let $H = \{e, h\}$ be any group of order 2. Define an action of H on the set G by

$$e * g = g \quad h * g = g^{-1}$$

Since $h * (h * g) = (g^{-1})^{-1} = g = e * g$, this is indeed an action. Note that

$$\mathrm{Fix}_G(H) = \{g \in G \mid g = g^{-1}\} = \{g \in G \mid g^2 = 1_G\}$$

Let t be the number of elements of order 2 in G. Then $|\mathrm{Fix}_G(H)| = t + 1$. By the Fixed-Point Equation

$$|\mathrm{Fix}_G(H)| \equiv |G| \pmod{2}$$

and so

$$t \not\equiv |G| \pmod{2}$$

So a group of even order has an odd number of elements of order 2. In particular it has an element of order 2.

Example 1.7.34. Let $\mathcal{E} = (\mathcal{P}, \mathcal{L}, \mathcal{R})$ be a projective plane of order. and T a 2-subgroup of $\mathrm{Aut}(\mathcal{E})$.

Since the number of points is odd, 1.7.32 implies that T fixes a point P. Let $\mathcal{A}$ be the set of lines incident with P. Since T fixes P, T acts on $\mathcal{A}$. Since $|\mathcal{A}| = 3$ is odd we conclude that $\mathrm{Fix}_{\mathcal{A}}(T) \neq \varnothing$. Hence T fixes a line l incident with P. Thus

$$T \leq \mathrm{Stab}_{\mathrm{Aut}(\mathcal{E})}(\{P, l\})$$

By Homework 2#6 $\mathrm{Stab}_{\mathrm{Aut}(\mathcal{E})}(\{P, l\})$ has order eight, and so is a 2-group. We conclude that the 2-subgroups of $\mathrm{Aut}(\mathcal{E})$ are exactly the subgroups fixing a point and a line, which are incident.

By definition of $\mathrm{Aut}(\mathcal{E})$, if $(P, l) \in \mathcal{R}$ and $\alpha \in \mathrm{Aut}(\mathcal{E})$, the $(\alpha(P), \alpha(l) \in \mathcal{R}$. So $\mathrm{Aut}(\mathcal{E})$ acts on $\mathcal{R}$. Let $(P, L) \in \mathcal{R}$. Let O be the orbit of $\mathrm{Aut}(\mathcal{E})$ on $\mathcal{R}$ containing (P, l). Then

$$|O| = |\mathrm{Aut}(\mathcal{E})/\mathrm{Stab}_{\mathrm{Aut}(\mathcal{E})}((P, l))| = \frac{168}{8} = 21.$$

On the otherhand, $\mathcal{E}$ has seven lines and each line is incident with 3 points and so $|\mathcal{R}| = 21$. Hence $O = \mathcal{R}$ and $\mathrm{Aut}(\mathcal{E})$ acts tranistively on $\mathcal{R}$.

Definition 1.7.35. *Let G be a group and $H \subseteq G$. Then*

$$\mathrm{N}_G(H) = \mathrm{N}^{\mathrm{c}}(H) = \{g \in G \mid {}^gH = H\}$$

$\mathrm{WN}_G(H) = \{a \in G \mid H \subseteq {}^aH\}$. $\mathrm{N}_G(H)$ *is called the normalizer of H in G and* $\mathrm{WN}_G(H)$ *the weak normalizer of H in G.*

Lemma 1.7.36. *Let G be a group and H a finite subset of G. Then* $\mathrm{N}_G(H) = \mathrm{WN}_G(H)$.

Proof. Let $g \in G$. As conjugation is an bijection, $|H| = |{}^gH|$. So for finite H, $H \subseteq {}^gH$ if and only if $H = {}^gH$. □

Lemma 1.7.37. *Let G be a group, $H \leq G$ and $a \in G$. With respect to the action of G on G/H be left multiplication:*

$$\mathrm{Stab}_G(aH) = {}^aH \quad \textit{and} \quad \mathrm{Fix}_{G/H}(H) = \mathrm{WN}_G(H)/H.$$

Proof. Let $g \in G$. Then $gH = H$ if and only if $g \in H$. Hence $\mathrm{Stab}^*_G(H) = H$ and so by 1.7.11(d)

$$\mathrm{Stab}_G(aH) = {}^a\mathrm{Stab}^*_G(H) = {}^aH.$$

Note that H fixes aH if and only if $H \subseteq \mathrm{Stab}^*_G(aH)$. That is if and only if $H \leq {}^aH$ and if and only if $a \in \mathrm{WN}_G(H)$. So also the second statement holds. □

Lemma 1.7.38. *Let P be a non-trivial finite p-group.*

(a) $\mathrm{Z}(P)$ *is non-trivial.*

(b) If $H \not\trianglelefteq P$ then $H \not\trianglelefteq \mathrm{N}_P(H)$.

Proof. (a) Consider first the action of P on P by conjugation. Then $\mathrm{Fix}_P(P) =$
$opZ(P)$ and by1.7.31

$$0 \equiv |P| \equiv |\mathrm{Z}(P)| \pmod{p}..$$

Thus $|\mathrm{Z}(P)| \neq 1$.

(b) Consider the action of H on P/H be left multiplication. By 1.7.37, 1.7.31 and 1.7.36

$$0 \equiv |P/H| \equiv |\mathrm{Fix}_{P/H}(H)| = |\mathrm{N}^*_P(H)/H)| = |\mathrm{N}_P(H)/H \pmod{p}.$$

So $|\mathrm{N}_P(H)/H| \neq 1$. □

Lemma 1.7.39. *Let p be a prime and P a p-group.*

(a) Let $H \leq P$. Then there exists $n \in \mathbb{N}$ and for $0 \leq i \leq n$, $H_i \leq P$ with

$$H = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = P$$

and $|H_i/H_{i-1}| = p$ for all $1 \leq i \leq n$.

(b) Let m be a divisor of $|P|$. Then P has a subgroup of order m.

Proof. (a) The proof is by induction on $|P/H|$. If $|P/H| = 1$, then $P = H$ and (a) holds with $n = 0$ and $H_0 = H = P$. So suppose $H \neq P$. The by 1.7.38(b), $H \lneq \mathrm{N}_P(H)$. Hence there exits $e \neq x \in \mathrm{N}_P(H)/H$. Let $|x| = p^l$ and put $y = x^{p^{l-1}}$. Then $|y| = p$. By the Correspondence Theorem (Homework 4#1), there exists $H_1 \leq N_G(H)$ with $H_1/H = \langle y \rangle /$ Then $H \trianglelefteq H_1$ and $|H_1/H| = |\langle y \rangle| = |y| = p$. Since $|P/H_1| < |P/H|$ (a) now follwos by induction.

(b) Apply (a) with $H = \{e\}$. Then $|H_i| = p^i$ and (b) holds. □

As a further example how actions an set can be used we give a second proof that $\mathrm{Sym}(n)$ has normal subgroup of index two. For this we first establish the following lemma.

Lemma 1.7.40. *Let Δ be a finite set and $\sim$ a equivalence relation on Δ such that each equivalence class has size at most 2. Put*

$$\Omega = \{R \subseteq \Delta \mid R \text{ contains exactly one element from each equivalence class of} \sim\}.$$

Define the relation $\approx$ on Ω by $R \approx S$ if and only if $|R \setminus S|$ is even. Then $\approx$ is an equivalence relation. If $\sim$ is not the equality relation, $\approx$ has exactly two equivalence classes.

Proof. For $d \in \Delta$ let $\tilde{d}$ be the equivalence class of $\sim$ containing d and let $\tilde{\Delta}$ be the set of equivalence classes. For $A \in \Omega$ and $X \in \tilde{\Delta}$, let X_A be the unique element of X contained in A. $A, B \in \Omega$ and define

$$\tilde{\Delta}_{AB} = \{X \in \tilde{\Delta} \mid X_A \neq X_B\}.$$

Let $d \in A$. Then $d = \tilde{d}_A$ and $d \in B$ if and only if $d = \tilde{d}_B$. Hence $\tilde{d}_A = \tilde{d}_B$ if and only if $d \in B$. Thus

$$(*) \qquad \tilde{d} \in \tilde{\Delta}_{AB} \Longleftrightarrow \tilde{d}_A \neq \tilde{d}_B \Longleftrightarrow d \in B$$

By definition of Ω, the map

$$A \setminus \Delta d \to \tilde{d}$$

is a bijection. By (*) the image of $A \setminus B$ under this map is Δ_{AB}. Thus $|A \setminus B| = |\tilde{\Delta}_{AB}|$ and so

$$A \approx B \Longleftrightarrow \tilde{\Delta}_{AB} \text{ is even.}$$

Observe that $\tilde{\Delta}_{AB} = \tilde{\Delta}_{BA}$ and so $\approx$ is symmetric. Since $|A \setminus A| = 0$ is even, $\approx$ is reflexive.

Let $R, S, T \in \Omega$ and $X \in \tilde{\Delta}$. If $X_R \neq X_S$, then $X = \{X_R, X_S\}$ and so X_T is either equal to X_R or to X_S, but not both. Hence $X_R \neq X_S$ exactly if $X_R = X_T \neq X_S$ or $X_R \neq X_T = X_S$. Hence

Thus

$$\tilde{\Delta}_{RT} = (\tilde{\Delta}_{RS} \setminus \tilde{\Delta}_{ST}) \cup (\tilde{\Delta}_{ST} \setminus \tilde{\Delta}_{RS})$$

and so

$$(*) \qquad |\tilde{\Delta}_{RT}| = |\tilde{\Delta}_{RS}| + |\tilde{\Delta}_{ST}| - 2|\tilde{\Delta}_{RS} \cap \tilde{\Delta}_{ST}|.$$

If $R \approx S$ and $S \approx T$, the right side of $(*)$ is an even number. So also the left side is even and $R \approx T$. Thus $\approx$ is transitive and so an equivalence relation.

Suppose now that $\sim$ is not the equality relation. Then there exists $r, t \in \Delta$ with $r \sim t$ and $r \neq t$. Let $R \in \Omega$ with $r \in R$. Put $T = (R \cup \{t\}) \setminus \{r\}$. Then $T \in \Omega$ and $|T \setminus R| = 1$. Thus R and T are not related under $\approx$. Let $S \in \Omega$. Then the left side of $(*)$ is odd and so exactly one of $|\tilde{\Delta}_{RS}|$ and $|\tilde{\Delta}_{ST}|$ is even. Hence $S \approx R$ or $S \approx T$. Thus $\approx$ has exactly two equivalence classes and all the parts of the lemma are proved. □

Definition 1.7.41. *Let G be a magma acting on the set I and $\sim$ and $\approx$ relation on I. Then $(\sim, \approx)$ is called G-invariant if for all $g \in G, a, b \in I$:*

$$a \sim b \qquad \Longrightarrow \qquad ga \approx gb$$

$\sim$ is called G-invariant if $(\sim, \sim)$ is G-invariant.

Note that $(\sim, \approx)$ is G-invariant s if and only if $(\sim, \approx)$ is g^* invariant for all $g \in G$, where $g^* : I \to I, i \to gi$.

Lemma 1.7.42. *Let $*$ be an action if the magma G on the set I, $\sim$ a relation on I and $\approx$ the equivalence relation generated by $\sim$. Suppose that $\sim$ or $(\sim, \approx)$ is G-invariant. Then*

$$*/\approx\colon\ G \times I/\approx \to I/\approx, \quad \big(g, [a]_\approx\big) \to [ga]_\approx$$

is a well-defined action of G in $I/\approx$.

Proof. If $\sim$ is G-invariant also $(\sim, \approx)$ is G-invariant. So we may assume that $(\sim, \approx)$ is H-invariant. Let $g \in G$. Then $(\sim, \approx)$ is g^*-invariant. Thus by 1.5.5(a) also $(\approx, \approx)$ is g^*-invariant and so by 1.5.7(b) the function

$$I/\approx \to I/\approx, \quad [a]_\approx \to [ga]_\approx$$

is well-defined. Hence also $*/! \approx$ is well-defined. Let $g, h \in G$ and $a \in I$. Then n

$$(gh)[a]_\approx = [(gh)a]_\approx = [g(ha)]_\approx = g[ha]_\approx = g\big(h[a]_\approx\big)$$

and so $*/\approx$ is a magma action. □

Proposition 1.7.43. *Let $n \geq 2$ be an integer. Define*

$$\Delta = \{(i,j) \mid 1 \leq i,j \leq n, i \neq j\}$$

Define the relation $\sim$ on Δ by

$$(i,j) \sim (k,l) \textit{ if } (k,l) = (i,j) \textit{ or } (k,l) = (j,i)$$

Then $\sim$ is an equivalence relation on Δ such that each equivalence classes has size 2. Define

$$\Omega = \{R \subseteq \Omega \mid |R \cap X| = 1 \textit{ for all } X \in \Delta/\sim\}$$

Define the relation $\approx$ on

$$A \approx B \textit{ if } |A \smallsetminus B| \textit{ is even}$$

Then $\approx$ is an equivalence relation on Ω with exactly two equivalence classes. Moreover,

(a) $\mathrm{Sym}(n)$ *acts on Δ, $\Delta/\sim$, Ω and $\Omega/\approx$.*

(b) Define $\mathrm{Alt}(n) = \mathrm{Stab}_{\mathrm{Sym}(n)}(\Omega/\approx)$. *and let $\pi \in \mathrm{Sym}(n)$. Then $\pi \in \mathrm{Alt}(n)$ if and only if the set*

$$\{(i,j) \mid 1 \leq i < j \leq n, \pi(i) > \pi(j)\}$$

has even size.

(c) $(1,2) \notin \mathrm{Alt}(n)$.

(d) $\mathrm{Alt}(n)$ *is a normal subgroup of index two in* $\mathrm{Sym}(n)$.

Proof. (a) Let $\pi \in \mathrm{Sym}(n)$ and $(i,j) \in \Delta$, then $\pi(i) \neq \pi(j)$ and so $\pi(i) \neq \pi(j)$. Thus Δ is a $\mathrm{Sym}(n)$-invariant subset of $S \times S$ and so $\mathrm{Sym}(n)$ act on Δ. If $(i,j) = (k,l)$ or $(i,j) = (l,k)$, then then also $(\pi(i),\pi(j)) = (\pi(k),\pi(l))$ or $((\pi(i),\pi(j)) = (\pi(l),\pi(k))$. So $\sim$ is $\mathrm{Sym}(n)$-invariant and $\mathrm{Sym}(n)$ acts on $\Delta/\sim$.

Let $R \in \Omega$ and $X \in \Delta/\sim$. Then $Y = \pi^{-1}(X) \in \Delta/\sim$ and so

$$|\pi R \cap X| = |\pi R \cap \pi Y| = |\pi(R \cap Y)| = |R \cap Y| = 1$$

So $\pi(R) \in \Omega$ and $\mathrm{Sym}(n)$ acts on Ω. If $A, B \in \Omega$ with $A \approx B$, then $|\pi(A) \smallsetminus \pi(B)| = |\pi(A \smallsetminus B| = |A \smallsetminus B|$ is even and so $\pi A \approx \pi B$. Thus $\approx$ is $\mathrm{Sym}(n)$-invariant and so $\mathrm{Sym}(n)$ acts $\Omega/\approx$.

(b) Put $R = \{(i,j)\ 1 \leq i < j \leq n\}$ and observe that $R \in \Omega$. If $\pi(R) \approx R$, then π fixes $[R]_\approx$ and since $\approx$ has only two equivalence classes, π also has to fix the other class. Hence $\pi \in \mathrm{Alt}(n)$. If $\pi(R) \not\approx R$, then π does not fix $[R]_\approx$ and so $\pi \notin \mathrm{Alt}(n)$. Thus

$$\pi \in \mathrm{Alt}(n) \iff |\pi R \smallsetminus R| \text{ is even}$$

We have

$$|\pi R \setminus R| = |\{\pi r \mid r \in R, \pi r \notin R\}| = |\{r \mid r \in R, \mid \pi r \notin R\}| = |\{(i,j) \mid 1 \le i < j \le n, \pi(i) > \pi(j)\}|$$

and so (b) holds.

(c) Let $1 \le i < j \le n$. If $i > 2$, then $(1,2)(i) = i < j = (1,2)(j)$. If $i = 2$, then $(1,2)i = 1 < j = (1,2)(j)$. If $i = 1$ and $j > 2$, then $(1,2)(i) = 2 < j = (1,2)j$. If $i = 1$ and $j = 2$, then $(1,2)(i) = 2 > 1 = (1,2)2$. So $(1,2)(i) > (1,2)(j)$ if and only if $(i,j) = (1,2)$. So by (b), $(1,2) \notin \mathrm{Alt}(n)$.

(d) By 1.7.10

$$\mathrm{Alt}(n) = \mathrm{Stab}_{\mathrm{Sym}(n)}(\Omega/\approx) \trianglelefteq \mathrm{Sym}(n) \text{ and } \mathrm{Sym}(n)/\mathrm{Alt}(n) \cong \mathrm{Sym}(n)^{\Omega/\approx} \le \mathrm{Sym}(\Omega/\approx)$$

Since $|\Omega/\approx|= 2$ also $|\mathrm{Sym}(\Omega/\approx)| = 2$. Thus $|\mathrm{Sym}(n)/\mathrm{Alt}(n)| \le 2$. By (c), $(1,2) \notin \mathrm{Alt}(n)$. So $\mathrm{Sym}(n) \ne \mathrm{Alt}(n)$ and $|\mathrm{Sym}(n)/\mathrm{Alt}(n)| = 2$. □

Example 1.7.44. The goal of this example is to find a subgroup of $\mathrm{Sym}(6)$ whihc is isomorphic to $\mathrm{Sym}(5)$ but acts tranistively on $\{1,\dots,6\}$. For this let J be the set of subgroups of order five in $\mathrm{Sym}(5)$. Let $F \in J$ and $(1) \ne f \in F$. Then $|f|$ divides $\mathbb{F}| = 5$ and so $|f| = 5$, $F = \langle f \rangle$ and any f is a five cycle. So $f = (abcde)$ for some pairwise a,b,c,d,e. Since thare are 5! choices for a,b,c,d,e but $(abcde) = (bcdea)\dots(eabcbde)$ there are $\frac{5!}{5} == 24$ 5-cycle in $\mathrm{Sym}(4)$. Each $F \in J$ contains four 5-cycles and $F_1 \cap F_2 = \{(1)\}$ for $F_1 \ne F_2 \in J$. Thus $|J| = \frac{24}{4} = 6$. For $i = 1,2$ let Let $F_i \in J$ and $(1) \ne f_i\mathbb{F}$. By 1.7.26(b), $f_2 = {}^g f_1$ for some $g \in \mathrm{Sym}(5)$. Thus

$${}^g F_1 = {}^g\langle f_1 \rangle = \langle {}^g f_1 \rangle = f_2 \rangle = F_2$$

and so $\mathrm{Sym}(5)$ acts tranistively on J. Note that $\mathrm{Sym}(5)_J \le \mathrm{Sym}(5)_F$ for any $F \in J$. Since $|Sym(5)/\mathrm{Sym}(5)_F = | = |J| = 6$, $\mathrm{Sym}(5)_F$ has order 24 and so $|\mathrm{Sym}(5)_J| \le 24$. Since $\mathrm{Sym}(5)_J$ is normal in $\mathrm{Sym}(5)$ and the only normal subgroups of $\mathrm{Sym}(5)$ are $\{(1)\}$, $\mathrm{Alt}(5)$ and $\mathrm{Sym}(5)$, we conclude that $\mathrm{Sym}(5)_J = \{(1)\}$. So $\mathrm{Sym}(5)$ acts faithfully on J. Thus $\mathrm{Sym}(J)$ contains a subgroup isomorphic to $\mathrm{Sym}(5)$ and acting transitively on J. Since $|J| = 6$ it follows that $\mathrm{Sym}(6)$ contains a subgroup H isomorphic to $\mathrm{Sym}(5)$ which acts transitively on $\{1,2,\dots,6\}$.

On the other hand by 1.10.15 H fixes the point $i = H$ in the $\mathrm{Sym}(6)$-set $I = \mathrm{Sym}(6)/H$. This seems to be contradictory, but isn't. The set I is a set with six elements on which $\mathrm{Sym}(6)$ acts but it is not isomorphic to the set $\{1,2,3,4,5,6\}$. So $\mathrm{Sym}(6)$ has two non-isomorphic action on sets of size six. Indeed this also follows from Homework 4#4: Let $\alpha : \mathrm{Sym}(6) \to \mathrm{Sym}(6)$ be an isomorphism which is not inner. Let $*_\alpha$ be the corresponding action of $\mathrm{Sym}(6)$ on $\{1,\dots,6\}$. It is fairly easy to see that since α is not inner, $*_\alpha$ is not isomorphic the standard action of $\mathrm{Sym}(6)$ on $\{1,\dots,6\}$. (see Homework 5#1).

1.8 Generation of subgroups and cyclic groups

Definition 1.8.1. *Let $\mathcal{D}$ be a class and I set.*

(a) $\mathrm{Fun}(I)$ *is the class of all functions with domain I.* $\mathrm{Fun}(I,\mathcal{D})$ *is the set of all functions from I to $\mathcal{D}$.*

(b) An I-tuple is function with domain I. An I-tuple in $\mathcal{D}$ is a function from I to $\mathcal{D}$.

(c) A $\mathcal{D}$-family is an I-tuple in $\mathcal{D}$ for some set I.

Notation 1.8.2. *Let f be an I-tuple. Then we denote f by $(f_i)_{i\in I}$, where f_i is the image of i under f.*

Lemma 1.8.3. *Let G be a group and $(G_i)_{i\in I}$ a family of subgroups of G. Then $\bigcap_{i\in I} G_i$ is a subgroup. If each G_i, $i \in I$ is normal in G, so is $\bigcap_{i\in I} G_i$.*

Proof. Since $e \in G_i$ for all i, $e \in \bigcap_{i\in I} G_i$. Let $a, b \in \bigcap_{i\in I} G_i$. Then $ab \in G_i$ and $a^{-1} \in G_i$ for all $i \in I$. Hence $ab \in \bigcap_{i\in I} G_i$ and $a^{-1} \in \bigcap_{i\in I} G_i$. Thus $\bigcap_{i\in I} G_i$ is a subgroup of G.

Suppose in addition that each G_i is normal in G and let $g \in G$ and $a \in \bigcap_{i\in I} G_i$. Then ${}^g a \in G_i$ and so ${}^g a \in \bigcap_{i\in I} G_i$. Thus $\bigcap_{i\in I} G_i$ is normal in G. □

Definition 1.8.4. *Let G be a group and $J \subseteq G$.*

(a) The subgroup $\langle J\rangle$ of G generated *by J is defined by*

$$\langle J\rangle = \bigcap_{J\subseteq H\leq G} H.$$

(b) The normal subgroup $\langle {}^G J\rangle$ of G generated by J is defined by

$$\langle {}^G J\rangle = \bigcap_{J\subseteq H\trianglelefteq G} H.$$

(c) If $(J_i)_{i\in I}$ is a family of subsets of J we write $\langle J_i \mid i \in I\rangle$ for $\langle \bigcup_{i\in I} J\rangle$.

(d) $J \subseteq G$ is called normal if ${}^g J = J$ for all $g \in G$.

Lemma 1.8.5. *Let I be a subset of G.*

(a) Let $\alpha : G \to H$ be a group homomorphism. Then $\alpha(\langle I\rangle) = \langle \alpha(I)\rangle$.

(b) Let $g \in G$. Then ${}^g\langle I\rangle = \langle {}^g I\rangle$.

(c) If I is normal in G, so is $\langle I\rangle$.

(d) $\langle I\rangle = \langle I^{-1}\rangle$.

(e) $\langle I\rangle$ consists of all products of elements in $I \cup I^{-1}$.

(f) $\langle {}^G I\rangle = \langle {}^g I \mid g \in G\rangle$ and consists of all products of elements in $\bigcup_{g\in G} {}^g(I \cup I^{-1})$.

Proof. (a) Let $A = \langle I \rangle$ and $B = \langle \alpha(I) \rangle)$. As $\alpha(A)$ is a subgroup of H and contains $\alpha(I)$ we have $B \le \alpha(A)$. Also $\alpha^{-1}(B)$ is a subgroup of G and contains I. Thus $A \le \alpha^{-1}(B)$ and so $\alpha(A) \le B$. Hence $B = \alpha(A)$.

(b) Apply (a) to the homomorphism $i_g : G \to G, x \to {}^g x$.

(c) Follows from (b).

(d) Let H be a subgroup of G. Then H is closed under inverses and so $I \subseteq H$ if and only of $I^{-1} \subseteq H$. Thus (f) follows from the definition of $\langle I \rangle$.

(e) Let H be the subset of G consists of all products of elements in $I \cup I^{-1}$, that is all elements of the form $a_1 a_2 \ldots a_n$, with $n \ge 0$ and $a_i \in I \cup I^{-1}$ for all $1 \le i \le n$. Here if $n = 0$ we define $a_1 \ldots a_n$ to be e. Clearly H is contained in any subgroup of G containing I. Thus $H \subseteq \langle I \rangle$. Now it is readily verified that H is also a subgroup containing I and so $\langle I \rangle \le H$.

(f) Note that $\bigcup_{g \in G} {}^g I$ is a normal subset of G. Hence by (c) $H := \langle {}^g I \mid g \in G \rangle$ is normal subgroup of G. So $\langle {}^G I \rangle \le H$. If $I \subseteq K \trianglelefteq G$, then ${}^g I \subseteq K$ for all $g \in G$. Thus also $H \le K$ and so $H \le \langle {}^G I \rangle$. It is also contained in every normal subgroup containing I and we get $\langle {}^G I \rangle = H$. The second statement now follows from (e). □

Lemma 1.8.6. *Let G be a group.*

(a) Let A, B be subgroups of G. Then AB is a subgroup of G if and only if $AB = BA$.

(b) If $K, H \le G$ and $K \le N_G(H)$, then KH is a subgroup of G and $\langle K, H \rangle = KH$.

(c) Let $K_i, i \in I$ be a family of subsets of G. If each $K_i \le N_G(H)$ for each $i \in I$, then $\langle K_i \mid i \in I \rangle \le N_G(H)$.

Proof. (a) Note that

$$(*) \qquad (AB)^{-1} = B^{-1}A^{-1} = BA.$$

If AB is a subgroup of G, then $AB = (AB)^{-1}$ and (*) shows that $AB = BA$.

Conversely suppose that $AB = BA$. Then (*) shows that AB is closed under inverses. Also $e = ee \in AB$ and

$$(AB)(AB) = A(BA)B = A(AB)B = A^2B^2 \subseteq AB.$$

So AB is closed under multiplication.

(b) Let $k \in K$. Then ${}^k H = H$, $kHk^{-1} = H$, $kH = Hk$ and so $HK = KH$. So by (a) HK is a subgroup of G. Hence $\langle H, K \rangle \le HK \le \langle H, K \rangle$ and (b) holds.

(c) Since $K_i \subseteq N_G(H)$ for all $i \in I$ and $N_G(H)$ is subgroup of G we have $\langle K_i \mid i \in I \rangle \le N_G(H)$ and (c) holds. □

Definition 1.8.7. *Let G be a group and $a, b \in G$ and $A, B \subseteq G$.*

(a) $[a, b] := aba^{-1}b^{-1}$. $[a, b]$ *is called the* commutator *of a and b*

(b) $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$. $[A, B]$ *is called the* commutator group *of A and B.*

(c) ${}^{-a}b = ({}^a b)^{-1} = {}^a(b^{-1})$

Lemma 1.8.8. *Let G be a group and $a, b \in G$.*

(a) $[a,b] = e$ *if and only if* $ab = ba$.

(b) $[a,b] = {}^{a}bb^{-1} = a \cdot {}^{-b}a$

(c) $[a,b]^{-1} = [b,a]$.

(d) $[A,B] = [B,A]$ *for any* $A, B \subseteq G$.

Proof. (a): $[a,b] = e \Longleftrightarrow aba^{-1}b^{-1} = e$. Multipliying with ba from the right the latter equation is equivalent to $ab = ba$.

(b) $[a,b] = (aba^{-1}b^{-1} = {}^{a}bb^{-1}$ and $[a,b] = a(ba^{-1}b^{-1}) = a({}^{-b}a)$.

(c) $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1}b^{-1}a^{-1} = bab^{-1}a^{-1} = [b,a]$.

(d) Using (c) and 1.8.5(d)

$$[A,B] = \langle [a,b] \mid a \in A, b \in B\rangle = \langle [a,b]^{-1} \mid a \in A, b \in B\rangle = \langle [b,a] \mid a \in A, b \in B\rangle = [B,A].$$

□

Lemma 1.8.9. *Let G be a group.*

(a) Let $N \leq G$. *Then* $N \trianglelefteq G$ *if and only if* $[G,N] \leq N$.

(b) Let $A, B \trianglelefteq G$. *Then* $[A,B] \leq A \cap B$.

(c) Let $A, B \trianglelefteq G$ *with* $A \cap B = \{e\}$. *Then* $[A,B] = \{e\}$ *and* $ab = ba$ *for all* $a \in A, b \in B$.

Proof. (a) ${}^{g}n \in N \Longleftrightarrow {}^{g}nn^{-1} \in N \Longleftrightarrow [g,n] \in N$. Thus (a) holds.

(b) By (a) $[A,G] = [G,A] \leq A$ and $[G,B] \leq B$. Thus

$$[A,B] \leq [A,G] \cap [G,B] \leq A \cap B$$

(c) By (b), $[A,B] \leq A \cap B = \{e\}$. Thus for all $a \in A, b \in B$, $[a,b] = e$ and so by 1.8.8(a) we have $ab = ba$. □

Definition 1.8.10. *Let G be a group.*

(a) G is called cyclic *if* $G = \langle x \rangle$ *for some* $x \in G$.

(b) Let $x \in G$. *Then* $|x| := |\langle x \rangle|$. $|x|$ *is called the* order *of x in G.*

We will now determine all cyclic groups up to isomorphism and investigate their subgroups and homomorphisms.

Lemma 1.8.11. *(a) Let H be a subgroup of* $(\mathbb{Z}, +)$ *Then* $H = n\mathbb{Z}$ *for some* $n \in \mathbb{N}$.

(b) Let $n, m \in \mathbb{N}$. *Then* $n\mathbb{Z} \leq m\mathbb{Z}$ *if and only if m divides n.*

Proof. (a) If $H = \{0\}$, then $H = 0\mathbb{Z}$. So we may assume that $H \neq \{0\}$. Since H is a subgroup, $m \in H$ implies $-m \in H$. So H contains some positive integer. Let n be the smallest such. Let $m \in H$ and write $m = rn + s$, $r, s \in \mathbb{Z}$ with $0 \leq s < n$. We claim that $rn \in H$. $rn \in H$ if and only if $-rn \in H$. So we may assume $r > 0$. But then

$$rn = \underbrace{n + n + \ldots + n}_{r-\text{times}}$$

and as $n \in H$, $rn \in H$. So also $s = m - rn \in H$. Since $0 \leq s < n$, the minimal choice of n implies $s = 0$. Thus $m = rn \in n\mathbb{Z}$ and $H = n\mathbb{Z}$.

(b) $n\mathbb{Z} \leq m\mathbb{Z}$ if and only if $n \in m\mathbb{Z}$. So if and only if m divides n. □

Lemma 1.8.12. *Let G be a group and $g \in G$. Then $\phi : \mathbb{Z} \to G, \quad n \to g^n$ is the unique homomorphism from $(\mathbb{Z}, +)$ to G which sends 1 to g.*

Proof. More or less obvious. □

Definition 1.8.13. *For $r \in \mathbb{Z}^+ \cup \{\infty\}$ define $r^* = \begin{cases} r & \text{if } r < \infty \\ 0 & \text{if } r = \infty \end{cases}$.*

This definition is motivated by the following lemma:

Lemma 1.8.14. *Let $n \in \mathbb{N}$. Then $|\mathbb{Z}/n\mathbb{Z}|^* = n$.*

Proof. If $n \neq 0$, then $|\mathbb{Z}/n\mathbb{Z}| = n$ and $n^* = n$. If $n = 0$, then $|\mathbb{Z}/0\mathbb{Z}| = \infty$ and $\infty^* = 0$. □

Lemma 1.8.15. *Let $G = \langle x \rangle$ be a cyclic group and put $n = |G|^*$*

(a) The map

$$\mathbb{Z}/n\mathbb{Z} \to G, \quad m + n\mathbb{Z} \to x^m$$

is a well-defined isomorphism.

(b) Let $H \leq G$ and put $m = |G/H|^*$. Then m divides n, and $H = \langle x^m \rangle$.

Proof. (a) By 1.8.12 the map $\phi : \mathbb{Z} \to G, m \to g^m$ is a homomorphism. As $G = \langle x \rangle$, ϕ is onto. By 1.8.11 $\ker \phi = t\mathbb{Z}$ for some non-negative integer t. By the isomorphism theorem the map

$$\overline{\phi} : \mathbb{Z}/t\mathbb{Z} \to G, m + t\mathbb{Z} \to x^m.$$

is a well defined isomorphism. Hence $\mathbb{Z}/t\mathbb{Z} \cong G$. Thus $t = |\mathbb{Z}/t\mathbb{Z}|^* = |G|^* = n$ and (a) is proved.

(b) By 1.8.11 $\phi^{-1}(H) = s\mathbb{Z}$ for some $s \in \mathbb{N}$. Since $\ker \phi = \phi^{-1}(e) \leq \phi^{-1}(H)$ we have $n\mathbb{Z} \leq s\mathbb{Z}$. Thus 1.8.11 implies that s divides n. As ϕ is onto, $\phi(s\mathbb{Z}) = H$ and so

$$H = \phi(s\mathbb{Z}) = \phi(\langle s \rangle) = \langle \phi(s) \rangle = \langle x^s \rangle$$

It follows that

$$\overline{\phi}(s\mathbb{Z}/n\mathbb{Z}) = \overline{\phi}(\langle s + n\mathbb{Z} \rangle) = \langle \overline{\phi}(s + n\mathbb{Z}) \rangle = \langle x^s \rangle = H$$

and since $\overline{\phi}$ is an isomorphism,

$$|G/H| = \left|\mathbb{Z}/n\mathbb{Z}\big/s\mathbb{Z}/n\mathbb{Z}\right| = |\mathbb{Z}/s\mathbb{Z}|.$$

Thus $s = m$ and (b) is proved. □

Lemma 1.8.16. *Let $G = \langle x\rangle$ be a cyclic group. Let H be any group and $y \in H$. Put $n = |G|^*$ and $m = |y|^*$. Then there exists a homomorphism $G \to H$ with $x \to y$ if and only if m divides n.*

Proof. Exercise. □

1.9 Direct products and direct sums

Definition 1.9.1. *Let $(S_i)_{i\in I}$ be a family of sets. Then $\bigtimes_{i\in I} S_i$ is the set of all I-tuples f with $f(i) \in S_i$ for all $i \in I$. For $i \in I$ define*

$$\pi_i : \bigtimes_{i\in I} S_i \to S_i, \quad f \mapsto f(i)$$

Then π_i is called the projection of $\bigtimes_{i\in I} S_i$ onto S_i.

Definition 1.9.2. *Let $(S_i)_{i\in I}$ be a family of sets. A* direct product *of $(S_i)_{i\in I}$ is pair $\big(S, (\pi_i)_{i\in I}\big)$, where S is a set and $(\pi)_{i\in I}$ is a family of functions $\pi_i : S \to S_i$, with the following property:*

Whenever T is a set and $(\alpha_i : T \to S)_{i\in I}$ is family of functions, then there exists a unique function $\alpha : T \to S$ such that $\alpha_i = \pi_i \circ \alpha$ for all $i \in I$.

Note that $\alpha_i = \pi_i \circ \alpha$ means that the diagram

$$\begin{tikzcd} T \arrow[rr, "\exists!\,\alpha"] \arrow[dr, "\alpha_i"'] & & S \arrow[dl, "\pi_i"] \\ & S_i & \end{tikzcd}$$

commutes for all $i \in I$.

Lemma 1.9.3. *Any family of sets $(S_i)_{i\in I}$ has a direct product $(S, (\pi_i : S \to G_i)_{i\in I})$. Moreover, if $(T, (\alpha_i : T \to S_i)_{i\in I})$ is also direct product of $(S_i)_{i\in I}$, then there exists a bijection $\alpha : T \to S$ with $\alpha_i = \pi_i \circ \alpha$ for all $i \in I$.*

Proof. We will first show the existence. Let $S = \bigtimes_{i\in I} S_i$ and for $i \in I$ let π_i be the projection of S onto S_i. We will show that $\big(S, (\pi_i)_{i\in I}\big)$ is a direct product of $(S_i)_{i\in I}$.

For this let T a set and $(\alpha_i : T \to S_i)_{i\in I}$ a family of functions. Let $\alpha : T \to S$ be a function. Then

$$\begin{aligned} & \pi_i \circ \alpha = \alpha_i && \text{for all } i \in I \\ \Longleftrightarrow\quad & \pi_i(\alpha(t)) = \alpha_i(t) && \text{for all } i \in I, t \in T \\ \Longleftrightarrow\quad & \alpha(t)(i) = \alpha_i(t) && \text{for all } i \in I, t \in T \\ \Longleftrightarrow\quad & \alpha(t) = (\alpha_i(t))_{i\in I} && \text{for all } t \in T \end{aligned}$$

So $\alpha : T \to S, (\alpha_i(t))_{i\in I}$ is the unique function from $T \to S$ with $\alpha \circ \pi_i$ for all $i \in I$. Thus $(\pi_i)_{i\in I}$ is indeed a direct product of $(S_i)_{i\in I}$.

To prove the uniqueness assertion let $\big(T, (\alpha_i : T \to S_i)_{i\in I}\big)$ also be direct product of $(S_i)_{i\in I}$. Since $\big(S, (\pi_i)_{i\in I}\big)$ is a direct product. there exists a function $\alpha : T \to S$ with $\alpha_i = \pi_i \circ \alpha$ for all $i \in I$. We need to show that α is bijection.

Since $\big(T, (\alpha_i)_{i\in I}\big)$ is a direct product there exists a function $\beta : S \to T$ with $\pi_i = \alpha_i \circ \beta$ for all $i \in I$. Consider the composition $\alpha \circ \beta : S \to S$. We have

$$\pi_i \circ (\alpha \circ \beta) = (\pi_i \circ \alpha) \circ \beta = \alpha_i \circ \beta = \pi_i$$

also

$$\pi_i \circ \mathrm{id}_S = \pi_i$$

Hence the diagrams

$$\begin{tikzcd} S \arrow[rr, "\alpha\circ\beta"] \arrow[dr, "\pi_i"'] & & S \arrow[dl, "\pi_i"] \\ & S_i & \end{tikzcd}$$

and

$$\begin{tikzcd} S \arrow[rr, "\mathrm{id}_S"] \arrow[dr, "\pi_i"'] & & S \arrow[dl, "\pi_i"] \\ & S_i & \end{tikzcd}$$

commute. So by the uniqueness assertion in the definition of a direct product we conclude that $\alpha \circ \beta = \mathrm{id}_S$. By symmetry also $\beta \circ \alpha = \mathrm{id}_T$. Thus α is a bijection. □

1.9.4 (Further Products of Sets)**.** Let $(S_i)_{i\in I}$. We will investigate what happens to Definition 1.9.2 in we reverse some or all of the arrows:

(1)

$$\begin{tikzcd} T \arrow[dr, "\alpha_i"'] & & S \arrow[ll, "\exists!\,\alpha"'] \arrow[dl, "\pi_i"] \\ & S_i & \end{tikzcd}$$

Here we can just choose $S = \varnothing$ and so also $\pi_i = \varnothing$ and $\alpha = \varnothing$.

(2)

$$\begin{tikzcd}
T \arrow[rr, "\exists!\,\alpha"] & & S \arrow[dl, "\pi_i"] \\
& S_i \arrow[ul, "\alpha_i"] &
\end{tikzcd}$$

This diagram makes no sense, since the composition of any two functions which can be composed is in the reverse direction of the third.

(3)

$$\begin{tikzcd}
T \arrow[rr, "\exists!\,\alpha"] \arrow[dr, "\alpha_i"'] & & S \\
& S_i \arrow[ur, "\pi_i"'] &
\end{tikzcd}$$

Here we can choose $S = \{s\}$ and define π_i and α by $\pi_i(s_i) = s = \alpha(t)$ for all $s_i \in S_i, t \in T$.

(4)

$$\begin{tikzcd}
T & & S \arrow[ll, "\exists!\,\alpha"'] \arrow[dl, "\pi_i"] \\
& S_i \arrow[ul, "\alpha_i"] &
\end{tikzcd}$$

As in (1) choose $S = \pi_i = \alpha = \varnothing$.

(5)

$$\begin{tikzcd}
T \arrow[dr, "\alpha_i"'] & & S \arrow[ll, "\exists!\,\alpha"'] \\
& S_i \arrow[ur, "\pi_i"'] &
\end{tikzcd}$$

Diagram makes no sense (just as (2)).

(6)

$$\begin{tikzcd}
T \arrow[rr, "\exists!\,\alpha"] & & S \\
& S_i \arrow[ul, "\alpha_i"] \arrow[ur, "\pi_i"'] &
\end{tikzcd}$$

As in (3) choose $S = \{s\}$ and define π_i and α by $\pi_i(s_i) = s = \alpha(t)$ for all $s_i \in S_i, t \in T$.

(7)

$$\begin{tikzcd}
T & & S \arrow[ll, "\exists!\,\alpha"'] \\
& S_i \arrow[ul, "\alpha_i"] \arrow[ur, "\pi_i"'] &
\end{tikzcd}$$

This is the only interesting case (other than the direct product). Let $S = \dot{\bigcup}_{i\in I} S_i$, the disjoint union of the $S_i, i \in I$. So

$$S = \{(i, s) \mid i \in I, s \in S_i\}.$$

Define

$$\pi_i : S_i \to S, s \to (i, s)$$

and for a given family $\alpha_i : S_i \to T$,

$$\alpha : S \to T, \quad (i, s) \mapsto \alpha_i(s)$$

$(S, (\pi)_{i\in S})$ is called the coproduct of the family $(S_i)_{i\in I}$.

We now will look at the direct product of groups and in section 1.12 at the coproduct of groups.

Definition 1.9.5. *Let $(G_i)_{i\in I}$ be a family of groups. A* direct product *of the $(G_i)_{i\in I}$ is a pair $\big(G, (\pi_i)_{i\in I}\big)$ where G is a group and $(\pi_i)_{i\in I}$ is a family of group homomorphism $\pi_i : G \to G_i$ with the following property:*

Whenever H is a group and $(\alpha_i : H \to G_i)_{i\in I}$ is family of group homomorphism, then there exists a unique homomorphism $\alpha : H \to G$ such that $\alpha_i = \pi_i \circ \alpha$ for all $i \in I$.

Just as for sets, the definition can be summarized in the following commutative diagram

$$\begin{tikzcd}
H \arrow[rr, "\exists!\,\alpha"] \arrow[dr, "\alpha_i"'] & & G \arrow[dl, "\pi_i"] \\
& G_i &
\end{tikzcd}$$

Lemma 1.9.6. *Any family of groups $(G_i)_{i\in I}$ has a direct product $\big(G, (\pi_i : G \to G_i)_{i\in I}\big)$. Moreover, if $\big(H, (\alpha_i : H \to G_i)_{i\in I}\big)$ is also a direct product of $(G_i)_{i\in I}$, then there exists an isomorphism $\alpha : H \to G$ with $\alpha_i = \pi_i \circ \alpha$ for all $i \in I$.*

Proof. We will first show the existence. As a set let $G = \bigtimes_{i\in I} G_i$ and for $i \in I$ let π_i be the projection of G onto G_i. Define a binary operation on G by

$$(*) \qquad (fg)(i) = f(i)g(i)$$

for all $f, g \in I$. It is a routine exercise to verify that G is a group under this operation.

By definition of π_i (*) can be rewritten as

$$\pi_i(fg) = \pi_i(f)\pi_i(g)$$

and so π_i is a homomorphism.

Let H a group and $(\alpha_i : H \to G_i)_{i\in I}$ a family of a family of group homomorphism. Since $(\pi_i)_{i\in I}$ is the set-theoretic direct product of $(G_i)_{i\in I}$ there exist a unique function $\alpha : H \to G$ with $\alpha_i = \pi_i \circ \alpha$, namely $\alpha(h) = (\alpha_i(h))_{i\in I}$ for all $i \in I$. Then for all $h, k \in H$:

$$\alpha(hk) = (\alpha_i(hk))_{i\in I} = (\alpha_i(h)\alpha_i(k))_{i\in I} = (\alpha_i(h))_{i\in I}(\alpha_i(k))_{i\in I} = \alpha(h)\alpha(k)$$

and so α is a homomorphism.

The proof of the uniqueness statement is the same is for sets. Essentially one just need to replace "function" by "homomorphism" everywhere in the proof. □

Definition 1.9.7. *Let $(G_i)_{i\in I}$ be a family of groups.*

(a) For $g \in \bigtimes_{i\in I} G_i$ define

$$\mathrm{Supp}(g) := \{i \in I \mid g(i) \neq 1_{G_i}\}$$

g is called almost trivial *if* Supp(g) *is finite.*

(b) $\bigoplus_{i\in I} G_i$ is the set of all almost trivial elements in $\bigtimes_{i\in I} G_i$. $\bigoplus_{i\in I} G_i$ is called the direct sum *of $(G_i)_{i\in I}$.*

Definition 1.9.8. *Let G be a group.*

(a) A family $(a_i)_{i\in I}$ of elements in G is called commuting if $a_i a_j = a_j a_i$ for all $i, j \in I$.

(b) Let $(a_i)_{i\in I}$ be an almost trivial, commuting family of elements in G. Then

$$\prod_{i\in I} a_i = a_{i_1} a_{i_2} \ldots a_{i_k}$$

where $i_1, i_2 \ldots i_k$ are the pairwise distinct elemenst of I with $a_{i_j} \neq 1$. Note that since $a_i a_j = a_j a_i$, this definition does not dependent on the order the $i_1, \ldots i_k$ are chosen.

Lemma 1.9.9. *Let $(G_i)_{i\in I}$ be a family of groups. For $j \in I$ define $\rho_j : G_j \to \bigoplus_{i\in I} G_i$ by*

$$\rho_j(g)(i) = \begin{cases} g & \text{if } i = j \\ 1_{G_i} & \text{if } i \neq j \end{cases}$$

for all $g \in G_i$.

(a) $\bigoplus_{i\in I} G_i$ is a subgroup of $\bigtimes_{i\in I} G_i$.

(b) For all $j \in I$, ρ_j is a 1-1 homomorphism.

(c) $[\rho_i(G_i), \rho_j(G_j)] = 1$ *for all* $i \neq j \in I$.

(d) Let $g \in \bigoplus_{i\in I} G_i$. *Then there exist a uniquely determined almost trivial family* $(h_i)_{i\in I} \in \bigtimes_{i\in I} G_i$ *with* $g = \prod_{i\in I} \rho_i(h_i)$. *Namely* $h = g$.

(e) $\bigoplus_{i\in I} G_i = \langle \rho_i(G_i) \mid i \in I\}\rangle$

Proof. (a) This follows since $\operatorname{Supp}(a^{-1}) = \operatorname{Supp}(a)$ and $\operatorname{Supp}(ab) \subseteq \operatorname{Supp}(a) \cup \operatorname{Supp}(b)$.

(b) This is readily verified.

(c) Let $j \neq k \in I$, $g_j \in G_j$ and $g_k \in G_k$. Then

$$(\rho(g_j)\rho(g_k))(i) = \begin{cases} g_j & \text{if } i = j \\ g_k & \text{if } i = k \\ 1 & \text{if } j \neq i \neq k \end{cases} = (\rho(g_k)\rho(g_j))(i)$$

Thus $\rho_j(g_j)\rho_k(g_k) = \rho_k(g_k)\rho_j(g_j)$ and (c) holds.

(d) Just observe that by the definition of $\rho_j(h_j)$

$$\left(\prod_{i\in I} \rho_i(h_i)\right)_j = h_j.$$

(e) By (d) $g = \prod_{i\in I} \rho_i(g_i) \in \langle \rho_i(G_i) \mid i \in I\rangle$. Thus (e) holds. □

Lemma 1.9.10. *Let* $(G_i)_{i\in I}$ *be family of groups,* H *a group and* $(\alpha_i : G_i \to H)_{i\in I}$ *a family of homomorphism such that*

$$(*) \qquad \alpha_i(g_i)\alpha_j(g_j) = \alpha_j(g_j)\alpha_i(g_i)$$

for all $i \neq j \in I$, $g_i \in G_i$ *and* $g_j \in G_j$. *Then there exists a unique homomorphism*

$$\alpha : \bigoplus_{i\in I} G_i \to H \qquad \textit{with} \qquad \alpha_i = \alpha \circ \rho_i \qquad \textit{for all } i \in I$$

Moreover,

$$\alpha\big(g_i)_{i\in I}\big) = \prod_{i\in I} \alpha_i(g_i)$$

for all $\big(g_i)_{i\in I}\big) \in \bigoplus_{i\in I} G_i$.

$$\begin{tikzcd}
H & & G \arrow[ll, "\exists!\,\alpha"'] \\
& G_i \arrow[ul, "\alpha_i"] \arrow[ur, "\rho_i"'] &
\end{tikzcd}$$

Proof. Let $(g_i)_{i\in I} \in \bigoplus_{i\in I} G_i$. If $g_i = 1_{G_i}$, then $\alpha(g_i) = 1_H$ and so $(\alpha_i(g_i))_{i\in I}$ is almost trivial. By (*) this family is commuting and so we obtain a function

$$\alpha : \bigoplus_{i\in I} G_i \to H, \quad (g_i)_{i\in I} \to \prod_{i\in I} \alpha_i(g_i)$$

Let $(g_i')_{i\in I} \in \bigoplus_{i\in I} G_i$. By (*) $\alpha_i(g_i)\alpha_j(g_j') = \alpha_j(g_j')\alpha_i(g_i)$ for all $i \neq j \in J$ and so an straightforward induction arguments shows

$$\Big(\prod_{i\in I} \alpha_i(g_i')\Big)\Big(\prod_{i\in I} \alpha_i(g_i)\Big) = \prod_{i\in I} \big(\alpha_i(g_i)\alpha_i(g_i')\big)$$

Since α_i is a homomorphism, $\alpha_i(g_i)\alpha_i(g_i') = \alpha_i(g_i g_i')$ and we conclude that α is a homomorphism.

Let $i \in I$ and $g \in G$. Then $\rho_i(g)_j = 1_{G_j}$ for all $i \neq j \in J$. So $\alpha_j(\rho_i(g)_j) = 1_H$ and thus $\alpha(\rho_i(g)) = \alpha_i(g)$. Hence $\alpha_i = \alpha \circ \rho_i$.

To show uniqueness let $\beta : \bigoplus_{i\in I} G_i \to G$ be a homomorphism with $\alpha_i = \beta \circ \rho_i$ for all $i \in I$. Then

$$\beta\big((g_i)_{i\in I}\big) = \beta\Big(\prod_{i\in I} \rho_i(g_i)\Big) = \prod_{i\in I} \beta\big(\rho_i(g_i)\big) = \prod_{i\in I} \alpha_i(g_i) = \alpha\big((g_i)_{i\in I}\big)$$

and so α is unique. □

Definition 1.9.11. *Let G be a group and $(G_i)_{i\in I}$ a family of subgroups of G. We say that G is the* internal direct sum *of $(G_i)_{i\in I}$ and write*

$$G = \bigoplus_{i\in I}^{\text{int}} G_i$$

provided that

(i) $G_i \trianglelefteq G$ *for all* $i \in I$.

(ii) $G = \langle G_i \mid i \in I\rangle$.

(iii) For each i, $G_i \cap \langle G_j \mid i \neq j \in I\rangle = 1$.

Proposition 1.9.12. *Let G be a group and $(G_i)_{i\in I}$ a family of subgroups of G. Suppose that G is the internal direct sum of $(G_i)_{i\in I}$.*

Then the map

$$\alpha : \bigoplus_{i\in I} G_i \to G, \quad (g_i)_{i\in I} \to \prod_{i\in I} g_i$$

is a well-defined isomorphism.

Proof. For $i \in I$ put $G^i := \langle G_j \mid i \neq j \in I\rangle$. Let $g \in G$. Since $G_j \trianglelefteq G$ we have ${}^g G_j = G_j$ and so using 1.8.5(b) we compute

$${}^g G^i = \langle {}^g G_j \mid i \neq j \in I\rangle = \langle G_j \mid i \neq j \in I\rangle = G^i$$

Thus $G^i \trianglelefteq G$. By 1.9.11(iii), $G_i \cap G^i = \{e\}$ and so by 1.8.9(c) $ab = ba$ for all $a \in G_i, b \in G^i$. If $j \neq i \in I$ then $G_j \leq G^i$ and so $g_i g_j = g_j g_i$ for all $g_i \in G_i$ and $g_j \in G_j$. So by 1.9.10 α is a well-defined homomorphism and $\alpha(\rho_i(g_i)) = g_i$. Thus $G_i \leq \operatorname{Im}\alpha$. Since $\operatorname{Im}\alpha$ is a subgroup of G we conclude $\langle G_i \mid i \in I\rangle \leq \operatorname{Im}\alpha$. Hence 1.9.11(ii), $\operatorname{Im}\alpha = G$ and so α is onto.

Suppose that

$$\prod_{i\in I} g_i = \prod_{i \in I} a_i$$

for some $(g_i)_{\in I}, (a_i)_{i\in I} \in \bigoplus_{i\in I}$. Then

$$a_i g_i^{-1} = \prod_{i \neq j \in I} a_j^{-1} g_j$$

Note that the left side is in G_i and the right side in G^i. Since $G_i \cap G^i = \{e\}$ we conclude that $a_i g_i^{-1} = e$ and so $a_i = g_i$. Thus α is 1-1 and the lemma is proved. □

Note that the preceeding lemma implies that if $G = \bigoplus_{i\in I}^{\text{int}} G_i$ then G is canonically isomorphic to $\bigoplus_{i\in I} G_i$. For this reason we will often abuse language and write $G = \bigoplus_{i\in I} G_i$ to indicated that G is the internal direct sum of $(G_i)_{i\in I}$.

Example 1.9.13. Let $G = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leq \operatorname{Sym}(4)$. Let $G_1 = \{(1), (1,2)(3,4)\}$ and $G_2 = \{(1), (1,3)(2,4)\}$. Since G is abelian, G_1 and G_2 are normal subgroup of G. Since $(1,2)(3,4) \circ (1,3)(2,4) = (1,4)(2,3)$, $\langle G_1, G_2\rangle = G$. Moreover, $G_1 \cap G_2 = \{(1)\}$ and so G is the internal direct sum of G_1 and G_2. Note that $G_i \cong \mathbb{Z}/2\mathbb{Z}$. Thus

$$G = G_1 \oplus G_2 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2\mathbb{Z}.$$

1.10 Sylow p-subgroup

Hypothesis 1.10.1. *Throughout this section G is a finite group and p a prime.*

Definition 1.10.2. *(a) A* p-subgroup *of G is a subgroup $P \leq G$ which is a p-group.*

(b) A Sylow p-subgroup *S of G is a maximal p-subgroup of G. That is S is a p-subgroup of G and if $S \leq Q$ for some p-subgroup Q, then $S = Q$.*

(c) $\operatorname{Syl}_p(G)$ *is the the set of all Sylow p-subgroups of G.*

Let $n \in \mathbb{Z}^+$ and $n = p^k m$ with $k \in \mathbb{N}$, $m \in \mathbb{Z}^+$ and $p \nmid m$, then $n_p = p^k$. n_p is called the p-part of n. Often a Sylow p-subgroup is defined to be a subgroup of order $|G|_p$. This turns out to be equivalent to our definition (see 1.10.3(b) and 1.10.9(c)), but I prefer the above definition for two reason: 1. It is easy to see that Sylow p-subgroups exists (see the next lemma). 2. The given definition also makes sense for infinite groups (allthough infinite groups may not have a Sylow p-subgroup).

Lemma 1.10.3. *(a) Any p-subgroup of G is contained in a Sylow p-subgroup of G. In particular,* $\operatorname{Syl}_p(G)$ *is not empty.*

(b) Let $S \leq G$ with $|S| = |G|_p$. Then S is a Sylow p-subgroup of G.

Proof. (a) Let P be a p-sugroups and let S be a p-subgroup of G such that $|S|$ is maximal with respect to $P \leq S$. We claim that $S \in \mathrm{Syl}_p(G)$. For this let Q be a p-subgroup of G with $S \leq Q$. Then also $P \leq Q$ and so by maxiality of $|S|$, $|Q| \leq |S|$. Since $S \leq Q$ this gives $S = Q$ and so $S \in \mathrm{Syl}_p(G)$.

In particular, $\{e\}$ is contained in a Sylow p-subgroup of G and so $\mathrm{Syl}_p(G) \neq \varnothing$.

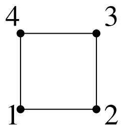
(b) Let Q be a p-subgroup of G with $S \leq Q$. By Lagrange's, $|Q|$ divides $|G$. Since $|Q|$ is a power of p, $|Q|$ divides $|G|_p = |S|$. Thuse $|Q| \leq |S|$ and $S = Q$. So $S \in \mathrm{Syl}_p(G)$. □

Example 1.10.4. 1. Let $G = \mathrm{Sym}(5)$. Then $|G| = 5! = 120 = 2^3 \cdot 3 \cdot 5$. Thus by 1.10.3(b),

$$\langle (123) \rangle \in \mathrm{Syl}_3(G)$$

$$\langle (12345) \rangle \in \mathrm{Syl}_5(G)$$

$$\mathrm{Dih}_8 \in \mathrm{Syl}_2(G)$$

Here $\mathrm{Dih}_8 = \langle (14)(23), (13) \rangle$ is the automorphism groups of the square 

2. $\mathcal{E}$ be a projective plane of order two and $G = \mathrm{Aut}(\mathcal{E})$. Then $|G| = 168 = 2^3 \cdot 3 \cdot 7$. Let P be a point incident to the line l. Then $\mathrm{Stab}_G(\{P, l\})$ is a Sylow 2-subgroups of G.

Lemma 1.10.5. *Let G be a finite group, p a prime and S a p-subgroup of G. Then $S \in \mathrm{Syl}_p(G)$ if and only if $N_G(S)/S$ has a non-trivial p-subgroup.*

Proof. We will prove the contrapositive.

Suppose first that $S \notin \mathrm{Syl}_p(G)$. Then there exists a p-subgroup T of G with $S \lneq T$. Then by 1.7.38, $S \lneq N_T(S)$. Thus $N_T(S)/S$ is a non-trivial p-subgroup of $N_G(S)/S$.

Suppose A is a non-trivial p-subgroup of $N_G(S)$. Let T be the inverse image of A under the natural homomorphism from $N_G(S) \to N_G(S)/S$. Then T is a subgroup of G and $|T| = |T/S||S| = |A||S|$. Thus T is a p-subgroup of G with $S \neq T$. Hence S is not a Sylow p-subgroup. □

Lemma 1.10.6. *Let I and J be sets. Then* $\mathrm{Sym}(I)$ *acts on J^I via $\pi * f = f \circ \pi^{-1}$ for all $\pi \in$* $\mathrm{Sym}(I)$ *and $f \in J^I$.*

Proof. Readily verified. □

Proposition 1.10.7 (Cauchy)**.** *If p divides $|G|$, then G has an element of order p*

Proof. Let $x = (1, 2, \ldots, p) \in \mathrm{Sym}(p)$ and $X = \langle x \rangle$. Then X is a subgroup order p of $\mathrm{Sym}(p)$. By 1.10.6 $\mathrm{Sym}(p)$ acts on G^p and so also X acts on G^p. Observe that

$$x * (a_1, \ldots, a_p) = (a_p, a_1 \ldots, a_{p-1})$$

Consider the subset

$$T = \{(a_1, \dots, a_p) \in G^p \mid a_1 a_2 \dots a_p = e\}.$$

of G^p Note that we can choose the first $p-1$ coordinates freely and then the last one is uniquely determined. So $|T| = |G|^{p-1}$.

We claim that T is X-invariant. For this note that

$$a_p a_1 \dots a_{p-1} = {}^{a_p}(a_1 \dots a_p)$$

Si if $a_1 \dots a_p = e$ also $a_p a_1 \dots a_{p-1} = e$. Thus $x \in N_X(S)$ and so also $X \leq N_G(S)$. Hence T is indeed X-invariant and so X acts on T.

From 1.7.31 we have

$$|T| \equiv |\mathrm{Fix}_T(X)| \pmod p$$

As p divides $|G|$, it divides $|T|$ and so also $|\mathrm{Fix}_T(X)|$. Hence there exists some $(a_1, a_2, \dots a_p) \in \mathrm{Fix}_S(X)$ distinct from $(e, e, \dots, e)$. But being in $\mathrm{Fix}_S(X)$ just means $a_1 = a_2 = \dots a_p$. Being in S implies $a_1^p = a_1 a_2 \dots a_p = e$. Therefore a_1 has order p. □

The following easy lemma is crucial for our approach to the theory of Sylow p-subgroups.

Lemma 1.10.8. *Let $P \in \mathrm{Syl}_p(G)$ and $\alpha \in \mathrm{Aut}(G)$. Then $\alpha(P) \in \mathrm{Syl}_p(G)$. In particular, G acts on $\mathrm{Syl}_p(G)$ by conjugation.*

Proof. Since α is an bijection, $|P| = |\alpha(P)|$ and so $\alpha(P)$ is a p-group. Let Qbe a p-subgroup of G with $\alpha(P) \leq Q$. Then $\alpha^{-1}(Q)$ is a p-subgroup of G with $P \leq \alpha^{-1}(Q)$ and the maximality of P implies $P = \alpha^{-1}(Q)$. Thus $\alpha(P) = Q$ and $\alpha(P)$ is indeed a maximal p-subgroup of G.

Let $g \in G$. Then ${}^gP = \mathrm{i}_g(P) \in \mathrm{Syl}_p(G)$. Thus $\mathrm{Syl}_p(G)$ is subset of $\mathcal{P}(G)$ invariant under the action by conjugation. Therefore G acts on $\mathrm{Syl}_p(G)$ be conjugation. □

Theorem 1.10.9 (Sylow's Theorem)**.** *Let G be a finite group, p a prime and $P \in \mathrm{Syl}_p(G)$.*

(a) All Sylow p-subgroups are conjugate in G.

(b) $|\mathrm{Syl}_p(G)| = |G/\mathrm{N}_G(P)| \equiv 1 \pmod p$.

(c) $|P| = |G|_p$.

Proof. Let $\mathcal{S} = {}^GP := \{{}^gP \mid g \in G\}$. So $\mathcal{S}$ is the set of Sylow p-subgroups conjugate to P. First we show

1°. *P has a unique fixed-point on $\mathcal{S}$ and on $\mathrm{Syl}_p(G)$, namely P itself*

Indeed, suppose that P fixes $Q \in \mathrm{Syl}_p(G)$. Then $P \leq \mathrm{N}_G(Q)$ and PQ is a subgroup of G. Now $|PQ| = \frac{|P||Q|}{|P \cap Q|}$ and so PQ is a p-group. Hence by maximality of P and Q, $P = PQ = Q$.

2°. $\mathcal{S} \equiv 1 \pmod p$.

By (1°) $\mathrm{Fix}_{\mathcal{S}}(P) = 1$ and by Fixed-Point Formula 1.7.31 $|\mathcal{S}| \equiv |\mathrm{Fix}_{\mathcal{S}}(G)| \pmod p$. So (2°) holds.

3°. $\mathrm{Syl}_p(G) = \mathcal{S}$ *and so (a) holds*

Let $Q \in \mathrm{Syl}_p(G)$. Then $|\mathrm{Fix}_{\mathcal{S}}(Q)| \equiv |\mathcal{S}| \equiv 1 \pmod p$. Hence Q has a fixed-point $T \in \mathcal{S}$. By (2°) applied to Q, this fixed-point is Q. So $Q = T \in \mathcal{S}$.

4°. *(b) holds.*

By (2°) and (5°) $|\mathrm{Syl}_p(G)| = |\mathcal{S}| \equiv 1 \pmod p$. Note that $\mathrm{N}\, N_G(P)$ is the stabilizer of P in G with respect to conjugation. As G is transitive on $\mathcal{S}$ we conclude from 1.7.20(c) that $|\mathcal{S}| = |G/\mathrm{N}_G(P)|$. Thus (b) holds.

5°. *p does not divides* $|\,\mathrm{N}_G(P)/P|$.

By 1.10.5 $\mathrm{N}_G(P)/P$ has no non-trivial p-subgroup and so by Cauchy's theorem $|\,\mathrm{N}_G(P)/P$ is not divisible by p.

By (b) and (5°), p divides neither $|G/\mathrm{N}_G(P)|$ nor $|\,\mathrm{N}_G(P)/P|$. Since

$$|G| = |G/\mathrm{N}_G(P)| \cdot |\,\mathrm{N}_G(P)/P| \cdot |P|$$

we get that p does not divide $|G/P|$. Hence $|G|_p$ divides $|P|$. By Lagrange's $|P|$ divides $|G|$ and so also $|G|_p$. Thus $|P| = |G|_p$. and (c) holds. □

Corollary 1.10.10. *Let G be a finite group, p a prime and* $P \in \mathrm{Syl}_p(G)$

(a) Let Q be a p-subgroup of G. Then $Q \in \mathrm{Syl}_p(G)$ if and only if $|Q| = |G|_p$ and if and only if p does not divide $|G/Q|$.

(b) Let $R \leq H \leq G$ with $p \nmid |G/H|$. Then $R \in \mathrm{Syl}_p(H)$ if and only if $R \in \mathrm{Syl}_p(G)$.

(c) $P \trianglelefteq G$ if and only if P is the unique Sylow p-subgroup of G.

(d) Let $s_p := |\mathrm{Syl}_p(G)|$. Then s_p divides $\frac{|G|}{|G|_p}$,$s_p \equiv 1 \pmod p$ and $s_p|G_p|$ divides $|G|$.

Proof. (a) Since $|Q|$ is a power of p, $|Q| = |G|_p$ if and only if p does not divide $\frac{|G|}{|Q|}$. If $|Q| = |G|_p$ then by 1.10.3(b), $Q \in \mathrm{Syl}_p(G)$ and if $Q \in \mathrm{Syl}_p(G)$ then by 1.10.9(c), $|Q| = |G|_p$.

(b) Note that $|H|_p = |G|_p$ and so (b) follows from (c).

(c) Since all Sylow p-subgroups are conjugate, $\mathrm{Syl}_p(G) = \{{}^gP \mid g \in G\}$. Hence $\mathrm{Syl}_p(G) = \{P\}$ if and only if $P = {}^gP$ for all $g \in G$.

(d) By 1.10.9(b), $s_p = |G/\mathrm{N}_G(P)| \equiv 1 \pmod p$. Also

$$\frac{|G|}{|G|_p} = \frac{|G|}{|P|} = \frac{|G|}{|\mathrm{N}_G(P)|}\frac{|\,\mathrm{N}_G(P)|}{|P|} = s_p \cdot \frac{|\,\mathrm{N}_G(P)|}{|P|}$$

So s_p divides $\frac{|G|}{|G|_p}$. □

Lemma 1.10.11. *Let G be a finite group, p a prime $M \trianglelefteq G$.*

(a) Let $H \leq G$. Then $H \in \mathrm{Syl}_p(G)$ if and only if $HM/M \in \mathrm{Syl}_p(G)$ and $H \cap M \in \mathrm{Syl}_p(G)$.

(b) Let $\pi : G \to M, g \to gM$ be the natural homomorphism and for $R \leq G$ let $\hat{R} = \pi^{-1}(R)$. Put

$$\mathcal{A} = \{(R, Q) \mid R \in \mathrm{Syl}_p(G/M), Q \in \mathrm{Syl}_p(\hat{R})\}.$$

Then

$$\alpha : \mathrm{Syl}_p(G) \to \mathcal{A}, \quad P \to (PM/M, P)$$

is a well-defined bijection.

(c) Let $P \in \mathrm{Syl}_p(G)$. Then $|\mathrm{Syl}_p(G)| = |\mathrm{Syl}_p(G/M)| \cdot |\mathrm{Syl}_p(PM)|$

Proof. (a) Note that $|H| = |H/H \cap M||H \cap M| = |HM/M||H \cap M|$ and $|G|_p = |G/M|_p|M|_p$. It follows that $|H|_p = |G|_p$ if and only if $|HM/M|_p = |G/M|_p$ and $|H \cap M|_p = |M_p|$. So (a) holds.

(b) By (a) $PM/M \in \mathrm{Syl}_p(G/M)$ also $P \in \mathrm{Syl}_p(PM)$ and so α is well defined. Clearly α is 1-1. Let $R \in \mathrm{Syl}_p(G/M)$ and $Q \in \mathrm{Syl}_p(\hat{R})$. Since $|\hat{R}| = |R||M|$,

$$|Q| = |\hat{R}|_p = |R|_p|M|_p = |G/M|_p|M|_p = |G|_p$$

So $Q \in \mathrm{Syl}_p(M)$. By (a) $QM/M \in \mathrm{Syl}_p(\hat{R}/M) = R$ and since R is a p-group, $QM/M = R$. Thus $\alpha(Q) = (QM/M, Q) = (R, Q)$ and α is onto.

By (b) $|\mathrm{Syl}_p(G)| = |\mathcal{A}|$. Let $R, T \in \mathrm{Syl}_p(G/M)$. Then $R = {}^aT$ for some $a \in G/M$. Let $a = gM$ with $g \in G$. Then $\hat{R} = {}^g\hat{T}$ and since conjugation is an automorphism, $|\mathrm{Syl}_p(\hat{R})| = |\mathrm{Syl}_p(\hat{T})| = |\mathrm{Syl}_p(PM)|$. Thus

$$|\mathrm{Syl}_p(G)| = |\mathcal{A}| = \sum_{R \in \mathrm{Syl}_p(G/M)} |\mathrm{Syl}_p(\hat{R})| = \sum_{R \in \mathrm{Syl}_p(G/M)} |\mathrm{Syl}_p(PM)| = |\mathrm{Syl}_p(G/M)| \cdot |Syl_p(PM)|$$

□

Lemma 1.10.12. *Let G be a finite group, p a prime, $P \in \mathrm{Syl}_p(G)$ and $M \trianglelefteq G$. Then the following statements are equivalent*

(a) $M \leq \mathrm{Stab}_G(\mathrm{Syl}_p(G))$

(b) $P \trianglelefteq PM$.

(c) P is the unique Sylow p-subgroup of PM.

(d) $|\mathrm{Syl}_p(G)| = |\mathrm{Syl}_p(G/M)|$

(e) The map

$$\beta : \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G/M) \quad Q \to QM/M$$

is a bijection.

Proof. (a) $\Longrightarrow$ (b): If $M \leq \mathrm{Stab}_G(\mathrm{Syl}_p(G))$, then $M \leq \mathrm{N}_G(P)$. Since also $P \leq \mathrm{N}_G(P)$ we conclude that $PN \leq \mathrm{N})G(P)$ and so $P \trianglelefteq PN$.

(b) $\Longrightarrow$ (c): If $P \trianglelefteq PM$, 1.10.10(c) shows that P is the unique Sylow p-subgroup of G.

(c) $\Longrightarrow$ (d): If P is the unique Sylpw p-subgroup of PM, then $|Syl_p(PM)| = 1$ and so by 1.10.11(c)

$$|\mathrm{Syl}_p(G)| = |\mathrm{Syl}_p(G/M)| \cdot |\mathrm{Syl}_p(PM)| = |\mathrm{Syl}_p(G/M)|$$

(d) $\Longrightarrow$ (e): Since the map α in 1.10.11(c) is a bijection, β is onto. So if $|\mathrm{Syl}_p(G)| = |\mathrm{Syl}_p(G/M)|, \beta$ is a bijection.

(e) $\Longrightarrow$ (a): Suppose β is a bijection. Let $m \in M$. Then $P^m M = PM$ and since β is 1-1, $P^m = P$. So M fixes all $P \in n\mathrm{Syl}_p(G)$, that is $M \leq \mathrm{Stab}_G(\mathrm{Syl}_p(G))$. □

Lemma 1.10.13. *Let G be a finite group, p a prime, $P \in \mathrm{Syl}_p(G)$ and $M \trianglelefteq G$ with $M \leq \mathrm{Stab}_G(\mathrm{Syl}_p(G))$. Then*

(a) $P \cap M \trianglelefteq G$.

(b) $PM \trianglelefteq G$ if and only of $P \trianglelefteq G$ and if and only if $P \leq \mathrm{Stab}_G(\mathrm{Syl}_p(G))$.

Proof. (a) By 1.10.12 $P \trianglelefteq MP$. Since $M \trianglelefteq G$ this gives $M \cap P \trianglelefteq M$. By 1.10.11 $P \cap M \in \mathrm{Syl}_p(M)$ and so by So by 1.10.10(c), $M \cap P$ is the only Sylow p-subgroup of N. Let $g \in G$. Then by 1.10.8 ${}^gN \cap P$ is a Sylow p-subgroup of M and so equal to $M \cap P$. Thus $M \cap P \trianglelefteq G$.

(b) Suppose that $PM \trianglelefteq G$. By 1.10.12 P is the only Sylow p-subgroup of PM and so $P \trianglelefteq G$. Suppose that $P \trianglelefteq G$. The $\mathrm{Syl}_p(G) = \{P\}$ and so $P \leq G = \mathrm{Stab}_G(\mathrm{Syl}_p(G))$. Put $\tilde{M} = \mathrm{Stab}_G(\mathrm{Syl}_p(G))$. If $P \leq \tilde{M}$, then $P\tilde{M} = \tilde{M} \trianglelefteq G$ and so $P \trianglelefteq G$. □

Lemma 1.10.14. *Let G be a finite group of order* $2n$ *with n odd. Then G index a normal subgroup of index* 2*.*

Proof. By Cayley's Theorem 1.7.8(1), G is isomorphic to $G^\cdot$, (the image of G in $\mathrm{Sym}(G)$ under the homomorphism $\Phi^\cdot$ corresponding the action $\cdot$ of G and G by left multiplication. Let $t \in G$ be an element of order 2. Since $tg \neq g$ for all $g \in G$, t and so also $t^\cdot = \Phi^\cdot(t)$ has no fixed-points on G. Hence $t^\cdot$ has n-cycles of length 2 and so $t^\cdot$ is an odd permutation. Thus $G^\cdot \nleq \mathrm{Alt}(G)$ and $G^\cdot \cap \mathrm{Alt}(G)$ is normal subgroup of index 2 in $G^\cdot$. □

The following lemma is an example how the actions on a subgroup can be used to identify the subgroup.

Lemma 1.10.15. *Let n be an integer with $n \geq 3$. Let $G = \mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$ and suppose $*$ is a faithful action of G in the set I with $|I| \leq n$. Then*

(a) *If $G = \mathrm{Sym}(n)$, then $G^* = \mathrm{Sym}(I)$ and $\mathrm{Stab}_G(i) \cong \mathrm{Stab}_G(i)^* = \mathrm{Stab}_{\mathrm{Sym}(I)}(i) \cong \mathrm{Sym}(n-1)$ for all $i \in I$.*

(b) *If $G = \mathrm{Alt}(n)$, then $G^* = \mathrm{Alt}(I)$ and $\mathrm{Stab}_G(i) \cong \mathrm{Stab}_G(i)^* = \mathrm{Stab}_{\mathrm{Alt}(I)}(i) \cong \mathrm{Alt}(n-1)$ for all $i \in I$.*

Proof. By assumption, G acts faithfully on I and so G is isomorphic to the subgroup G^* of $\mathrm{Sym}(I)$. In particular, $|G^*| = |G|$ and so

$$|I|! = |\mathrm{Sym}(I)| \geq |G^*| = |G| \geq \frac{n!}{2}.$$

Since $|I| \leq n$ and $n \geq 3$ this gives $|I| = n$ and $|\mathrm{Sym}(I)| = |\mathrm{Sym}(n)|$.

Hence $|\mathrm{Sym}(I)/G^*| = |\mathrm{Sym}(n)/G| \leq 2$. By **??** $\mathrm{Alt}(I)$ is the unique subgroup of index two in $\mathrm{Sym}(I)$. Thus either $G = \mathrm{Sym}(n)$ and $G^* = \mathrm{Sym}(I)$ or $G = \mathrm{Alt}(n)$ and $G^* = \mathrm{Alt}(I)$. Let $i \in I$. Suppose $G = \mathrm{Alt}(n)$. Then

$$\mathrm{Stab}_G(i) \overset{\Phi_* \text{ 1-1}}{\cong} \mathrm{Stab}_G(i)^* \overset{1.7.10(\mathrm{g})}{=} \mathrm{Stab}_{G^*}(i) = \mathrm{Stab}_{\mathrm{Alt}(I)}(i) \cong \mathrm{Alt}(I \setminus \{i\}) \cong \mathrm{Alt}(n-1)$$

and similar statement with Alt replaced by Sym. So (a) and (b) holds. □

Corollary 1.10.16. *Let H be a finite group of order 60 with exactly six Sylow 5-subgroups. Then $H \cong \mathrm{Alt}(5)$.*

Proof. By **??** we may assume that H is a subgroup of $G = \mathrm{Alt}(6)$. Let $I = G/H$ and $i = H \in I$. Note that G acts on I be left multiplication and $H = \mathrm{Stab}_G(i)$. Put $M = \mathrm{Stab}_G(I)$. Then $M \leq \mathrm{Stab}_G(i) = H$. By **??** H is simple and so $M = 1$ or $M = H$.

If $M = H$, then $H \trianglelefteq G$ and since $5 \nmid G/H$, $\mathrm{Syl}_5(G) = \mathrm{Syl}_5(H)$. But $\mathrm{Alt}(6)$ has $\frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{5} = 36 \cdot 4$ 5-cycles and so $\frac{36 \cdot 4}{5-1} = 36$ Sylow 5 subgroups, a contradiction since H has only 6 Sylow 5-subgroups.

Thus $M = 1$. Hence G acts faithfully on I and since $|I| = \frac{|G|}{|H|} = 6$, 1.10.15 shows that $H = \mathrm{Stab}_G(i) \cong \mathrm{Alt}(5)$. □

Lemma 1.10.17. (a) *Let G be a group of order 12. Then either G has unique Sylow 3-subgroup or $G \cong \mathrm{Alt}(4)$.*

(b) *Let G be group of order 15. Then $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.*

(c) *Let G be a group of order 30. Then G has a unique Sylow 3-subgroup and a unique Sylow 5-subgroup.*

Proof. (a) By **??**a the number of Sylow 3 subgroups divides $\frac{12}{3}$ is $1 \pmod 3$. Thus $|\mathrm{Syl}_3(G)| = 1$ or 4. In the first case we are done. In the second case let $N = \mathrm{Stab}_G(\mathrm{Syl}_3(G))$. By **??**, G/N still has 4 Sylow 3-subgroups. Thus $|G/N| \geq 4 \cdot 3 = 12 = |G|$, $N = \{e\}$ and G is isomorphic to a subgroup of order 12 in $\mathrm{Sym}(4)$. Such a subgroup is normal and so $G \cong \mathrm{Alt}(4)$ by 1.11.9.

(b) The numbers of Sylow 5-subgroups is $1 \pmod 5$ and divides $\frac{15}{3} = 5$. Thus G has a unique Sylow 5-subgroup S_5. Also the number of Sylow 3 subgroups is $1 \pmod 3$ and divides $\frac{15}{3} = 5$. Thus G has a unique Sylow 3-subgroup S_3. Then $S_3 \cap S_5 = 1$, $|S_3S_5| = 15$ and so $G = S_3S_5$. Hence by 1.9.12

$$G \cong S_3 \times S_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$$

where the latter isomorphism holds since we just proved that any group of order 15 is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

(c) By 1.10.14 any group which as order twice an odd number has a normal subgroup of index two. Hence G has a normal subgroup of order 15. This normal subgroup contains all the Sylow 3 and Sylow 5-subgroups of G and so (c) follows from (b). □

Lemma 1.10.18. *Let G be a group of order 120. Then one of the following holds:*

(a) G has a unique Sylow 5*-subgroup.*

(b) $G \cong \mathrm{Sym}(5)$.

(c) $|\mathrm{Z}(G)| = 2$ *and* $G/\mathrm{Z}(G) \cong \mathrm{Alt}(5)$.

Proof. Let $P \leq \mathrm{Syl}_5(G)$ and put $I = \mathrm{Syl}_5(G)$.

If $|I| = 1$, (a) holds.

So suppose that $|I| > 1$. Then by**??**(**??**), $|I| \equiv 1 \pmod 5$ and $|I|$ divides $|G/P| = 24$. The numbers which are larger than 1, are less or equal to 24 and are $1 \pmod 5$ are $1, 6, 11, 16$ and 21. Of these only 6 divides 24. Thus $|I| = 6$. Let $\phi : G \to \mathrm{Sym}(I)$ be the homomorphism corresponding to the action of G on I. Put $N = \ker \phi$ and $H = \phi(G)$. Then H is subgroup of $\mathrm{Sym}(I) \cong \mathrm{Sym}(6)$ and $H \cong G/N$. By **??**(**??**), G/N (and so also H) has exactly six Sylow 5-subgroups. In particular the order of H is a multiple of 30. By 1.10.17c, $|H| \neq 30$.

Suppose that $|H| = 120$. Then $N = 1$ and so $G \cong H$ in this case. Now $H \leq \mathrm{Sym}(I) \cong \mathrm{Sym}(6)$. Thus 1.10.15(a) implies $G \cong H \cong \mathrm{Sym}(5)$.

Suppose next that $|H| = 60$. If $H \nleq \mathrm{Alt}(I)$, then $H \cap \mathrm{Alt}(I)$ is a group of order 30 with six Sylow 5-subgroups, a contradiction to 1.10.17. Thus $H \leq \mathrm{Alt}(I) \cong Alt(6)$. So by 1.10.15(b), $H \cong \mathrm{Alt}(5)$. Since $|N| = 2$ and $N \trianglelefteq G$, $N \leq \mathrm{Z}(G)$. Also $\phi(\mathrm{Z}(G))$ is a abelian normal subgroup of $H \cong \mathrm{Alt}(5)$ and so $\phi(\mathrm{Z}(G)) = e$. Hence $N = \mathrm{Z}(G)$ and

$$G/\mathrm{Z}(G) = G/N \cong H \cong \mathrm{Alt}(5).$$

□

1.11 Normal Subgroups of Symmetric Groups

In this section we will investigate the normal subgroups of symmetric group $\mathrm{Sym}(n)$, n a positive integer. We start by defining a particular normal subgroup called the alternating group $\mathrm{Alt}(n)$.

1.11.1 (Alternating Groups)**.** Put

$$e_i = (\delta_{ij})_{j=1}^n \in \mathbb{R}^n.$$

Then $(e_i \mid 1 \leq i \leq n)$ is a basis of $\mathbb{R}^n$. So for $\pi \in \mathrm{Sym}(n)$ we can define $\alpha(\pi) \in GL_n(\mathbb{R})$ by $\alpha(\pi)(e_i) = e_{\pi(i)}$ for all $1 \leq i \leq n$. Define $\alpha : \mathrm{Sym}(n) \to \mathrm{GL}_n(\mathbb{R}), \pi \to \alpha(\pi)$. Let $\pi, \mu \in \mathrm{Sym}(n)$ and $1 \leq i \leq n$. Then

$$\alpha(\mu \circ \pi)(e_i) = e_{\mu(\pi(i))} = \alpha(\mu)(e_{\pi(i)}) = \alpha(\mu)(\alpha(\pi)(e_i)) = (\alpha(\mu) \circ \alpha(\pi))(e_i).$$

So $\alpha(\mu \circ \pi) = \alpha(\mu) \circ \alpha(\pi)$ and α is a homomorphism. Now define $\mathrm{sgn} = \det \circ \alpha : \mathrm{Sym}(n) \to (\mathbb{R} \setminus \{0\}, \cdot), \pi \to \det(\alpha(\pi))$. Since both det and α are homomorphisms, sgn is a homomorphism. Also if $x = (i, j) \in \mathrm{Sym}(n)$ is a 2-cycle it is easy to see that $\det(\alpha(x)) = -1$.

Since

$$(a_1, a_2, \dots a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$$

and sgn is a homomorphism,

$$\mathrm{sgn}((a_1, a_2, \dots a_k)) = \mathrm{sgn}((a_1, a_2))\mathrm{sgn}((a_2, a_3)) \dots \mathrm{sgn}((a_{k-1}, a_k)) = (-1)^{k-1}$$

Using that sgn is a homomorphism one more time we get

$$\mathrm{sgn}((a_{11}, a_{12}, \dots a_{1k_1})(a_{21}, a_{22}, \dots a_{2k_2}) \dots (a_{l1}, a_{l2}, \dots a_{lk_l})) = (-1)^{k_1-1}(-1)^{k_2-1} \dots (-1)^{k_l-1}$$

This implies

$$\mathrm{sgn}(x) = \begin{cases} 1 & \text{if } x \text{ has an even number of even cycles} \\ -1 & \text{if } x \text{ has an odd number of even cycles} \end{cases}$$

An permutation π with $\mathrm{sgn}\pi = 1$ is called an *even permutation* and a permutation with $\mathrm{sgn}(\pi) = -1$ is called an *odd permutation*.

Define $\mathrm{Alt}(n) = \ker \mathrm{sgn}$. Then $\mathrm{Alt}(n)$ is a normal subgroup of $\mathrm{Sym}(n)$, $\mathrm{Alt}(n)$ consists of all permutation which have an even number of even cycles and if $n \geq 2$,

$$\mathrm{Sym}(n)/\mathrm{Alt}(n) \cong \mathrm{sgn}(\mathrm{Sym}(n)) = \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}.$$

In particular,

$$|\mathrm{Alt}(n)| = \frac{n!}{2}$$

for all $n \geq 2$.

We have $\mathrm{Alt}(2) = \{(1)\}$.

$$\mathrm{Alt}(3) = \{(1), (1, 2, 3), (1, 3, 2)\}$$

and

$$\mathrm{Alt}(4) = \{(1),(1,2,3),(1,3,2),(1,2,4),(1,4,2),(1,3,4),(1,4,3),(2,3,4),(2,4,3)$$
$$(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$$

Before continuing to investigate the normal subgroup of $\mathrm{Sym}(n)$ we introduce conjugacy classes in arbitrary groups.

Definition 1.11.2. *We say that two elements x, y in G are* conjugate *in G if $y = {}^{g}x = gxg^{-1}$ for some $g \in G$. It is an easy exercise to verify that this is an equivalence relation. The equivalence classes are called the* conjugacy classes *of G. The conjugacy class containing x is ${}^{G}x := \{x^{g} \mid g \in G\}$.*

Proposition 1.11.3. *A subgroup of G is normal if and only if it is the union of conjugacy classes of G.*

Proof. Let $N \leq G$. The following are clearly equivalent:

$$N \trianglelefteq G$$
$${}^{g}n \in N \text{ for all } n \in N, g \in G$$
$${}^{G}n \subseteq N \text{ for all } n \in N$$
$$N = \bigcup_{n \in N} {}^{G}n$$
$$N \text{ is a union of conjugacy classes}$$

□

1.11.4 (Normal sugroups of Sym(3))**.** Lets now investigate the normal subgroups of $\mathrm{Sym}(3)$. We start by listing the conjugacy classes

e	1 element
$(123),(132)$	2 elements
$(12),(13),(23)$	3 elements

Let $e \neq N \trianglelefteq \mathrm{Sym}(3)$. If N contains the 2-cycles, then $|N| \geq 4$. Since $|N|$ divides $|\mathrm{Sym}(3)| = 6$ we get $|N| = 6$ and $N = \mathrm{Sym}(3)$.

If N does not contain the 2-cycles we get $N = \{e,(123),(132)\} = \mathrm{Alt}(3)$.

So the normal subgroups of $\mathrm{Sym}(3)$ are

$$(1), \mathrm{Alt}(3), \text{ and } \mathrm{Sym}(3)$$

1.11.5 (Normal subgroups of $\mathrm{Sym}(4)$)**.** The conjugacy classes of $\mathrm{Sym}(4)$ are:

e	1 element
$(123),(132),(124),(142),(134),(143),(234),(243)$	8 elements
$(12)(34),(13)(24),(14)(23)$	3 elements
$(12),(13),(14),(23),(24),(34)$	6 elements
$(1234),(1243),(1324),(1342),(1423),(1432)$	6 elements

Let N be a proper normal subgroup of $\mathrm{Sym}(4)$. Then $|N|$ divides $24 = |\mathrm{Sym}(4)|$. Thus $|N| = 2,3,4,6,8$ or 12. So N contains $1,2,3,5,7$ or 11 non-trivial elements. As $N \setminus \{e\}$ is a union of conjugacy classes, $|N|-1$ is a sum of some of the numbers $3,6,6$ and 8. In particular, $|N|-1 \geq 3$ and so $|N|-1 \in \{3,5,7,11\}$. Thus $|N|-1$ is odd. Since 3 is the only of the possible summands which is odd, we conclude that 3 is one of the summands. So $K \subseteq N$, where $K = \{e,(12)(34),(13)(24),(14)(23)\}$. Then $|N \setminus K| \in \{0,3,8\}$ and $|N \setminus K|$ is a sum of some of the numbers $6,6$ and 8. It follows that $|N \setminus K| = 0$ or 8. In the first case $N = K$ and in the second case, N consist of K and the 3-cycles and so $N = \mathrm{Alt}(4)$. Note also that $(12)(34) \circ (13)(24) = (14)(23)$ and so K is indeed a normal subgroup of $\mathrm{Sym}(4)$.

Thus the normal subgroups of $\mathrm{Sym}(4)$ are

$$\{(1)\}, \quad \{(1),(12)(34),(13)(24),(14)(23)\}, \quad \mathrm{Alt}(4) \quad \text{and} \quad \mathrm{Sym}(4).$$

Let us determine the quotient group $\mathrm{Sym}(4)/K$. No non-trivial element of K fixes ”4”. So $\mathrm{Sym}(3) \cap K = \{e\}$ and

$$|\mathrm{Sym}(3)K| = \frac{|\mathrm{Sym}(3)||K|}{|\mathrm{Sym}(3) \cap K|} = \frac{6 \cdot 4}{1} = 24 = |\mathrm{Sym}(4)|.$$

Thus $\mathrm{Sym}(3)K = \mathrm{Sym}(4)$. And

$$Sym(4)/K = \mathrm{Sym}(3)K/K \cong \mathrm{Sym}(3)/(\mathrm{Sym}(3) \cap K) = \mathrm{Sym}(3)/\{e\} \cong \mathrm{Sym}(3)$$

So the quotient of $\mathrm{Sym}(4)$ by K is isomorphic to $\mathrm{Sym}(3)$.

Counting arguments as above can in theory be used to determine the normal subgroups in all the $\mathrm{Sym}(n)$'s, but we prefer to take a different approach.

Lemma 1.11.6. *(a)* $\mathrm{Alt}(n)$ *is the subgroup of* $\mathrm{Sym}(n)$ *generated by all the 3-cycles.*

(b) If $n \geq 5$ then $\mathrm{Alt}(n)$ *is the subgroup of* $\mathrm{Sym}(n)$ *generated by all the double 2-cycles.*

(c) Let N be a normal subgroup of $\mathrm{Alt}(n)$ *containing a 3-cycle. Then* $N = \mathrm{Alt}(n)$.

(d) Let $n \geq 5$ and N a normal subgroup of $\mathrm{Alt}(n)$ *containing a double 2-cycle. Then* $N = \mathrm{Alt}(n)$.

Proof. (a) By induction on n. If $n \leq 2$, then $\mathrm{Alt}(n) = \{(1)\}$ and (a) holds . So we may assume $n \geq 3$. Let H be the subgroup of $\mathrm{Sym}(n)$ generated by all the 3-cycles. Then $H \leq \mathrm{Alt}(n)$ and by induction $\mathrm{Alt}(n-1) \leq H$. Let $g \in \mathrm{Alt}(n)$. If $g(n) = n$, $n \in \mathrm{Alt}(n-1) \leq H$. So suppose $g(n) \neq n$. Since $n \geq 3$, there exists $1 \leq a \leq n$ with $a \neq n$ and $a \neq g(n)$. Let h be the 3-cycle $(g(n), n, a)$. Then $(hg)(n) = h(g(n)) = n$. Hence $hg \in Alt(n-1) \leq H$ and so also $g = h^{-1}(hg) \in H$. We proved that $g \in H$ and so $\mathrm{Alt}(n) \leq H$ and $H = \mathrm{Alt}(n)$.

(b) Let $h = (a,b,c)$ be a 3-cycle in $\mathrm{Sym}(n)$. Since $n \geq 5$, there exist $1 \leq d < e \leq n$ distinct from a, b and c. Note that

$$(a,b,c) = (a,b)(d,e) \circ (b,c)(d,e)$$

and so the subgroup generated by the double 2-cycles contains all the 3-cycles. Hence (b) follows from (a).

(c) Let $h = (a,b,c)$ be a 3-cycle in N and g any 3-cycle in $\mathrm{Sym}(n)$. By (a) it suffices to prove that $g \in N$. Since all 3-cycles are conjugate in $\mathrm{Sym}(n)$ there exists $t \in \mathrm{Sym}(n)$ with ${}^t h = g$. If $t \in \mathrm{Alt}(n)$ we get $g = {}^t h \in N$, as N is normal in $\mathrm{Alt}(n)$.

So suppose that $t \notin \mathrm{Alt}(n)$. Then $t(a,b) \in \mathrm{Alt}(n)$. Note that $h^{-1} = (c,b,a) = (b,a,c)$ and so ${}^{(a,b)}(h^{-1}) = {}^{(a,b)}(b,a,c) = (a,b,c) = h$. Thus

$${}^{t(a,b)}(h^{-1}) = {}^{t}({}^{(a,b)}(h^{-1})) = {}^t h = g$$

As the left hand side is in N we get $g \in N$.

(d) This is very similar to (c) : Let $h = (a,b)(c,d)$ be a double 2-cycle in N and let g be any double 2-cycle in $\mathrm{Sym}(n)$. Then $g = {}^t h$ for some $t \in \mathrm{Sym}(n)$. Note that also $g = {}^{t(a,b)}h$ and either $t \in \mathrm{Alt}(n)$ or $t(a,b) \in \mathrm{Alt}(n)$. Since $N \trianglelefteq \mathrm{Alt}(n)$ we conclude that $g \in N$ and so by (b), $N = \mathrm{Alt}(n)$. □

Definition 1.11.7. *Let G be a group. Then G is called* simple *if* $G \neq \{e\}$ *and* $\{e\}$ *and G are the only normal subgroup of G.*

Proposition 1.11.8. *Let* $n \geq 5$. *Then* $\mathrm{Alt}(n)$ *is simple.*

Proof. If $n > 5$ we assume by induction that $\mathrm{Alt}(n-1)$ is simple. Let N be a non-trivial normal subgroup of $\mathrm{Alt}(n)$.

Case 1. *N contains an element* $g \neq e$ *with* $g(i) = i$ *for some* $1 \leq i \leq n$.

Let $H = \{h \in \mathrm{Alt}(n) \mid h(i) = i\}$. Then $H \cong \mathrm{Alt}(n-1)$, $g \in H \cap N$ and so $H \cap N$ is a non-trivial normal subgroup.

We claim that $H \cap N$ contains a 3-cycle or a double 2-cycle. Indeed if $n = 5$, then $n - 1 = 4$ and the claim holds as every non-trivial element in $\mathrm{Alt}(4)$ is either a 3-cycle or a double 2-cycle. So suppose that $n > 5$. Then by the induction assumption $H \cong \mathrm{Alt}(n-1)$ is simple. Since $H \cap N$ is a non-trivial normal subgroup of H, this implies $H \cap N = H$ and again the claim holds.

By the claim N contains a 3-cyle or a double 2-cycle. So by 1.11.6(c),d we conclude $N = \mathrm{Alt}(n)$.

Case 2. *N contains an element g with a cycle of length at least* 3.

Let $(a, b, c, \dots)$ be a cycle of g of length at least 3. Let $1 \leq d \leq n$ be distinct from a, b and c. Put $h = {}^{(adc)}g$. Then h has the cycle $(d, b, a, \dots)$. Also as N is normal in $\mathrm{Alt}(n)$, $h \in N$. So also $hg \in N$.

We compute $(hg)(a) = h(b) = a$ and $(hg)(b) = h(c) \neq h(d) = b$. So $hg \neq (1)$. Hence by (Case 1) (applied to hg in place of g), $N = \mathrm{Alt}(n)$.

Case 3. *N contains an element g with at least two 2-cycles.*

Such a g has the form $(ab)(cd)t$ where t is a product of cycles disjoint from $\{a, b, c, d\}$. Put $h = {}^{(abc)}g$. Then $h = (bc)(ad)t$. Thus

$$gh^{-1} = (ab)(cd)tt^{-1}(bc)(ad) = (ac)(bd).$$

As h and gh^{-1} are in N, (Case 1) (or 1.11.6(d)) shows that $N = \mathrm{Alt}(n)$.

Now let $e \neq g \in N$. As $n \geq 4$, g must fulfill one of the three above cases and so $N = \mathrm{Alt}(n)$. □

Proposition 1.11.9. *Let $N \trianglelefteq \mathrm{Sym}(n)$. Then either $N = \{e\}, \mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$, or $n = 4$ and $N = \{e, (12)(34), (13)(24), (14)(23)\}$.*

Proof. For $n \leq 2$, this is obvious. For $n = 3$ see 1.11.4 and for $n = 4$ see 1.11.5. So suppose $n \geq 5$. Then $N \cap \mathrm{Alt}(n)$ is a normal subgroup of $\mathrm{Alt}(n)$ and so by 1.11.8, $N \cap \mathrm{Alt}(n) = \mathrm{Alt}(n)$ or $\{e\}$.

In the first case $\mathrm{Alt}(n) \leq N \leq \mathrm{Sym}(n)$. Since $|\mathrm{Sym}(n)/\mathrm{Alt}(n)| = 2$, we conclude $N = \mathrm{Alt}(n)$ or $N = \mathrm{Sym}(n)$.

In the second case we get

$$|N| = |N/N \cap \mathrm{Alt}(n)| = |N\mathrm{Alt}(n)/Alt(n)| \leq |\mathrm{Sym}(n)\mathrm{Alt}(n)| \leq 2.$$

Suppose that $|N| = 2$ and let $e \neq n \in N$. As $n^2 = e$, n has a 2-cycle (ab). Let $a \neq c \neq b$ with $1 \leq c \leq n$. The ${}^{(abc)}n$ has cycle (bc) and so $n \neq {}^{(abc)}n$. A contradiction to $N = \{e, n\}$ and $N \trianglelefteq \mathrm{Sym}(n)$. □

Lemma 1.11.10. *The abelian simple groups are exactly cyclic groups of prime order.*

Proof. Let A be an abelian simple group and $e \neq a \in A$. Then $\langle a \rangle \trianglelefteq A$ and so $A = \langle a \rangle$ is cyclic. Hence $A \cong \mathbb{Z}/m\mathbb{Z}$ for some $m \geq 0$. If $m = 0$, $2\mathbb{Z}$ is a normal subgroup. Hence $m > 0$. If m is not a prime we can pick a divisor $1 < k < m$. But then $k\mathbb{Z}/m\mathbb{Z}$ is a proper normal subgroup. □

1.12 Coproducts and free groups

Having looked at the direct product and direct sum of groups we now define the coproduct of a family of groups:

Definition 1.12.1. *Let $(G_i)_{i \in I}$ be a family of groups. A* coproduct *of $(G_i)_{i \in I}$ is a pair $\left(G, (\rho_i)_{i \in I}\right)$, where G is a group and each ρ_i, $i \in I$, is homomorphism from G_i to G, with the following property:*

Whenever H is a group and $(\alpha_i : G_i \to H)_{i \in I}$ a family of homomorphisms, then there exists a unique homomorphism $\alpha : G \to H$ with $\alpha_i = \alpha \circ \rho_i$ for all $i \in I$.

As usual we summarize the definition in a commutative diagram:

$$\begin{tikzcd}
H & & G \arrow[ll, "\exists!\,\alpha"'] \\
& G_i \arrow[ul, "\alpha_i"] \arrow[ur, "\rho_i"'] &
\end{tikzcd}$$

On an intuitive level this group is the largest group which contains the G_i's and is generated by them. Notice also that the defintion of the coproduct is nearly identical to the defintion of the direct product. The difference is that all the arrows are reversed, that is a map fro A to B is replaced by a map from B to A. But it turns out the the coproduct is much harder to construct. We will proceed in three steps:

Step 1 Construction of coproduct X set-theoretic coproduct of $(G_i)_{i\in I}$.

Step 2 Construction of the free monoid W for X.

Step 3 Definition of an equivalence relation $\approx$ on W.

The coproduct then will defined as $W/\approx$.

Definition 1.12.2. *Let $(S_i)_{i\in I}$ be a family of sets. A (set-theoretic) coproduct of $(S_i)_{i\in I}$ of $(S_i)_{i\in I}$ is pair $\big(S, (\iota_i)_{i\in I}\big)$ where S is a set and each $\iota_i, i \in I$ is function $\iota_i : S_i \to S$, with the following property:*

Whenever T is a set and $(f_i : S_i \to T)_{i\in I}$ is a family of functions, then there exists a unique function $f : S \to T$ with $f_i = f \circ \iota_i$ for all $i \in I$.

$$\begin{tikzcd}
T & & S \arrow[ll, "\exists!\,f"'] \\
& S_i \arrow[ul, "f_i"] \arrow[ur, "\iota_i"'] &
\end{tikzcd}$$

Lemma 1.12.3. *Let $(S_i)_{i\in I}$ be a family of sets. Let $\big(S, (\iota_i)_{i\in I}\big)$ be a coproduct of $(S_i)_{i\in I}$, T a set and $(f_i : S_i \to T)$ a family of function. Let $f : S \to T$ be the unique function with $f_i = f \circ \iota_i$ for all $i \in I$. Then f is bijection, if and only if $(T, (f_i)_{i\in I})$ is a coproduct of $(S_i)_{i\in I}$.*

Proof. Let R be a set, $(g_i : S_i \to R)_{i\in I}$ a family of functions and $g : T \to R$ a function. Then

$$(*) \qquad g_i = g \circ f_i \text{ for all } i \in I$$

if and only if $g_i = (g \circ f) \circ \iota_i$ for all $i \in I$ and so if and only if

$$(**) \qquad g \circ f = h$$

where $h : S \to R$ is the unique function with $g = h \circ \iota_i$ for all $i \in I$.

If ι is a bijection, then $g = h^\circ f^{-1}$ is the unique function fulfilling (**) and so $(T, (f_i)_{i\in I})$ is a coproduct of $(S_i)_{i\in I}$.

Suppose now that $(T, (f_i)_{i\in I})$ is a coproduct of $(S_i)_{i\in I}$. Then there exists a unique function $g : T \to S$ with $\iota_i = g \circ f_i$ for all $i \in I$. The unique function $h : S \to S$ with $\iota_i = h \circ \iota_i$ is $h = \mathrm{id}_S$. Since (*) is equivalent to (**) this shows that $g \circ f = \mathrm{id}_S$. By symmetry $f \circ g = \mathrm{id}_T$ and so f is a bijection. □

Definition 1.12.4. *Let $(S_i)_{i\in I}$ be a family of sets.*

(a)

$$\dot{\bigcup_{i\in I}} S_i = \{(s, i) \mid i \in I, s \in S_i\}$$

$\dot\bigcup_{i\in I} S_i$ is called the disjoint union of $(S_i)_{i\in I}$..

(b) We say that $(S_i)_{i\in I}$ is pairwise disjoint if $S_i \cap S_j = \varnothing$ for all $i, j \in I$ with $i \neq j$.

(c) Let S be a set. We say that S is the internal disjoint union of $(S_i)_{i\in I}$ and write

$$S = \overset{\text{int}}{\dot{\bigcup_{i\in I}}} S_i$$

if $S = \bigcup_{i\in I} S_i$ and $(S_i)_{i\in I}$ is pairwise disjoint.

Lemma 1.12.5. *Let $(S_i)_{i\in I}$ be a set. Put $S = \dot\bigcup_{i\in I} S_i$ and for $i \in I$ define $\iota_i : S_i \to S, s \to (s, i)$. Then $\big(S, (\iota_i)_{i\in I}\big)$ is a set-theoretic coproduct of $(S_i)_{i\in I}$.*

Proof. Let T be a set and $(f_i : S_i \to T)$ be a family of function. Let $f : S \to T$ be a function. Then the following are equivalent:

$$\begin{array}{rccr}
 & f_i = f \circ \iota_i & & \text{for all } i \in I \\
\iff & f_i(s) = f(\iota_i(s)) & & \text{for all } i \in I, s \in S_i \\
\iff & f_i(s) = f(i, s) & & \text{for all } (i, s) \in S
\end{array}$$

Thus the function

$$f : S \to T, \quad (i, s) \to f_i(s)$$

is the unique function from S to I with $f_i = f \circ \iota_i$ for all $i \in I$. So $(S, (\iota_i)_{i\in I}$ is indeed a coproduct of $(S_i)_{i\in I}$. □

Lemma 1.12.6. *Let $(S_i)_{i\in I}$ be a family of subset of the set S. Define*

$$\iota : \dot{\bigcup_{i\in i}} S_i \to S, \quad (s, i) \to s$$

Then the following statements are equivalent *(a) For each $s \in S$ there exist a unique $i \in I$ with $s \in S_i$.*

(b) $S = \dot{\bigcup}^{\text{int}}_{i\in I} S_i$.

(c) ι is a bijection.

(d) $\big(S, (\mathrm{id}_{S_i})_{i\in I}\big)$ is a coproduct of $(S_i)_{i\in I}$.

Proof. (a) $\Longleftrightarrow$ (b) : The existence statement in (a) holds if and only if $S = \bigcup_{i\in I} S_i$. The uniqueness statement holds holds if and only if $S_i \cap S_j \neq \emptyset$ implies $i = j$, that is if and only if $(S_i)_{i\in I}$ is pairwise disjoint.

(b) $\Longleftrightarrow$ (c) : Let $s \in S$. Then $s = \iota(r, i)$ for some $(r, i) \in \dot{\bigcup}_{i\in I} S_i$ if and only if $s = r$ and $s \in S_i$ for some $i \in R$. Thus $\iota^{-1}(s) = \{(s, i) \mid i \in I, s \in S_i\}$. Hence ι is onto if and only if $S = \bigcup_{i\in I} S_i$ and ι is $1-1$ if and only if $S_i \cap S_j \neq \emptyset$ implies $i = j$.

(c) $\Longleftrightarrow$ (d) : By 1.12.3 (c) and (d) are equivalent. □

Definition 1.12.7. *Let I be a set. A free monoid for I is pair (W, ρ), where W is a monoid and $\rho : I \to W$ is a function, with the following property*

Whenever M is monoid and $\beta : I \to M$ is a function then there exists a unique homomorphism of monoids $\gamma : W \to M$ with $\beta = \gamma \circ \rho$.

$$\begin{tikzcd}
M & & W \arrow[ll, "\exists!\gamma"'] \\
& I \arrow[ul, "\beta"] \arrow[ur, "\rho"'] &
\end{tikzcd}$$

Proposition 1.12.8. *Let I be a set and let M_I be the set of all tuples $(i_1, i_2, \dots, i_n)$, where $n \in \mathbb{N}$ and $i_j \in I$ for all $1 \le j \le n$. For $i = (i_1, i_2, \dots, i_n)$ and $j = (j_1, \dots j_m)$ in M_I define*

$$ij = (i_1, i_2, \dots, i_n, j_1, \dots j_m)$$

Then

(a) M_I is a monoid.

(b) The map $\rho : I \to M_I, i \to (i)$ is 1-1.

(c) (M_I, ρ) is a free monoid for I.

Proof. (a) The binary operation is clearly associative and $()$ is an identity element.

(b) Obvious.

(c) Let M be a monoid and $\beta : I \to M$ a function. Define $\gamma((i_1, \dots, i_n)) = \beta(i_1)\beta(i_2)\dots\beta(i_n))$ where as usually the empty product is defined to be 1_M. This is clearly a homomorphism and $\beta = \gamma \circ \rho$.

Conversely if $\delta : M_I \to M$ is a homomorphism with $\beta = \delta \circ \rho$. Then

$$\delta\big((i_1, i_2, \dots i_n)\big) = \delta\big(\rho(i_1)\rho(i_2)\dots\rho(i_n)\big) = \delta\big(\rho(i_1)\big)\delta\big(\rho(i_2)\big)\dots\delta\big(\rho(i_n)\big) = \beta(i_1)\dots\beta(i_n)$$

So γ is a unique. Thus (M_I, ρ) is indeed a free monoid on I. □

Remark 1.12.9. *Let I be a set. By 1.12.8 there exists a free monoid (M_I, ρ) and ρ is 1-1. So we can identify $i \in I$ with $\rho(i)$ and obtain a free monoid of the form (M_I, id_I). Then each element $w \in M_I$ can be uniquely written as*

$$w = i_1 i_2 \dots i_n$$

with $n \in \mathbb{N}$ and $i_1, \dots, i_n \in I$. n is called the length of w and is denoted by $l(w)$. Moreover, the multiplication is given by

$$(i_1 \dots i_n)(j_1 \dots j_m) = i_1 \dots i_n j_1 \dots j_m$$

Lemma 1.12.10. *Let $(G, \cdot)$ be a magma, $\sim$ a relation on G and $\approx$ the equivalence relation on G generated by $\sim$. Suppose that $ab \approx ac$ and $ba \approx ca$ for all $a, b, c \in G$ with $b \sim c$.*

(a) The map $* : G/\!\approx \times G/\!\approx \to G/\!\approx, \quad ([a],[b]) \to [ab]$ is a well-defined binary operation.

(b) If $\cdot$ is associative, then $*$ is associative.

(c) If 1 is an identity in G, then $[1]$ is an identity in $G/\!\approx$.

(d) Suppose G is a monoid and H is a subset of G such

(i) G is generated by H as a monoid.

(ii) For each $h \in H$ there exists $h' \in G$ with $hh' \approx 1 \approx hh'$.

Then $G/\!\approx$ is a group.

Proof. (a) Let $a, b, c, d \in G$ with $a \approx c$ and $b \approx d$. Define $f : G \to G, x \to xb$. Since $x \sim y$ implies $xb \sim yb$, 1.5.5 shows that $a \approx c$ implies $ab \approx cb$. Choosing $f : G \to G, x \to cx$ instead, shows that $b \approx d$ implies $cb \approx cd$. Since $\approx$ is transitive this gives $ab \approx cd$ and so $*$ is well-defined.

(b) and (c) follows easily from the definition of $*$.

(d) Let $h \in H$. Then $[hh'] = [1] = [hh']$ and so $[h]$ is invertible in $G/\!\approx$. Put

$$K := \{g \in G \mid [g] \text{ is invertible in } G/\!\approx\}$$

Then $H \subseteq K$ and $e \in K$. let $a, b \in K$. Then by 1.2.3(d), $[ab] = [a][b]$ is invertible. Hence $ab \in K$ and K is a submonoid of G. Thus (d:i) implies $K = G$. Hence every $[g]$ for $g \in G$ is invertible. Together with (b) and (c) we conclude that $G/\!\approx$ is a group. □

Theorem 1.12.11. *Let $(G_i)_{i\in I}$ be a family of groups. Let $\big(X, (\iota_i)_{i\in I}\big)$ be coproduct of the family of sets $(G_i)_{i\in I}$ and put $G_i^\bullet = \iota_i(G_i)$. (So $X = \biguplus_{i\in I} G_i = \biguplus^{\mathrm{int}}_{i\in I} G_i^\bullet$). Let $1_i = \iota_i\big(1_{G_i}\big)$. Let (W, id_X) be a free monoid on X. We denote the binary operation on W by $*$ and the binary operation on $G_i^\bullet$ (for $i \in I$) by $\cdot$. Define the relation $\sim$ on W by $v \sim w$ if one of the following holds:*

(i) There exist $x, y \in W$, $i \in I$ and $a, b \in G_i^\bullet$ with $w = x * a * b * y$ and $v = x * \big(a \cdot b\big) * y$

(ii) There exists $x, y \in W$ and $i \in I$ with $w = x * 1_i * y$ and $v = x * y$.

Let $\approx$ be the equivalence relation on W generated by $\sim$. Then $W/\approx$ is a group under the well-defined operation

$$W/\approx \; \times W/\approx \to W/\approx, \quad [v][w] \to [vw].$$

Moreover,

$$\rho_i : G_i \to W/\approx, \quad g \to [\iota_i(g)]$$

is a group homomorphism and

$$\big(W/\approx, (\rho_i)_{i\in I}\big)$$

is a coproduct of the family of groups $(G_i)_{i\in I}$.

Proof. To simplify notation we assume without loss that the G_i's are pairwise disjoint. So $\iota_i = \mathrm{id}_{G_i}$ and $X = \dot\bigcup^{\text{int}}_{i\in I} G_i$.

Note that the defintion of $\sim$ implies that if $u, v, w \in W$ with $v \sim w$, then also $u * v \sim u * w$ and $v * u \sim w * u$. Thus by 1.12.10 $W/\approx$ is a monoid with identity $[()]$.

Let $i \in I$ and $a, b \in G_i$. We will apply (i) and (ii) with $x = y = ()$. By (i)

$$(1) \qquad a * b \sim a \cdot b \text{ and so } [a] * [b] = [a \cdot b]$$

By (ii)

$$1_i \sim () \text{ and so } [1_i] = [()]$$

If follows that $a * a^{-1} \approx a \cdot a^{-1} = 1_i \approx ()$. Thus by 1.12.10(d) $W/\approx$ is a group.

Define $\rho_i : G_i \to W/\approx, g \to [g]$. Then by (1), ρ_i is a homomorphism.

Now let H be a group and $(\alpha_i : G_i \to H)_{i\in I}$ a family of homomorphism. Define $\beta : X \to H$ by $\beta(x) = \alpha_i(w)$ if $i \in I$ with $x \in G_i$. Note here that i is uniquely determined since the G_i's are pairwise disjoint. By 1.12.8(c) there exists a unique homomorphism $\gamma : W \to H$ with $\gamma(x) = \beta(x)$ for all $x \in X$ and so $\gamma(a) = \alpha_i(a)$ for all $a \in G_i$.

We claim that $\gamma(v) = \gamma(w)$ whenever $v \approx w$. By 1.5.5 applied with $f = \gamma$ and $\approx$==, it suffices to show that $\gamma(v) = \gamma(w)$ whenever $v \sim w$.

Suppose first that (i) holds. Then $w = x * a * b * y$ and $v = x * (a \cdot b) * y$ for some $x, y \in W$, $i \in I$ and $a, b \in G_i$ Hence

$$\gamma(w) = \gamma(x)\gamma(a)\gamma(b)\gamma(y) = \gamma(x)\big(\alpha_i(a)\alpha_i(b)\big)\gamma(y) =$$
$$\gamma(x)\alpha_i(a \cdot b)\gamma(y) = \gamma(x)\gamma(a \cdot b)\gamma(y) = \gamma(v).$$

Suppose next that (ii) holds. Then $w = x * 1_i * y$ and $v = x * y$ for some $x, y \in W$ and $i \in I$ Hence

$$\gamma(w) = \gamma(x)\gamma(1_i)\gamma(y) = \gamma(x)\alpha_i(1_i)\gamma(y) = \gamma(x)1_H\gamma(y) = \gamma(x)\gamma(y) = \gamma(v).$$

By the claim we get a well defined map $\alpha : W/\approx \to H, [w] \to \gamma(w)$. Also as γ is a homomorphism, α is, too.

Suppose now that $\delta : W/\approx H$ is a homomorphism with $\alpha_i = \delta \circ \rho_i$ for all $i \in I$. Define $\delta^* : W \to H$ be $\delta^*(w) = \delta([w])$. Let $x \in X$. Then $x \in G_i$ for some $i \in I$. We have $\delta^*(x) = \delta(\rho_i(x)) = \alpha_i(x) = \beta(x) = \gamma(x)$ and since W is the free monoid on X, $\delta^* = \gamma$. Thus for all $w \in W$, $\delta([w]) = \delta^*(w) = \gamma(w) = \alpha([w])$, and so α is unique. □

Lemma 1.12.12. *Let $\big(G, (\rho_i)_{i\in I}\big)$ be a coproduct of the family of groups $(G_i)_{i\in I}$.*

(a) Each ρ_j, $j \in I$, is 1-1.

(b) $G = \langle \rho_i(G_i) \mid i \in I\rangle$.

Proof. (a) Fix $j \in I$. For $i \in I$ we will define homomorphism $G_i \to G_j$ as follows:

If $i = j$ put $\alpha_i = \mathrm{id}_{G_i}$.

If $i \neq j$ define α_i by $\alpha_i(g) = 1_{G_j}$ for all $g \in G_i$.

Then by definition of the coproduct there exists a homomorphism $\alpha : G \to G_j$ with $\alpha_i = \alpha \circ \rho_i$ for all $i \in I$. For $i = j$ we conclude,

$$\mathrm{id}_{G_j} = \alpha \circ \rho_j$$

Note that this implies that ρ_j is 1-1.

(b) Let $H = \langle \rho_i(G_i) \mid i \in I\rangle$. Then $(\rho_i)_{i\in I}$ is also a family of homomorphism $\rho_i : G_i \to H$. Thus there exists a homomorphism $\alpha : G \to H$ with $\rho_i = \alpha \circ \rho_i$ for all $i \in I$. Note that α is also a homomorphism from G to G, and that id_G is a homomorphism from G to G with $\rho_i = \mathrm{id}_G \circ \rho_i$ for all $i \in I$. So by the uniqueness assertion in the definition of a coproduct, $\alpha = \mathrm{id}_G$. Hence

$$G = \mathrm{Im}\,\mathrm{id}_G = \mathrm{Im}\,\alpha \leq H \leq G$$

So indeed $G = H = \langle \rho_i(G_i) \mid i \in I\rangle$. □

Proposition 1.12.13. *Let $(G_i)_{i\in I}$ be a pairwise disjoint family of groups. Let 1_i be the identity in G_i. Let $X = \bigcup_{i\in I} G_i$ and let (W, id_X) be a free monoid for X. Let $\approx$ be the equivalence relation introduced in 1.12.11. Let $w \in W$ and let $n \in \mathbb{N}$, $i_k \in I$ and $x_k \in G_{i_k}$ with $w = x_1 \dots x_n$. Call w reduced if*

(i) $x_k \neq 1_{i_k}$ for all $1 \leq k \neq n$.

(ii) $i_{k-1} \neq i_k$ for all $2 \leq k \leq n$.

Then for each $w \in W$ there exists a unique reduced $w_r \in W$ with $w \approx w_r$. So if W_r is the set of reduced elements, the function

$$W_r \to W/\approx, \quad u \to [u]$$

is a bijection with well-defined inverse

$$W/\approx \to W_r, \quad [w] \to w_r$$

Proof.

1°. *Let $w \in W$. Then w is reduced if and only if there does not exists $v \in W$ with $v \sim w$.*

Indeed, let $w = x_1 \dots x_n$ with $x_k \in X$. Then definition of $\sim$ shows that there exists $v \in W$ with $v \sim w$ if and only if either $x_k = 1_{i_k}$ for some $1 \leq k \leq n$ or $i_{k-1} = i_k$ for some $2 \leq k \leq n$. Note that this just means that w is not reduced.

Define the relation $\leq$ on W by $v \leq w$ if there exists $m \in N$ and an m-tuple $(v_0, v_1, \dots, v_m)$ in W such that

$$v_0 = v, v_m = w \text{ and } v_{k-1} \sim v_k \text{ for all } 1 \leq k \leq m$$

The following assertion follow immediately from the definitions:

2°.

(a) *$\leq$ is reflexive and transitive.*

(b) *If $v \leq w$, then $l(v) \leq l(w)$, with equality if and only if $v = w$.*

(c) *$v \leq w$ implies $v \approx w$.*

Next we prove:

3°. *For each $w \in W$ there exists a reduced word $v \in W$ with $v \leq w$.*

Choose $v \in V$ with $v \leq w$ and $l(v)$ minimal. If v is not reduced, then by (1°), $u \sim v$ for some $u \in W$. But then $l(u) = l(v) - 1 < l(v)$ and $u \leq w$, a contradiction to the choice of v.

4°. *Let $v_1, v_2, w \in W$ with $v_1 \sim W$ and $v_2 \sim w$. Then there exists $v \in W$ with $v \leq v_1$ and $v \leq v_2$.*

Let $l \in \{1, 2\}$. Since $v_l \sim w$, one of the following holds:

(li) There exist $d_l, e_l \in W$, $j_l \in J$ and $a_l, b_l \in G_{j_l}$ with $w = d_l * a_l * b_l * e_l$ and $v_l = d_l * (a_l \cdot b_l) * e_l$.

(lii) There exist $d_l, e_l \in W$, $j_l \in J$ with $w = d_l * 1_{j_l} * e_l$ and $v_l = d_l * e_l$.

Since we have two cases for $l = 1$ and $l = 2$ each, we will have two consider four different cases:

Case 1. *$(1i)$ and $(2i)$ holds, that is*

$$w = d_1 * a_1 * b_1 * e_1 \qquad v_1 = d_1 * (a_1 \cdot b_1) * e_1$$
$$w = d_2 * a_2 * b_2 * e_2 \qquad v_2 = d_2 * (a_2 \cdot b_2) * e_2$$

We may assume without loss that $l(d_2) \geq l(d_1)$.

Suppose first that $l(d_2) \geq l(d_1) + 2$. Then $d_2 = d_1 * a_1 * b_1 * d$ for some $d \in W$. Thus

$$w = d_1 * a_1 * b_1 * d * a_2 * b_2 * e_2, v_1 = d_1 * (a_1 \cdot b_1) * d * a_2 * b_2 * e_2, v_2 = d_1 * a_1 * b_1 * d * (a_2 \cdot b_2) * e_2$$

Put

$$v = d_1 * (a_1 \cdot b_1) * d * (a_2 \cdot b_2) * e_2.$$

Then $v \sim v_1$ and $v \sim v_2$ and so (4°) hold.

Suppose that $l(d_2) = l(d_1) + 1$. Then $d_2 = d_1 * a_1$ and $b_1 = a_2$. Thus

$$w = d_1 * a_1 * b_1 * b_2 * e_2, v_1 = d_1 * (a_1 \cdot b_1) * b_2 * e_2, v_2 = d_1 * a_1 * (b_1 \cdot b_2) * e_2$$

Choose $v = d_1 * (a_1 \cdot b_1 * b_2) * e_2$. Then $v \sim v_1$ and $v \sim v_2$ and (4°) holds.

Suppose that $l(d_2) = l(d_1)$. Then $d_1 = d_2$, $v_1 = v_2$ and we can choose $v = v_1 = v_2$.

Case 2. *$(1i)$ and $(2ii)$ holds, that is*

$$w = d_1 * a_1 * b_1 * e_1 \qquad v_1 = d_1 * (a_1 \cdot b_1) * e_1$$
$$w = d_2 * 1_{j_2} * e_2 \qquad v_2 = d_2 * e_2$$

Suppose first that $l(d_1) > l(d_2)$. Then $d_1 = d_2 * 1_{j_2} * d$ for some $d \in W$. Thus

$$w = d_2 * 1_{j_2} * d * a_1 * b_1 * e_1, v_1 = d_2 * 1_{j_2} * d * (a_1 \cdot b_1) * e_1, v_2 = d_2 * d * a_1 * b_1 * e_1$$

Put $v = d_2 * d * (a_1 \cdot b_1) * e_1$. Then $v \sim v_1$ and $v \sim v_2$. So (4°) holds.

Suppose that $l(d_1) = l(d_2)$. Then $d_1 = d_2$, $j_1 = j_2$ and $a_1 = 1_{j_1} = 1_{j_2}$.

Thus

$$w = d_1 * 1_{j_1} * b_1 * e_2, \quad v_1 = d_1 * (1_{j_1} \cdot b_1) * e_2 \quad v_2 = d_1 * b_1 * e_2$$

Thus $v_1 = v_2$ and we can choose $v_1 = v_2$.

If $l(d_1) + 1 = l(d_2)$ we have $1_{j_2} = b_1$ and similar argument as in case $l(d_1) = l(d_2)$ shows that $v_1 = v_2$ (In fact fact we could apply the $l(d_1) = l(d_2)$ result to opposite groups of W and G_i to treat this case.)

The case $l(d_1) + 2 \geq l(d_2)$ is similar to $l(d_1) < l(d_2)$ case. and can also by deduced from that case by looking at the opposite groups.

Case 3. *$(1ii)$ and $(2i)$ holds*

Follows from the previous case with the roles of v_1 and v_2 interchanged.

Case 4. $(1ii)$ *and* $(2i)$ *holds, that is*

$$w = d_1 * 1_{j_1} * e_1 \qquad v_1 = d_1 * e_1$$
$$w = d_2 * 1_{j_2} * e_2 \qquad v_2 = d_2 * e_2$$

We may assume that $l(d_2) \geq l(d_1)$.

Suppose that $l(d_1) = l(d_2)$, then $d_1 = d_2$ and $v_1 = v_2$. So we can choose $v = v_1 = v_2$.

So suppose $l(d_2) > l(d_1)$. Then $d_2 = d_1 1_{j_1} d$ for some $d \in W$ and so

$$w = d_1 * 1_{j_1} * d * 1_{j_2} * e_2, \quad v_1 = d_1 * d * 1_{j_2} * e_2 \quad v_2 = d_1 * 1_{j_1} * d * e_2$$

Put $v = d_1 * d * e_2$. Then $v \sim v_1$ and $v \sim v_2$ and so (4°) also holds in this last sub case.

5°. *For each $w \in W$ there exists a unique reduced word $w_r \in W$ with $w_r \leq w$.*

The existence has been established in (3°). For the uniqueness let z_1 and z_2 be reduced with $z_i \leq w$.

If $z_1 = w$ then w is reduced. So there does not exist $y \in W$ with $y \sim w$ and so $z_2 \leq w$ implies $z_2 = w = z_1$. So we may assume that $z_1 \neq w \neq z_2$.

By definition of $\leq$ there exist $v_i \in W$ with $z_i \leq v_i \sim w$.

By (4°) there exists $v \in W$ with $v \leq v_1$ and $v \leq v_2$. By (3°) there exist a reduced $z \in W$ with $z \leq v$. Since $\leq$ is transitive, $z \leq v_l$ for $l = 1, 2$. Since also z_l is reduced with $z_i \leq v_i$ and since v_i has length less than w, we conclude by induction that $z = z_l$. Thus $z_1 = z = z_2$ and (5°) is proved.

6°. *Let $v, w \in W$. Then $v \approx w$ if and only $v_r = w_r$.*

If $v_r = w_r$, then $v \approx v_r = w_r \approx w$ and so $v \approx w$.

Suppose that $v \sim w$. Since $v_r \leq v$ and $\leq$ is transitive, $v_r \leq w$. Since v_r is reduced, (5°) gives that $v_r = v_w$. We have shows that $v \sim w$ implies $v_r \sim w_r$. By 1.5.5 applies with $f : W \to W, w \to w_r$ and $\approx==$ we conclude that also $v \approx w$ implies $v_r = w_r$.

7°. *Let $w \in W$ then w_r is the unique reduced word with $w \approx w_r$.*

Let $v \in W$ be reduced. Then $v_r = v$ and so by (6°), $v \approx w$ if and only if $v = w_r$. □

1.12.14 (Products of reduced elements)**.** Note that W_r is usually not closed under multiplication (unless all G_i but one of the G_i's are trivial. But it is not difficult to figure out what the reduction of the product is. Indeed let $x = x_1 x_1 \ldots x_n$ and $y = y_0 y_1 \ldots y_m$ be reduced words. Let $0 \leq s \leq \min(n, m+1)$ be maximal with $y_t^{-1} = x_{n-t}$ for all $0 \leq t < s$. Then

$$xy \approx x_1 x_2 \ldots x_{n-s} y_s y_{s+1} \ldots y_m$$

If $s = n$, $s = m + 1$ or x_{n-s} and y_s are not contained in a common G_i this is the reduction of xy.

On the other hand if x_{n-s} and y_s both are contained in G_i, then

$$xy \approx x_1, \ldots x_{n-s-1}(x_{n-s} \cdot y_s) y_{s+1} \ldots y_m$$

By maximality of s, $x_{n-s} \cdot y_s \neq 1_i$ and it is easy to seen that the element on the right hand side of the last equation is reduced, and so is the reduction of xy.

Remark 1.12.15. *Coproducts also exists for semigroups and for monoids. Indeed, everything we did for groups carries over with one exception though. In case of semigroups we do not include the empty tuple in the sets of words and omit 1.12.11(ii) in the definition of $v \sim w$.*

Example 1.12.16. Let $A \cong B \cong \mathbb{Z}/2\mathbb{Z}$. We will compute $D = A \coprod B$. To simply notation we identify $x \in A \cup B$ with its image in D. In particular $1 := 1_G = 1_A = 1_B$, $\rho_A = \mathrm{id}_A$ and $\rho_B = \mathrm{id}_B$. Let $1 \neq a \in A$ and $1 \neq b \in B$. Then every elements in D has one of the following forms:

$$\begin{gathered} 1 \\ \underbrace{(ab)(ab)\dots(ab)}_{n \text{ times}} \\ \underbrace{(ba)(ba)\dots(ba)}_{n \text{ times}} \\ b\,\underbrace{(ab)(ab)\dots(ab)}_{n \text{ times}} \\ a\,\underbrace{(ba)(ba)\dots(ba)}_{n \text{ times}} \end{gathered}$$

Put $z = ab$. Then $z^{-1} = b^{-1}a^{-1} = ba$. So the above list now reads

$$z^0, z^n, z^{-n}, bz^n, \text{ and } az^{-n}.$$

Note that

$$bz^n = b(ab)^n = (aa)b(ab)^n = a(ab) = (ab)^{n+1} = az^{n+1}$$

and so

$$D = \{z^n, az^n \mid n \in \mathbb{Z}\}.$$

It is also easy to compute the product of two elements in D: Observe that

$$z^n a = a(ba)^{n-1}ba = az^{-n}$$

and so

$$z^n * z^m = z^{n+m}, \quad z^n * az^m = az^{m-n}, \quad az^n * z^m = az^{n+m}, \quad az^n * az^m = aaz^{-n}z^m = z^{m-n}$$

This can be combined in one formula: Define $\epsilon(0) = 1$ and $\epsilon(1) = -1$. Then for $n, m \in \mathbb{Z}$ and $i, j \in \{0, 1\}$:

$$(a^i z^n) * (a^j z^m) = a^{i+j} z^{\epsilon(j)n+m}$$

By now we determined the complete multiplication table of D. D is called the infinite *dihedral* group.

We will know constructed a second group $\tilde{D}$ and show that it is isomorphic to D. Define

$$\tilde{a}: \quad \mathbb{Z} \to \mathbb{Z} \quad\quad m \to -m$$

$$\tilde{b}: \quad \mathbb{Z} \to \mathbb{Z} \quad m \to 1 - m$$

Then $\tilde{a}, \tilde{b} \in \mathrm{Sym}(\mathbb{Z})$, $\tilde{a}$ is a reflection at 0 and $\tilde{b}$ is the reflection at $\frac{1}{2}$ Put $\tilde{D} = \langle \tilde{a}, \tilde{b} \rangle$. Since both $\tilde{a}$ and $\tilde{b}$ have order two, there exist homomorphism,$\alpha_A : A \to \tilde{D}$ and $\alpha_B : B \to \tilde{D}$ with $\alpha_A(a) = \tilde{a}$ and $\alpha_B(b) = \tilde{b}$. Hence by the definition of the co-product, there exists a homomorphism $\beta : D \to \tilde{B}$ with $\alpha_A = \beta \circ \rho_A$ and $\alpha_B = \beta \circ \rho_B$. Then

$$\beta(a) = \beta(\rho_A(a)) = \alpha_A(a) = \tilde{a}$$

and similarly $\beta(b) = \tilde{b}$.

Hence

$$\beta(D) = \beta(\langle a, b \rangle) = \langle \beta(a), \beta(b) \rangle = \langle \tilde{a}, \tilde{b} \rangle = \tilde{D}$$

So β is onto. Put $\tilde{z} = \tilde{a} \circ \tilde{b}$. Then

$$\tilde{z}(m) = \tilde{a}(\tilde{b}(m)) = \tilde{a}(1 - m) = m - 1$$

So $\tilde{z}$ is the translation by -11. Also $\tilde{z}^j(m) = m - n$ and $(\tilde{a}\tilde{z}^j)(m) = \tilde{a}(m - j) = j - m$. Thus z^j is translation by $-j$ and $\tilde{a}\tilde{z}^n$ is the reflection at $\frac{j}{2}$.

We have $\beta(z) = \beta(ab) = \beta(a)\beta(b) = \tilde{a}\tilde{b} = \tilde{z}$ and so also $\beta(a^i z^j) = \beta(a)^i \widetilde{(b)}^j = \tilde{a}^i \tilde{z}^j$. Since the $\tilde{a}^i \tilde{z}^j, i = 0, 1, j \in \mathbb{Z}$ are pairwise distinct, we conclude that β is 1-1. Thus β is an isomorphism and

$$D \cong \tilde{D}$$

Let $Z = \langle z \rangle$. Then $Z \cong (\mathbb{Z}, +)$ and Z has index two in $G_1 * G_2$. In particular, $Z \trianglelefteq D$. Also $z^a = aza = aaba = ba = z^{-1}$. Thus

$$(z^n)^a = z^{-n} \quad \text{and} \quad z^n a = a z^{-n}.$$

In particular, if $A \leq Z$ then both Z and a normalize D and $A \trianglelefteq G$.

Here is a property of D which will come in handy later on:

All elements in $D \setminus Z$ are conjugate to a or b.

Indeed $z^n a z^{-n} = z^n z^n a = z^{2n} a$ and $z^n b z^{-n} = z^{2n} b = z^{2n} baa = z^{2n+1} a$. So $z^{2n} a$ is conjugate to a and $z^{2n+1} a$ is conjugate to b.

Fix $n \in \mathbb{Z}$. Consider the relation $z^n = e$. Put $N = \langle z^n \rangle$. Then $N \trianglelefteq D$ and so

$$\coprod_{i \in \{1,2\}} G_i / \langle (ab)^n = e \rangle = D/N$$

Since $Z/D \cong \mathbb{Z}/n\mathbb{Z}$, D/N has order $2n$. D/N is called the dihedral group of order $2n$, or the dihedral group of degree n.

Suppose now that $\bar{D}$ is any group generated by two elements of order two, $\bar{a}$ and $\bar{b}$. Then there exists a homomorphism $\alpha : D \to \bar{D}$ sending a to $\bar{a}$ and b to $\bar{b}$. Let $\bar{z} = \bar{a}\bar{b}$ and $\bar{Z} = \langle \bar{z} \rangle$. Since neither a nor b are in $\ker\alpha$ and all elements in $D \smallsetminus Z$ are conjugate to a or b, $\ker\alpha \leq Z$. Thus $\ker\alpha = \langle z^n \rangle$ for some $n \in \mathbb{N}$ and so $\bar{D} \cong D/\ker\alpha = D/N$. So any group generated by two elements of order 2 is a dihedral group.

Definition 1.12.17. *Let I be a set. A free group generated by I is pair (F, ρ), where F is group and $\rho : I \to F_I$ is a function, with the following property:*

Whenever H is a group and $\alpha : I \to H$ is a function, then there exists a unique homomorphism $\beta : F \to H$ with $\alpha = \beta \circ \rho$.

$$\begin{tikzcd}
H & & F \arrow[ll, "\exists!\beta"'] \\
& I \arrow[ul, "\alpha"] \arrow[ur, "\rho"'] &
\end{tikzcd}$$

Lemma 1.12.18. *Let I be a set. Then there exists a free group generated by I.*

Proof. For $i \in I$ let $G_i = (\mathbb{Z}, +)$ and let $\left(F, (\rho_i)_{i \in I}\right)$ be a coproduct of $(G_i)_{i \in I}$. Define $\rho : I \to F$, $i \to \rho_i(1)$. Now let H be a group and $\alpha : I \to H$ be function. Define

$$\alpha_i : G_i \to H, m \to \alpha(i)^m.$$

Since $h^{n+m} = h^n h^m$ for all $h \in H, n, m \in \mathbb{Z}$, α_i is a homomorphism. So by definition of the coproduct of $(G_i)_{i \in I}$ there exists a unique homomorphism $\beta : F_I \to H$, with $\alpha_i = \beta \circ \rho_i$. Then

$$\alpha(i) = \alpha_i(1) = \beta(\rho_i(1)) = \beta(\rho(i))$$

and so $\alpha = \beta \circ \rho$. Suppose also $\gamma : F \to H$ fulfills $\alpha = \gamma \circ \rho$. Then for all $m \in G_i$,

$$\alpha_i(m) = \alpha(i)^m = \gamma(\rho(i))^m = \gamma(\rho_i(1)^m) = \gamma(\rho_i(m))$$

Hence $\alpha_i = \gamma \circ \rho_i$ and so by the uniqueness assertion in the definition of the coproduct $\beta = \gamma$. □

Lemma 1.12.19. *Let (F, ρ) be a free group generated by I. Then ρ is 1-1.*

Proof. Let H be any non-trivial group and $1 \neq h \in H$. Let $j \in J$ and define $\alpha : I \to H$ by

$$\alpha(j) = \begin{cases} h & \text{if } i = j \\ 1 & \text{if } i \neq j \end{cases}$$

Then there exists a homomorphism $\beta : F \to H$ with $\alpha = \beta \circ \rho$. Then for $i \in I$ with $i \neq j$.

$$\beta(\big(\rho(i)\big) = \alpha(i) = 1 \neq h = \alpha(j)\beta(\big(\rho(i)\big)$$

and so $\rho(i) \neq \rho(j)$. □

In view of the preceding lemma we can identify $i \in I$ with $\rho(i)$ in F. This gives rise to the following

Notation 1.12.20. *Let I be a set. Then F_I is a group with $I \subseteq F_I$ such that (F_I, id_I) is a free group generated by I.*

1.12.21 (Reduced words in free groups)**.** Let I be a set and $G_i = \langle i \rangle = \{i^m \mid m \in \mathbb{Z}\}$, the subgroup of F_I generated by I. Then by proof of 1.12.18 $G_i \cong \mathbb{Z}$ and F_I is the co-product of the $(G_i)_{i \in I}$. So by 1.12.13 each element in F_I can be uniquely written as $g_1 g_2 \dots g_k$ where $k \in \mathbb{N}$, $g_j \in G_{i_j}$, $g_j \neq 1_{G_{i_j}}$ for all $1 \leq j \leq k$ and $i_{j-1} \neq i_j$ for all $2 \leq j < k$. Since $G_{i_j} = \langle i_j \rangle$ we have $g_j = i_j^{m_j}$ for some $0 \neq n_j \in \mathbb{Z}$. Thus every element w in F_I can be uniquely written as

$$(*) \qquad w = i_1^{n_1} i_2^{n_2} \dots i_n^{n_k}$$

where $k \in \mathbb{N}$, $i_j \in I$, $0 \neq n_j \in \mathbb{Z}$ and $i_{j-1} \neq i_j$. (*) is called

is called the *reduced form* of w. G be group and $g = (g_i)_{i \in I}$ a family of elements of G. Then by definition of the free group there exists a unique homomorphism $\beta : F_I \to G$ with $g = \beta \circ \mathrm{id}_I$. Note that $g = \beta \circ \mathrm{id}_I$ just means $\beta(i) = g_i$ for all $i \in I$. Thus

$$\beta(i_1^{n_1} i_2^{n_2} \dots i_k^{n_k}) = g_{i_1}^{n_1} g_{i_2}^{n_2} \dots g_{i_k}^{n_k}$$

Definition 1.12.22. *Let I be a set.*

(a) A group relation *is an ordered pair (v, w) with $v, w \in F_I$. We will usually denoted such an ordered pair by $v \equiv w$.*

(b) Let G be a group and $g \in G^I$. We say that g fulfills the relation $v \equiv w$ provided that $\beta(v) = \beta(w)$, where β is the unique homomorphism from F_I to G with $beta|_I = g$.

Let $v, w \in F_I$ with $v = i_1^{n_1} \dots i_k^{n_k}$ and $w = j_1^{m_1} \dots j_l^{m_l}$. Then $g = (g_i)_{i \in I}$ fulfills the relation

$$i_1^{n_1} \dots i_k^{n_k} \equiv j_1^{m_1} \dots j_l^{m_l}$$

if and only if

$$g_{i_1}^{n_1} \dots g_{i_k}^{n_k} = g_{j_1}^{m_1} \dots g_{j_l}^{m_l}$$

Example 1.12.23. Let $I = \{a, b\}$, $G = \mathrm{Sym}(3)$ and consider the relation $aba^{-1} \equiv b^{-1}$.

Do $g_a = (12)$ and $g_b = (123)$ fulfill the relation? In other words is

$$(12) \circ (123) \circ (12)^{-1} \overset{?}{=} (123)^{-1}$$

The left hand side is (213) and the right hand side is (321), both of which are equal to (132). So the answer is yes.

Do $h_a = (12)$ and $h_b = (23)$ fulfill the relation?

$$(12) \circ (23) \circ (12)^{-1} \overset{?}{=} (23)^{-1}$$

The left side is (13) the right side is (23), so this time the answer is no.

Definition 1.12.24. *Let I be a set and $\mathcal{R}$ a set of group relations on I. Then a group with generators I and relations $\mathcal{R}$ is a pair $\big(G, g\big)$, where G is a group and $g \in G^I$ such that*

(a) f fulfills all the relations in $\mathcal{R}$.

(b) Whenever H is a group and $h \in H^I$ fulfills all the relations in $\mathcal{R}$, then there exists a unique homomorphism $\delta : G \to H$ with $h = \delta \circ g$.

Lemma 1.12.25. *Let I be a set and $\mathcal{R}$ a set of group relations on I. Then there exists a group G with generators I and relations $\mathcal{R}$.*

Proof. Note that the relation $v \equiv w$ is fulfilled if and only if the relation $vw^{-1} \equiv 1$ is fulfilled. So we may assume that $\mathcal{R} = \{r \equiv 1 \mid r \in R\}$ for some subset R of F_I. Put

$$N := \langle {}^{F_I}R \rangle,$$

so N is the intersection of all the normal subgroup of F_I containing R. Put $G = F_I/N$ and let $g_i = iN$ for $i \in N$. Note that

$$\pi_N : F_I \to G, w \to wN$$

is the unique homomorphism from F_I to G with $\pi_N(i) = g_i = iN$. Also

$$\pi_N(r) = rN = N = 1_G$$

for all $r \in R$ and so $g = (g_i)_{i \in I}$ fulfills all the relation in $\mathcal{R}$.

Now let H be a group and let $h \in H^I$ fulfill all the relations in $\mathcal{R}$. Let $\beta : F_I \to H$ be the unique homomorphism with $\beta|_I = h$. Let $r \in R$. Since h fullfills all the relations $r \equiv 1$, we have $\beta(r) = 1$. Hence $r \in \ker\beta$ and $R \subseteq \ker\beta$. Since $\ker\beta \trianglelefteq F_I$ and $N = \langle {}^{F_I}R \rangle$, $N \leq \ker{}'$. It follows that the map

$$\delta : G \to H, wN \to \beta(w)$$

is a well-defined homomorphism. Also $\delta(g_i) = \delta(iN) = \beta(i) = h_i$.

It remains to show that uniqueness δ. So let $\alpha : G \to H$ be a homomorphism with $\alpha(g_i) = h_i$. Then $(\alpha \circ \pi_N)(i) = \alpha(g_i) = h_i$ and so $\alpha \circ \pi_N = \beta$ by uniqueness of β. Hence for all $w \in F_I$, $\alpha(wN) = (\alpha \circ \pi_N)(w) = \beta(w)$ and so $\alpha = \delta$. □

Remark 1.12.26. *Let (G, g) be a group with generators I and relations $\mathcal{R}$. Then $G = \langle g_i \mid i \in I\rangle$.*

Proof. This follows from the construction above but can also be proven directly from the definition:

Let $H = \langle g_i \mid i \in I\rangle$. Since $g = (g_i)_{i\in I}$ is a family of elements in H fulfilling the relations $\mathcal{R}$, there exists a homomorphism $\alpha : G \to H$ with $\alpha(g_i) = g_i$ for all $i \in I$. Note that α is also a homomorphism from G to G, and that id_G is a homomorphism from G to G with $\mathrm{id}_G(g_i) = g_i$ for all $i \in I$. It follows that $\mathrm{id}_G = \alpha$ and so

$$G = \operatorname{Im} \mathrm{id}_G = \operatorname{Im} \alpha \le H \le G$$

So indeed $G = H = \langle g_i \mid i \in I\rangle$. □

1.12.27 (Notation in groups with generators and relation)**.** Let I be a set and $\mathcal{R}$ a set of group relations on I. Then

$$G = \langle I \mid \mathcal{R}\rangle$$

means that G is a group and there exists a family of elements $(g_i)_{i\in I}$ in G such that $\big(G, (g_i)_{i\in I}\big)$ is group with generators I and relations $\mathcal{R}$. So if

$$(*) \qquad i_1^{n_1} \dots i_k^{n_k} \equiv j_1^{m_1} \dots j_l^{m_l}$$

is one of the relation in $\mathcal{R}$ then

$$(**) \qquad g_{i_1}^{n_1} \dots g_{i_k}^{n_k} = g_{j_1}^{m_1} \dots g_{j_l}^{m_l}.$$

In practical computation is often quite cumbersome to work with elements with subscripts. We therefore often just write a for the element g_a in G. This should be only done if this is clearly from the context that the computation are done in G and that a no longer stands for the element a in F_I. Note also that this is not an identification, since the map $I \to G, a \to g_a$ is (in general) not 1-1. The advantage of this convention is that, replacing all g_a by a, the equation (**) now turns into the easier

$$(***) \qquad i_1^{n_1} \dots i_k^{n_k} = j_1^{m_1} \dots j_l^{m_l}.$$

So the group relation (*) in F_I turns into the actual equality (***) in G.

Example 1.12.28. 1. We will show that

$$G := \langle a, b, c \mid ab \equiv c, ab \equiv ba, c^2 \equiv= a, c^3 \equiv= b, c^5 \equiv 1\rangle$$

is the trivial group.

We will follow the conventions of 1.12.27 and just write a for g_a, b for g_b and c for g_c, that is we treat a, b, c as elements of G, rather than elements of $F_{\{a,b,c\}}$. Then the relations defining G become actual equalities and so $c = ab = c^2c^3 = c^5 = e$. Hence also $a = c^2 = e$ and $b = c^2 = e$. Thus $G = 1$.

2. The group

$$G = \langle a, b \mid a^2 \equiv 1, b^2 \equiv 1 \rangle$$

is the infinite dihedral group. To see that let $H_a = \langle h_a \rangle$ and $H_b = \langle h_b \rangle$ be cyclic groups of order 2 and $H = H_a \coprod H_b$. Let $G_a = \langle g_a \rangle \leq G$ and $G_b = \langle g_b \rangle \leq G$. Since $g_a^2 = g_b^2 = 1$. There exists homomorphism $\alpha_a : H_a \to G_a$ and $\alpha_b : H_b \to G_b$ with $\alpha_a(h_a) = g_a$ and $\alpha_b(h_b) = g_b$. So by defintion of the coproduct, there exists unique homomorphism $\alpha : H \to G$ with $\alpha(h_a) = g_a$ and $\alpha(h_b) = g_b$. Conversely, since (g_a, g_b) fulfills the relation $a^2 \equiv 1$ and $b^2 \equiv 1$, there exists a unique homomorphism $\beta : G \to H$, with $\beta(g_a) = h_a$ and $\beta(g_b) = h_b$. It is now easy to see that $\alpha \circ \beta = \mathrm{id}_G$ and $\beta \circ \alpha = \mathrm{id}_H$. So $G \cong H$.

Informally what we just proved is that the 'largest' group generated by two elements of order two is same as the 'largest' groups generated by two groups of order two.

3. The group

$$\langle a, b \mid a^2 = 2, b^2 = e, (ab)^n = e \rangle$$

is the called the *dihedral group* Dih_{2n} of degree n or the *dihedral group* of order $2n$

Let $F = F_{\{a,b\}}$ and $K = \langle^F \{a^2, b^2\}$ and $N = \langle^F \{a^2, b^2, (ab)^n\}\rangle$. Then by (2), F/K is the infinite dihedral group. For $x \in F$ let $\overline{x} = xK$. Put $z = ab$ and $y = (ab)^n$. Then $N = K\langle^F y\rangle$. By 1.12.16, $\overline{az} = \overline{z}^{-1}\overline{a}$. If follows that ${}^{\overline{a}}\overline{z} = \overline{z}^{-1}$, ${}^{\overline{a}}\overline{y} = \overline{y}^{-1}$ and ${}^{\overline{a}}\overline{y}\rangle = \langle {}^{\overline{a}}\overline{y}\rangle = \langle \overline{y}^{-1}\rangle = \langle o\ y\rangle$. Hence $\overline{a}$ and $\overline{z}$ normalizes $\langle \overline{y}\rangle$. Since $\overline{F} = \langle \overline{a}, \overline{z}\rangle$, $\langle \overline{y}\rangle$ is normal in $\overline{F}$. Hence $K\langle y\rangle$ is normal in F and $N = K\langle \overline{y}\rangle$. Thus

$$F/N \cong \overline{F}/\overline{N} = \overline{F}/\langle \overline{y}\rangle = \overline{F}/\langle \overline{z}^n\rangle$$

By 1.12.16 $\overline{F} = \{\overline{a}^i\overline{z}^j \mid i \in 0, 1, j \in \mathbb{Z}\}$. Since $(\overline{a}^i\overline{z}^j)\overline{z}^{nm} = \overline{a}^i\overline{z}^{l+nm}$ we see that

$$a^i z^j N = a^k z^l N \quad < ri = k \text{ and } j \equiv k \pmod{n}$$

Thus $F/N = \{a^i z^j N \mid 0 \leq i \leq 1, 0 \leq j < n\}$ and so $|F/N$ has order 2.

We will now construct a second group which is isomorphic to F/N. This is similar to construction of the group $\tilde{D}$ in Example 1.12.16. The only difference is that we repalce $\mathbb{Z}$ by $\mathbb{Z}/n\ mbZ$ where n is an integer with $n \geq 2$.

Define $\tilde{a} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, m \to -m$ and $\tilde{b} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, m \to 1 - m$. Put $\tilde{z} = \tilde{a} \circ \tilde{b}$. Then as in 1.12.16

$$\tilde{z}(m) = m + 1, \quad \tilde{z}^j(m), \quad = m - j, \quad \tilde{a}\tilde{z}^j(m) = j - m$$

Put $\tilde{G} = \langle \tilde{a}, \tilde{b}\rangle$. Since the calculation are done modulo n we conclude that

$$|\tilde{z}| = n, \tilde{D} = \{\tilde{a}^i\tilde{z}^j \mid 0 \leq 1 \leq i, 0 \leq j < n\}, \text{ and } |\tilde{D}| = 2n$$

So $(\tilde{a}, \tilde{b})$ fulfills the relations for G and so there exists a unique homomorhism $\beta : G \to \tilde{G}$ with $\beta(aN) = \tilde{a}$ and $\beta(bN) = \tilde{b}$. Then $\beta(a^i z^j N) = \tilde{a}^i \tilde{b}^j$ and so β is a bijection. Thus $G \cong \tilde{G}$.

Here is a more geometric version of the above. Let $\xi = e^{\frac{2\pi i}{n}} \in \mathbb{C}$ and $U_n = \{\xi^i \mid 0 \leq i < n\}$. So U_n is the set of n-roots of unity in $\mathbb{C}$ and the map $\mathbb{Z}/n\mathbb{Z}, +) \to (U_n, \cdot), i \to \xi^i$ is an isomorphism. $\tilde{z}^j$ corresponds to clockwise rotation by $\frac{j}{n} 2\pi$ radiants and $\tilde{a}z^i$ correponds to the reflection at the line through 0 and $\xi^{\frac{j}{2}}$. Note that if j is even $xi^{\frac{j}{2}}$ is in U_n, while if j is odd $xi^{\frac{j}{2}}$ is the midpoint on the unit circle between $\xi^{\frac{j-1}{2}}$ and $\xi^{\frac{j+1}{2}}$.

4.

$$G := \langle a, b \mid a^3 \equiv 1, b^3 \equiv 1, (ab)^2 \equiv 1 \rangle$$

To determine G let $z = ab$. Then $z^2 = 1$. We compute

$$^{a^2}z \cdot {}^{a}z \cdot z = a^2(ab)a^{-2} \cdot a(ab)a^{-1} \cdot ab = a^3 b(a^{-2}a^2)b(a^{-1}a)b = a^3 b^3 = 1.$$

Since $z^2 = 1$ this implies

$$^{a^2}z = {}^{a}z \cdot z = z \cdot {}^{a}z, \quad z = {}^{a^2}z \cdot {}^{a}z = {}^{a}z \cdot {}^{a^2}z \quad \text{and} \quad {}^{a}z = {}^{a^2}z \cdot z = z \cdot {}^{a^2}z$$

Thus

$$K := \{1, z, {}^{a}z, {}^{a^2}z\}$$

is a subgroup of G. Now

$$^{a}({}^{a^2}z) = {}^{a^3}z = {}^{1}z = z.$$

and so $a \in \mathrm{N}_G(K)$. Put $A = \langle a \rangle$. Then $A \leq \mathrm{N}_G(K)$ and so AK is a subgroup of G. It contains a and $z = ab$ and so also $b = a^{-1}z$. Thus $G = \langle a, b \rangle = AB$. Since $a^3 = 1$, $|A| leq 3$. Also $|K| \leq 4$ and so $|G| \leq |A||K| \leq 12$.

Put

$$H = \mathrm{Alt}(4), \quad h_a = (123) \quad h_b = (124)$$

Then $h_a^3 = 1, h_b^3 = 1$, $h_a h_b = (123)(124) = (13)(24)$ and $(h_a h_b)^2 = 1$. So (h_a, h_b) fulfills the relations and so there exists a homomorphism

$$\alpha : G \to \mathrm{Alt}(4) \text{ with } a \to (123), b \to (124)$$

Put $L = \langle 123, (124) \rangle$. Then L has more than one Sylow 3-subgroup and so has at least four Sylow 3 subgroup. Hence $|L| \geq 12$ and $L = \mathrm{Alt}(4)$. Since $L \leq \mathrm{Im}\,\alpha$, α is onto. Since $|G| \leq 12 = |\mathrm{Alt}(4)|$ we conclude that α is a isomorphism. Thus

$$G \cong \mathrm{Alt}(4)$$

5. Let $(G_i)_{i\in I}$ be a pairwise disjoint family of groups. Then

$$\langle \bigcup_{i\in I} G_i \mid a * b \equiv a \cdot b \text{ for all } i \in I, a, b \in G_i, a * b \equiv b * a \text{ for all } i, j \in I, i \neq j, a \in G_i, b \in G_j \rangle$$

   is $\bigoplus_{i\in I} G_i$

6. Let I be a set, then

$$\langle I \mid ij \equiv ji \text{ for all } i, j \in I \rangle$$

   is $\bigoplus_{i\in I} \mathbb{Z}$ and is denote by $\mathbb{Z}_I$. This group is called the free abelian group on the set I. Using additive notation, each elements of $\mathbb{Z}_I$ can be uniquely written as

$$\sum_{i\in I} n_i i$$

   where $(n_i)_{i\in I}$ is an almost zero sequence of integers and

$$\sum_{i\in I} n_i i + \sum_{i\in I} m_i i = \sum_{i\in I} (n_i + m_i) i$$

Definition 1.12.29. *Let $(M, \cdot)$ be a magma and $(F_M, *, \mathrm{id}_M)$ a free group on the set M. Let (G, ρ) be the group with generators $(m)_{m\in M}$ and relations*

$$a * b \equiv a \cdot b, \qquad a, b \in M$$

Then (G, ρ) is called the group generated by the magma M.

Lemma 1.12.30. *(G, ρ) be a group generated by the magma M. Let H be group and $\alpha : M \to H$ a homomorphism. Then there exists a unique homomorphism $\beta : G \to H$ with $\alpha = \beta \circ \rho$.*

Proof. Let $a, b \in M$. Then $\alpha(ab) = \alpha(a)\alpha(b)$ and so (H, α) fulfills the relations $a * b \equiv a \cdot b, a, b \in M$. So the lemma follows from the definition of a group with generators and relations. □

Lemma 1.12.31. *Let G be group. Then (G, id_G) is the group generated by the magma G.*

Proof. Let H be a group and $\alpha : G \to H$ be a homomorphism. Then α is the unique homomorphism from G to H with $\alpha = \alpha \circ \mathrm{id}_G$. So the lemma follows from 1.12.30. □

1.13 Fractions

Definition 1.13.1. *Let G and H be magma. A (G,H)-biset is triple $(A,*,\diamond)$ such that*

(a) $*$ is a action of G on A.

(b) $\diamond$ is a right action of H on A.

(c) $g*(a\diamond h)=(g*a)\diamond h$ for all $g\in G, a\in A$ and $h\in H$.

Lemma 1.13.2. *Let G and H be magma and A an (G,H)-biset. Then the function*

$$G\times A/H\to A/H,\quad (g,[a])\quad\to\quad [ga]$$

is a well defined action of G on the set A/H of orbits of H on A.

Proof. Let $\sim=\{(a,ah)\mid a\in A, h\in H\}$ and $\approx$ the equivalence relation on A generated by $\sim$. Then by definition the orbit $[a]$ of H on A containing a is $[a]_\approx$. Let $a,b\in A$ with $a\sim b$ and $g\in G$. Then $b=ah$ for some $h\in H$ and

$$gb=g(ah)=(ga)h$$

Thus $ga\sim gb$ and so $\sim$ is G-invariant. The lemma now follows from 1.7.42. □

Definition 1.13.3. *Let H be magma, A a right H-set, B an H set.*

(a) Let $\sim_H$ be the relation

$$\left\{\,\big(\,(ah,b)\,,(a,hb)\,\big)\,\middle|\,a\in A, h\in H, b\in B\right\}$$

Let $\approx_H$ be the equivalence relation on $A\times B$ generated by $\sim_H$. Define

$$a\times_H b=[(a,b)]_{\approx_H}\qquad \textit{and}\qquad A\times_H B=A\times B/\approx_H$$

$A\times_H B$ is called the balanced product of A and B over H.

(b) A function $f\in\mathrm{Fun}(A\times B)$ is called H-balanced if $(\sim_H,=)$ is f-invariant, that is $f(ah,b)=f(a,hb)$ for all $a\in A, h\in H$ and $b\in B$.

Lemma 1.13.4. *Let H be magma, A a right H-set, B an H set and $f\in\mathrm{Fun}(A\times B)$ an H-balanced function. Then*

$$\overline{f}\in\mathrm{Fun}(A\times_H B),\ a\times_H b\to f(a,b)$$

is a well-defined function.

Proof. Since $(\sim_H,=)$ is f-invariant, 1.5.5 shows that $(\approx_H,=)$ is f-invariant. Thus f is well-defined. □

Lemma 1.13.5. *Let G and H be magma, A a (G,H)-biset and B an H-set. Then*

$$*: G\times(A\times_H B)\to A\times_H B,\ (g,a\times_H b)\to ga\times_H b$$

is a well-defined action of G on $A\times_H B$.

Proof. Let $g\in G$. Define

$$f_g : A\times B\to A\times B, (a,b)\to(ga,b).$$

Since

$$f_g(ah,b)=\big(g(ah),b\big)=\big(ga)h,b\big)\sim_H\big(ga,hb\big)=f_g(a,hb)$$

$(\sim_H,\approx_H)$ is f_g-invariant. Hence by 1.5.5 also $(\approx_H,\approx_H)$ is f_g-invariant and so $*$ is well-defined. Note also that

$$(gg')*(a\times_H b)=\big((gg')a\big)\times_H b=\big(g(g'a)\big)\times_H b=g*\big((g'a)\times_H b\big)=g*\big(g'*(a\times_H b)\big)$$

and so $*$ is an action of G on $A\times_H B$. □

Lemma 1.13.6. *Let X be a non-empty abelian semigroup and $*$ a magma action of X on set S. Let $\sim$ be the relation on $X\times S$ defined by*

$$(x,s)\sim(zx,zs)\qquad \textit{for all } x,z\in X, s\in S$$

Let $\approx$ be the relation on $X\times S$ defined by

$$(x,s)\approx(y,t)\qquad \textit{if there exists } z\in X \textit{ with}\qquad zxt=zys$$

For $x\in X$ and $s\in S$ put $\frac{s}{x}=[(x,s)]_\approx$ and $X^{-1}S=(X\times S)/\approx=\{\frac{s}{x}\mid s\in S, x\in X\}$. Then

(a) $\approx$ is the equivalence relation on $X\times S$ generated by $\sim$.

(b) Let $(s,x),(t,y)\in X\times S$. Then

$$sy=xt\qquad\Longrightarrow\qquad \frac{s}{x}=\frac{t}{y}$$

(c) $\alpha: X\times X^{-1}S\to X^{-1}S,\ (y,\frac{s}{x})\to\frac{ys}{x}$ is well-defined action of X on $X^{-1}S$.

(d) $\beta: X\times X^{-1}S\to X^{-1}S,\ (y,\frac{s}{x})\to\frac{s}{yx}$ is well-defined action of X on $X^{-1}S$.

(e) For all $y\in X$, the function $y^\alpha: X^{-1}S\to X^{-1}S, \frac{s}{x}\to\frac{ys}{x}$ is inverse to the function $y^\beta: X^{-1}S\to X^{-1}S, \frac{s}{x}\to\frac{s}{yx}$.

(f) *For all $y, z \in X$ and $\frac{s}{x} \in X^{-1}S$,*

$$(y^\alpha \circ z^\beta)(\frac{s}{x}) = \frac{ys}{zx} = (z^\alpha \circ x^\beta)(\frac{s}{x})$$

and $y^\alpha \circ z^\beta = z^\beta \circ y^\alpha$.

(g) *Let $x \in X$. Then map $\tau : S \to X^{-1}S, s \to \frac{xs}{x}$ is a X-equivariant and independent of the choice of $x \in X$.*

(h) *$\tau(s) = \tau(t)$ if and only if $zs = zt$ for some $z \in X$.*

(i) *τ is 1-1 if and only if z^* is 1-1 for all $z \in X$.*

(j) *$\frac{s}{x} = x^\beta(\tau(s))$ for all $x \in X, s \in S$.*

(k) *Suppose $\diamond$ is an action of X on the set $\tilde{S}$, $\rho : S \to \tilde{S}$ is X-equivariant and $x^\diamond$ is invertible for each $x \in X$. Then*

$$\gamma : S^{-1}X \to \tilde{S}, \frac{g}{s} \to (x^\diamond)^{-1}(\rho(s))$$

is well-defined and is the unique X-equivariant map from $S^{-1}X$ to $\tilde{S}$ with $\rho = \gamma \circ \tau$.

Proof. Note first that $\sim$ is just the relation associated to the magma-action

$$X \times (X \times S) \to (X \times S), \quad \big(z, (x, s) \ \to\ (zx, zs)$$

of X on $X \times S$. Let $≋$ by the equivalence relation generated by $\sim$.

(a) Let $(x, s), (y, t) \in X \times S$. By 1.7.15(b)

$$(x, s) ≋ (y, t) \qquad \Longleftrightarrow \qquad (ux, us) = (vy, vt) \text{ for some } u, v \in X$$

Suppose this holds. Then $ux = vy$ and $us = vt$. Thus

$$u(xt) = (ux)t = (vy)t = (yv)t = y(vt) = y(us) = (yu)s = (uy)s = u(ys)$$

and so using $z = u$ we see that $(x, s) \approx (y, t)$. Hence $≋\subseteq\approx$.
Conversely suppose that $z(xt) = z(ys)$ for some $z \in X$. Put $u = zy$ and $v = zx$. Then

$$ux = (zy)x = z(yx) = z(xy) = (zx)y = vy \quad \text{ and } us = (zy)s = z(ys) = z(xt) = (zx)t = vt$$

and so $(x, s) \approx (y, t)$ and $\approx\subseteq≋$.

(b) Note that $xt = ys$ implies $xxt = xys$ and using $z = x$ we see that $(x, s) \approx (y, t)$. Since $\approx$ is an equivalence relation, this gives (b).

(c) Observe that X acts on $X \times S$ via $y * (x, s) = (yx, s)$ and since X is abelian, X acts on $X \times S$ from the right via $(x, s)z = (zx, zs)$. Moreover,

$$(y * (x, s))z = (yx, s)z = (zyx, zs) = (y(zx), zs) = y * (zx, zs) = y * \big(x, s)z.$$

$X \times S$ is an $X, X)$-biset and the assertion follows from 1.13.2.

(d) Observe that X acts on $X \times S$ via $y \cdot (x, s) = (x, ys)$
Moreover,

$$(y \cdot (x, s))z = (x, ys)z = (zx, zys) = (zx, y(zs)y \cdot (zx, zs) = y \cdot \big((x, s)z\big)$$

So $X \times S$ is an (X, X)-biset and the assertion follows from 1.13.2.

(f):

$$(y^\alpha \circ z^\beta)(\frac{s}{x}) = y^\alpha(z^\beta(\frac{s}{x})) = y^\alpha(\frac{s}{zx}) = \frac{ys}{zx} = z^\beta(\frac{ys}{x}) = z^\beta(y^\alpha(\frac{s}{x})) = (z^\alpha \circ x^\beta)(\frac{s}{x})$$

and so (f) holds.

(e) Since $(x, s) \sim (yx, ys)$, $\frac{ys}{yx} = \frac{s}{x}$. Thus (e) follows from (f).

(g)

$$\tau(ys) = \frac{ysx}{x} = y\frac{sx}{x} = y\tau(s)$$

and so τ is X equivariant. Note that $x(ys) = y(xs)$ and so by (b) $\frac{xs}{x} = \frac{ys}{y}$. Thus τ is independent of x.

(h) Suppose $zs = zt$ for some z in X. Then $\tau(s) = \frac{zs}{z} = \frac{zt}{z} = \tau(z)$. Suppose next that $\tau(s) = \tau(t)$. Then $\frac{xs}{x} = \frac{xt}{x}$ and so $yxxs = yxxt$ for some $y \in X$. Thus $zs = zt$ for $z = yxx$.

(i) follows immediately from (h).

(j) $x^\beta(\tau(s)) = x^\beta(\frac{xs}{x}) = \frac{xs}{xx} = \frac{s}{x}$.

(k) Consider the function:

$$\mu : X \times S \to \tilde{S}, (x, s) \to (x^\diamond)^{-1}(\rho(s))$$

If $(x, s) \sim (y, t)$, then $(y, t) = (zx, zt)$ for some $z \in X$. Thus

$$\begin{aligned}\mu(y, t) &= (y^\diamond)^{-1}(\rho(t)) = (zx)^\diamond)^{-1}(\rho(zs)) = (z^\diamond x^\diamond)^{-1}(z \diamond \rho(x)) \\ &= \big((x^\diamond)^{-1} \circ (z^\diamond)^{-1}\big)(z^\diamond(\rho(x)) = (x^\diamond)^{-1}(\rho(s)) = \mu(x, s)\end{aligned}$$

Since $\approx$ is the equivalence relation generated by $\sim$, 1.5.5(b) shows that γ is well-defined.
Since X is abelian, $xy = yx$ and so also $x^\diamond \circ y^\diamond = y^\diamond \circ x^\diamond$. Since $x^\diamond$ is invertible this implies

$$y^\diamond \circ (x^\diamond)^{-1} = (x^\diamond)^{-1} \circ y^\diamond$$

Thus

$$\gamma(y\frac{s}{x}) = \gamma(\frac{ys}{x}) = (x^\diamond)^{-1}(\rho(ys) = (x^\diamond)^{-1}(y^\diamond(s)) = y^\diamond((x^\diamond)^{-1}(s)) = y \diamond \gamma(\frac{x}{s})$$

and so γ is X-equivariant.

Suppose next that $\delta : X^{-1}S \to \tilde{S}$ is X-equivariant with $\rho = \delta \circ \tau$. Then

$$x \diamond \delta(\frac{s}{x}) = \delta(x\frac{s}{x}) = \delta(\frac{xs}{x}) = \delta(\tau(s)) = \rho(s)$$

and so

$$\delta(\frac{s}{x}) = (x^\diamond)^{-1}(\rho(s)) = \gamma(s)$$

Hence γ is unique. □

Lemma 1.13.7. *Let G be a non-empty semigroup, and S a non-empty subsemigroup of G. Let*

$$\sim\; = \left\{ \big((g, s), (gu, su)\big) \;\Big|\; g \in G, s, u \in S \right\}$$

and note that $\sim$ is a relation on $G \times S$. Let $\approx$ be the relation on $G \times S$ defined by

$$(a, s) \approx (a', s') \quad \textit{if there exists } u \in S \textit{ with } as'u = a'su$$

Then $\approx$ is the equivalence relation generated by $\sim$. For $a \in G$ and $s \in S$ put $\frac{a}{s} = [(a, s)]_\approx$ and $S^{-1}G = (G \times S)/\approx$. Then

(a)

$$S^{-1}G \times S^{-1}G \to S^{-1}G, \quad \left(\frac{a}{s}, \frac{b}{t}\right) \to \frac{as}{bt}$$

is a well defined associative binary operation on $S^{-1}G$.

(b) For each $s \in S$, $\frac{s}{s}$ is an identity in $S^{-1}G$.

(c) For each $s, t \in S$, $\frac{s}{t}$ is an inverse of $\frac{t}{s}$.

(d) Let $s \in S$. Then map $\tau : G \to S^{-1}G, g \to \frac{gs}{s}$ is a homomorphism and independent of the choice of $s \in S$.

(e) $\tau(g) = \tau(h)$ if and only if $gu = hu$ for some $u \in S$.

(f) τ is 1-1 if and only if the Cancellation Law holds for elements in S.

(g) For all $g \in G$, $s \in S$, $\frac{a}{s} = \tau(a)\tau(s)^{-1}$.

(h) Let H be a commutative monoid and $\alpha : G \to H$ be a homomorphism such that each $\alpha(s)$, $s \in S$ is invertible in H. Then

$$\beta : S^{-1}G \to H, \frac{g}{s} \to \alpha(g)\alpha(s)^{-1}$$

is well-defined and is the unique homomorphism from $S^{-1}H$ to G with $\alpha = \beta \circ \tau$.

Proof. □

Chapter 2

Rings

2.1 Rings

Definition 2.1.1. *A* ring *is a tuple* $(R, +, \cdot)$ *such that*

(a) $(R, +)$ *is an abelian group.*

(b) $(R, \cdot)$ *is a semigroup.*

(c) For each $r \in R$ *both left and right multiplication by* r *are homomorphisms of* $(R, +)$

2.1.2 (Ring Axioms)**.** Unwinding definitions we see that a ring is a set R together with two binary operations $+ : R \times R \to R, (a, b) \to a + b$ and $\cdot : R \times R \to R, (a, b) \to ab$ such that

(R1) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$

(R2) There exists $0_R \in R$ with $0_R + a = a = a + 0_R$ for all $a \in R$.

(R3) For each $a \in R$ there exists $-a \in R$ with $a + (-a) = 0_R = (-a) + a$.

(R4) $a + b = b + a$ for all $a, b \in R$.

(R5) $a(bc) = (ab)c$ for all $a, b, c \in R$.

(R6) $a(b + c) = ab + ac$ for all $a, b, c \in R$.

(R7) $(a + b)c = ab + ac$ for all $a, b, c \in R$.

Definition 2.1.3. *Let* R *and* S *be rings.*

(a) A ring homomorphism *is a function* $\phi : R \to S$ *such that*

$$\phi : (R, +) \to (S, +) \quad \textit{and} \quad \phi : (R, \cdot) \to (S, \cdot)$$

are homomorphism of semigroups

(b) A ring homomorphism $\phi : R \to S$ is called an isomorphism if there exists a ring homomorphism $\psi : S \to T$ with $\phi \circ \psi = \mathrm{id}_S$ and $\psi \circ \phi = \mathrm{id}_R$.

(c) R and S are called isomorphic *and we write $R \cong S$ if there exists a ring isomorphism from R to S.*

Note that $\phi : R \to S$ is an homomorphism if and only if $\phi(r + s) = \phi(r) + \phi(s)$ and $\phi(rs) = \phi(r)\phi(s)$ for all $r, s \in R$.

Definition 2.1.4. *Let $(R, +\cdot)$ be a ring.*

(a) An identity *in R is an element 1_R which is an identity for $\cdot$, what is $1_R r = r = r1_R$ for all $r \in R$. If there exists an identity in R we say that R is a ring with identity.*

(b) R is called commutative *if $\cdot$ is commutative, that is $rs = sr$ for all $r, s \in R$.*

In the following lemma we collect a few elementary properties of rings.

Lemma 2.1.5. *Let R be a ring.*

(a) $0a = a0 = 0$ for all $a \in R$

(b) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.

(c) $(-a)(-b) = ab$ for all $a, b \in R$.

(d) $(na)b = a(nb) = n(ab)$ for all $a, b \in R, n \in \mathbb{Z}$.

(e) $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$

Proof. This holds since since right and left multiplication by elements in R are homomorphisms of $(R, +)$. For example any homomorphism sends 0 to 0. So (a) holds. We leave the details to the reader. □

Example 2.1.6. 1. $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are rings

2. Let V be a vector space over $\mathbb{R}$. Let $\mathrm{End}_R(V)$ be set of $\mathbb{R}$-linear maps from V to V. Then $(\mathrm{End}_{\mathbb{R}}(V), +, \circ)$ is a ring called the *endomorphism ring* of V over $\mathbb{R}$.

3. Let $(A, +)$ be any abelian group. Define $\cdot_0 : A \to A, (a, b) \to 0_R$. Then $(A, +, \cdot_0)$ is a ring, called the ring on A with zero-multiplication.

4. Let $(A, +)$ be an abelian group and $\mathrm{End}(A)$ the set of endomorphisms of A, (that is the homomorphisms from A to A). Define

$$(\alpha + \beta)(a) = \alpha(a) + \beta(a) \text{ and } (\alpha \circ \beta)(a) = \alpha(\beta(a))$$

We will show that $(\mathrm{End}(A), +, \circ)$ is a ring (called the *endomorphism ring* of A.)

Let $\alpha, \beta, \gamma \in \operatorname{End}(A)$ and $a, b \in A$. Then

$$\begin{aligned}(\alpha+\beta)(a+b) &= \alpha(a+b)+\beta(a+b) & &= \big(\alpha(a)+\alpha(b)\big)+\big(\beta(a)+\beta(b)\big)\\ &= \big(\alpha(a)+\beta(a)\big)+\big(\alpha(b)+\beta(b)\big) & &= (\alpha+\beta)(a)+(\alpha+\beta)(b)\end{aligned}$$

and so $\alpha+\beta \in \operatorname{End}(A)$

Composition of homomorphisms are homomorphisms and so $\alpha \circ \beta \in \operatorname{End}(a)$. The addition in $\operatorname{End}(A)$ is associative, since the addition on A is associative. The map $A \to A, a \to 0$, is the identity elements. Since A is abelian, the map $-\mathrm{id}_A : a \to -a$ is homomorphism. The $(-\mathrm{id}_A) \circ \alpha : A \to A, a \to -\alpha(a)$ is the additive inverse of α. Composition is always associative.

We compute

$$\begin{aligned}\big((\alpha+b)\circ\gamma\big) &= \big(\alpha+\beta\big)\big(\gamma(a)\big) & &= \alpha\big(\gamma(a)\big)+\beta\big(\gamma(a)\big)\\ &= (\alpha\circ\gamma)(a)+(\alpha\circ\gamma)(a) & &= (\alpha\circ\gamma+\beta\circ\gamma)(a)\end{aligned}$$

and

$$\begin{aligned}\big(\gamma\circ(\alpha+b)\big)a &= \gamma\big((\alpha+\beta)a\big) & &= \gamma(\alpha a+\beta a)\\ &= \gamma(\alpha a)+\gamma(\beta a) & &= (\gamma\circ\alpha)a+(\gamma\circ\beta)a\\ &= (\gamma\circ\alpha+\gamma\circ\beta)a\end{aligned}$$

So $\operatorname{End}(A)$ is indeed a ring.

5. Up to isomorphism there is unique ring with one element:

+	0
0	0

·	0
0	0

6. Up to isomorphism there are two rings of order two :

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0 .
1	0	n

Here $n \in \{0,1\}$. For $n = 0$ this is a ring with zero-multiplication. For $n = 1$ this is $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$.

7. Rings of order 3 up to isomorphism:

$+$	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

$\cdot$	0	1	-1
0	0	0	0
1	0	n	$-n$
-1	0	$-n$	n

Indeed if we define $n = 1 \cdot 1$, then $(-1) \cdot 1 = -(1 \cdot 1) = -n$. Here $n \in \{0, 1, -1\}$. For $n = 0$ this is a ring with zero multiplication. For $n = 1$ this is $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$. For $n = -1$ we see that -1 is an identity and the ring for $n = -1$ is isomorphic to the ring with $n = 1$ case under the bijection $0 \leftrightarrow 0$, $1 \leftrightarrow -1$.

8. Direct products and direct sums of rings are rings. Indeed, let $(R_i, i \in I)$ be a family of rings. For $f, g \in \bigtimes_{i\in I} R_i$ define $f + g$ and fg by

$$(f + g)(i) = f(i) + g(i) \quad \text{and} \quad (fg)(i) = f(i)g(i).$$

With this definition both $\bigtimes_{i\in I} R_i$ and $\bigoplus_{i\in I} R_i$ are rings.

If a is an identity in $\bigtimes_{i\in I} R_i$ or $\bigoplus_{i\in I} R_i$, then for all $i \in I$, a_i is identity in R_i

If each R_i has an identity 1_i, then $(1_i)_{i\in I}$ is an identity of $\bigtimes_{i\in I} R_i$.

If $1_i \neq 0_i$ for infinitely many $i \in I$, then $(1_i)_{i\in I}$ is not in $\bigoplus_{i\in I} R_i$ and $\bigoplus_{i\in I} R_i$ does not have an identity.

If each R_i is commutative then both $\bigtimes_{i\in I} R_i$ and $\bigoplus_{i\in I} R_i$ are commutative.

2.2 Group Rings

Definition 2.2.1. *Let R be a ring and G a semigroup. The* semigroup ring $R[G]$ *of G over R is defined as follows:*

As an abelian group we put $R[G] = \bigoplus_{g\in G} R$. For elements $r = (r_g)_{g\in G}$ and $s = (s_g)_{g\in G}$ of $R[G]$ define $rs \in R[G]$ by

$$(rs)_g = \sum_{\substack{(k,l)\in G\times G \\ kl=g}} r_k s_l$$

for all $g \in G$.

Note that since the $\operatorname{Supp}(r)$ *and* $\operatorname{Supp}(s)$ *are finite, these sums are defined. Also* $\operatorname{Supp}(rs) \subseteq \operatorname{Supp}(r)\operatorname{Supp}(s)$ *and so* $\operatorname{Supp}(rs)$ *is finite and $rs \in R[G]$.*

For $r \in R$ and $g \in G$ we denote the element $\rho_g(r)$[1] *in $R[G]$ by rg so*

$$(rg)_g = r \text{ and } (rg)_h = 0_R \text{ for } h \neq g$$

[1] see 1.9.9

Lemma 2.2.2. *Let R be a ring and G a semigroup.*

(a) $(R[G], +, \cdot)$ *is a ring.*

(b) For each $a \in RG$ *there exist uniquely determined* $r_g \in R$, $g \in G$ *with* $r_g = 0_R$ *for almost all* $g \in G$ *and*

$$a = \sum_{g \in G} r_g g$$

(c) $\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G}(r_g + s_g)g.$

(d) $\sum_{k \in G} r_k k \ \cdot \ \sum_{l \in G} s_l l = \sum_{k \in G, l \in G}(r_k s_l)kl.$

(e) If R and G have identities, then $1_R 1_G$ *is an identity in* $R[G]$.

(f) If R and G are commutative, $R[G]$ *is too.*

Proof. This is Homework 5#1. □

Definition 2.2.3. *A sesquiring is a triple* $(R, G, \cdot)$ *where R is a ring, G is a semigroup and* $\cdot$ *is the binary operation on* $R \times G$ *defined by*

$$(a, g) \cdot (a', g') = (aa', gg').$$

for all $a, a' \in R$ *and* $g, g' \in G$.

So $(R \times G, \cdot)$ *is the direct product of the semigroups* $(R, \cdot)$ *and G.*

Definition 2.2.4. *Let* (R, G) *be a sesquiring and S a ring. A function*

$$f : R \times G \to S$$

is called a sesquihomomorphism if

(i) f is a multiplicative homomorphism, that is

$$f(aa', gg') = f(a, g)f(a', g')$$

for all $a, a' \in R, g, g' \in G$.

(ii) f is an additive homomorphism in the first coordinate. This means that for for each $g \in G$*, the function* $f_g : R \to S, a \to f(a, g)$ *is an additive homomorphism, that is*

$$f(a + a', g) = f(a, g) + f(a', g)$$

for all $a, a' \in R$, $g \in G$.

Lemma 2.2.5. *Let* R, S, T *be rings and G and H semigroups.*

(a) The map $\iota : R \times G \to R[G], (r, g) \to r$ *is a sesquihomomorphism.*

(b) The map $\rho = \rho_{R,G} : R \times G \to R[G], (r,g) \to rg$ is a sesquihomomorphism.

(c) Let $\phi : S \times H \to T$ be a sesquihomomorphism, $\delta : R \to S$ a ring homomorphism and $\epsilon : G \to H$ a semigroup homomorphism. Then

$$\phi \circ (\delta \times \epsilon) : R \times G \to S, (r,g) \to \phi(\delta(r), \epsilon(g))$$

is a sesquihomomorphism.

(d) Let $\phi : R \times G \to S$ be a sesquihomomorphism and $\delta : S \to T$ be a ring homomorphism. Then

$$\delta \circ \phi : R \times S \to T, (r,g) \to \delta(\phi(r,g))$$

is a sesquihomomorphism.

(e) Suppose

$$\tau : R \times G \to S, \quad \sigma : S \times H \to T$$

are sesquihomomorphisms. Define

$$\phi : R \times (G \times H) \to T, (r,g,h) \to \sigma\big(\tau(r,g), h\big)$$

Then ϕ is a sesquihomomorphism.

Proof. (a) ι is clearly a multiplicative homomorphism. (cf. 1.9.6). Also $\iota_g = \mathrm{id}_R$ for all $g \in G$ and so ι_g is an additive homomorphism.

(b) By 2.2.2 $(ag)(a'g') = (aa')(gg')$ and $ag + a'g = (a + a')g$. So ρ is a sesquihomomorphism.

(c) Note that both δ and $\delta \circ \epsilon : R \times G \to S \times H, (r,g) \to (\delta(r), \epsilon(g))$ are multiplicative homomorphisms. So also $\alpha := \phi \circ (\delta \times epsilon)$ is a multiplicative homomorphism. Note that for $g \in G$, $\alpha_g = \delta \circ \phi_{\epsilon(g)}$. Since both δ and $\phi_{\epsilon(g)}$ are additive homomorphism, so is α_g.

(d) $\beta := \delta \circ \phi$ is the composition of two multiplicative homomorphisms and so a multiplicative homomorphism. $\beta_g = \delta \circ \phi_g$ and so β_g is an additive homomorphism.

(e) Note that

$$\delta : R \times (G \times H) \to R \times G, (r,g,h) \to (r,g) \quad \text{and} \quad \epsilon : R \times (G \times H) \to H(r,g,h) \to h.$$

are multiplicative homomorphisms. Hence also the composition $\tau \circ \delta$ and the direct product $(\tau \circ \delta) \times \epsilon$ are multiplicative homomorphism. Thus also

$$\phi = \sigma \circ \big((\tau \circ \delta) \times \epsilon\big)$$

is a multiplicative homomorphism.

Also

$$\phi_{(g,h)}(r) = \sigma\big(\tau(r,g), h\big) = \sigma_h(\tau(r,g)) = \sigma_h(\tau_g(r))$$

and so $\phi_{(g,h)} = \sigma_h \circ \tau_g$ is the composition of two additive homomorphisms and so a homomorphism. □

Lemma 2.2.6. *Let (R,G) be a sesquiring.*

(a) Whenever S is a ring and $\phi : R\times G\to S$ is a sesquihomomorphism, then

$$\alpha : R[G]\to S,\quad \sum_{g\in G} r_g g\ \to\ \sum_{g\in G}\phi(r_g,g)$$

is the unique ring homomorphism from $R[G]$ to S with $\phi = \alpha\circ\rho$.

$$\begin{tikzcd}
S & & R[G] \arrow[ll, "\exists!\alpha"'] \\
& R\times G \arrow[ul, "\phi"] \arrow[ur, "\rho"'] &
\end{tikzcd}$$

(b) Let $\alpha : R[G]\times S$ be a ring homomorphism. Then $\phi = \alpha\circ\rho$ is a sesquihomomorphism from $R\times G$ to S.

Proof. (a) Suppose first $\alpha : R[G]\to S$ is a ring homomorphism with $\phi = \alpha\circ\rho$. Then $\alpha(rg) = \alpha(\rho(r,g)) = \phi(r,g)$ for all $r\in R$, $g\in G$ and so

$$(*)\qquad \alpha\Big(\sum_{g\in G} r_g g\Big) = \sum_{g\in G}\alpha(r_g g) = \sum_{g\in G}\phi(r,g)$$

Thus α is unique. It remains to verify the function

$$\alpha : R[G]\to S,\ \sum_{g\in G} r_g g\to\sum_{g\in G}\phi(r,g)$$

is homomorphism.

We compute

$$\begin{aligned}
\alpha\Big(\sum_{g\in G} r_g g+\sum_{g\in G} s_g g\Big) &= \alpha\Big(\sum_{g\in G}(r_g+s_g)g\Big) && = \sum_{g\in G}\phi(r_g+s_g,g)\\
&= \sum_{g\in G}\big(\phi(r_g,g)+\phi(s_g,g)\big) && = \sum_{g\in G}\phi(r_g,g)+\sum_{g\in G}\phi(s_g,g)\\
&= \alpha\Big(\sum_{g\in G} r_g g\Big)+\alpha\Big(\sum_{g\in G} s_g g\Big)
\end{aligned}$$

$$\begin{aligned}
\alpha\Big(\sum_{k\in G} r_k k \cdot \sum_{l\in G} s_l l\Big) &= \alpha\Bigg(\sum_{g\in G}\Big(\sum_{\substack{(k,l)\in G\times G\\ kl=g}} r_k s_l\Big)g\Bigg) & &= \sum_{g\in G}\phi\left(\sum_{\substack{(k,l)\in G\times G\\ kl=g}} r_k s_l, g\right)\\
&= \sum_{g\in G}\left(\sum_{\substack{(k,l)\in G\times G\\ kl=g}} \phi(r_k s_l, g)\right) & &= \sum_{g\in G}\left(\sum_{\substack{(k,l)\in G\times G\\ kl=g}} \phi(r_k s_l, kl)\right)\\
&= \sum_{(k,l)\in G\times G} \phi(r_k s_l, kl) & &= \sum_{(k,l)\in G\times G} \phi(r_k, k)\phi(s_l, l)\\
&= \sum_{k\in G}\phi(r_k, k) \cdot \sum_{l\in G}\phi(s_l, l) & &= \alpha\Big(\sum_{k\in G} r_k k\Big) \cdot \alpha\Big(\sum_{l\in G} s_l l\Big)
\end{aligned}$$

(b) By 2.2.5(a) is a sesquihomomorphism. Since α is a homomorphism, 2.2.5(d) shows that $\alpha \circ \rho$ is a sesquihomomorphism.

□

Example 2.2.7. *Let (R, G) be a sesquiring. Then*

$$\alpha : R[G] \to R,\ \sum_{g\in G} r_g g \to \sum_{g\in G} r_g$$

is a ring homomorphism. If $G \neq \varnothing$, α is onto.

By 2.2.5(a) $\phi : R \times G \to R,\ (r, g) \to r$ is a sesquihomomorphism. Thus 2.2.6 implies that α is a homomorphism.

Lemma 2.2.8. *Let (R, G) be a sesquiring and S a ring. Let $\beta : R \to S$ be a ring homomorphism and $\gamma : G \to S$ a multiplicative homomorphism such that*

$$\beta(r)\gamma(g) = \gamma(g)\beta(r)$$

for all $r \in R$, $g \in G$. Define

$$\phi : R \times G \to S, (r, g) \to \beta(r)\gamma(g)$$

Then ϕ is a sesquihomomorphism. Moreover

$$\alpha : R[G] \to S,\ \sum_{g\in G} r_g g \to \sum_{g\in G}\beta(r)\gamma(g)$$

is the unique ring homomorphism with $\alpha(rg) = \beta(r)\gamma(g)$ for all $r \in R$, $g \in G$.

Proof.

$$\beta(ab)\gamma(gh) = \big(\beta(a)\beta(b)\big)\big(\gamma(g)\gamma(h)\big) = \big(\beta(b)\gamma(g)\big)\big(\beta(b)\gamma(h)\big)$$

and

$$\beta(a)\gamma(g) + \beta(b)\gamma(g) = \big(\beta(a) + \beta(b)\big)\gamma(g) = \beta(a+b)\gamma(g)$$

So ϕ is a sesquihomomorphism. The second statement now follows from 2.2.6 □

Lemma 2.2.9. *Let (R, G) be sesquiring and S ring. Suppose R and G have identities and $\phi : R\times G \to S$ is a sesquihomomorphism. Define*

$$\beta : R \to S, r \to \phi(r, 1_G) \quad \textit{and } \gamma : G \to S, g \to \phi(1_R, g)$$

Then

(a) β is a ring homomorphism.

(b) γ is a multiplicative homomorphism.

(c) $\beta(1_R) = \gamma(1_G)$.

(d) $\beta(r)\gamma(g) = \phi(r, g) = \gamma(g)\beta(r)$ for all $r \in R$, $g \in G$

Proof. Since ϕ is a multiplication homomorphism and $1 \cdot 1 = 1$, both β and γ are multiplicative homomorphism. Since ϕ is an additive homomorphism in the first coordinate, β is a additive homomorphism. So (a) and (d) hold.

(c): $\beta(1_R) = \phi(1_R, 1_G) = \gamma(1_G)$.

(d):

$$\beta(r)\gamma(g) = \phi(r, 1)\phi(1, g) = \phi(r1, 1g) = \phi(r, g) = \phi(1r, g1) = \phi(1, g)\phi(r, 1) = \gamma(g)\beta(r)$$

□

Example 2.2.10. *Let R and S be rings with zero homomorphism. Let G be semigroup and $(\alpha_g)_{g\in G}$ a family of additive homomorphism from R to S. Define*

$$\alpha : R \times G \to S, (r, g) \to \alpha_g(r)$$

Then α is a sesquihomomorphism.

Since each α_g is an additive homomorphism, α is an additive homomorphism in the first coordinate. Note that $\alpha_g(0_R) = 0_S$ for all $g \in G$ and so

$$\alpha(ab, gh) = \alpha(0, gh) = \alpha_{gh}(0) = 0 = \alpha(a, g)\alpha(b, h)$$

for all $a, b \in R$, $g, h \in R$.

Corollary 2.2.11. *Let (R, G) and (S, H) be sesquirings, $\beta : R \to S$ a ring homomorphism and $\gamma : G \to H$ a semigroup homomorphism. Then*

$$R[G] \to S[H], \quad \sum_{g\in G} r_g g \to \sum_{g\in G} \beta(r)\gamma(g)$$

is the unique ring homomorphism $\alpha : R[G] \to S[H]$ with $\alpha(rg) = \beta(r)\gamma(g)$ for all $r \in R$, $g \in G$.

Proof. Define $\phi : R \times G \to S[H](r,g) \to \beta(r)\gamma(g)$. Note that $\phi = \rho_{S,H} \circ (\beta \times \gamma)$ and so by 2.2.5 ϕ is a sesquihomomorphism. So the Corollary follows from 2.2.6. □

2.2.12 (Identities in Group Rings)**.** If $R[G]$ has an identity and $G \neq \varnothing$, then $\alpha : R[G] \to R, \sum_{g\in G} r_g g \to \sum_{g\in G} r_g$ is an onto homomorphism and so $\alpha(1_{R[G]})$ is an identity in R. But G does not have to have an identity:

Let R be any ring with an identity: Let $G = \{a, b, i\}$ as a set. Define a multiplication by

$$xy = \begin{cases} x & \text{if } x = y \\ i & \text{if } x \neq y \end{cases}$$

Then

$$(xy)z = (xy)z = \begin{cases} x & \text{if } x = y = z \\ i & \text{otherwise} \end{cases}$$

Hence the binary operation is associative and G is a semigroup. Put $r = a + b - i \in R[G]$. We claim that r is an identity. We compute $ar = ra = aa+ab-ai = i+a-i = a$, $br = rb = ba+bb-bi = i+b-i = b$ and $ir = ri = ia + ib - ii = i + i - i = i$. Since right multiplication by r is a additive homomorphism, $\{t \in R[g] \mid tr = t\}$ is a additive subgroup of $R[G]$ and so equal to $R[G]$. Hence r is a right identity. By symmetry, r is also a left identity.

Since $ab = i$ neither a nor b is an identity in G. Since $ai = i$, i is not an identity. So G has no identity.

2.2.13 (Commutative Group Rings)**.** Suppose $R[G]$ is commutative and $G \neq \varnothing$. Then there exists an onto homomorphism from $R[G]$ to R and so R is commutative. Let $r, s \in R$ and $g, h \in G$. Then

$$(rs)(gh) = (rg)(sh) = (sh)(rg) = (sr)(hg) = (rs)(hg).$$

So if $rs \neq 0$ for some $r, s \in R$ we get $gh = hg$ and G is commutative.

But if $rs = 0$ for all $r, s \in R$ then also $xy = 0$ for all $x, y \in R[G]$. So $R[G]$ is commutative, regardless whether G is or not.

Notation 2.2.14. *Let T be a semigroup, $t = (t_i)_{i\in I}$ a commuting family of elements in T, $u \in T$ and $n = (n_i)_{i\in I}$ an almost zero family of non-negative integers. Let $J = \mathrm{Supp}(n) = \{i \in I \mid n_i \neq 0\}$. If $n \neq 0$ (that is $J \neq 0$), define*

$$t^n = \prod_{j\in J} t_j^{n_j}$$

If $n = 0$, define

$$ut^n = u \quad \text{and } t^n u = u$$

If T has an identity and $n = 0$ define $t^n = 1_T$.

Notation 2.2.15. *(a) Let G be monoid and I a set. Then $G_I = \bigoplus_{i\in I} G$.*

(b) (X_I, id_I) is a free abelian monoid on I.

Remark 2.2.16. *Let I be set and put $x = \mathrm{id}_I = (i)_{i\in I}$. Then x is a commuting family in X_I and the function*

$$(\mathbb{N}_I, +) \to (X_I, \cdot), n \to x^n$$

is isomorphism.

Definition 2.2.17. Let R be a ring. Let I be a set. Then the semigroup ring $R[X_I]$ is called the polynomial ring of R in the variables I.

2.2.18 (elements in polynomial rings)**.** Let R be a ring and I a set. Put $x = \mathrm{id}_I = (i)_{i\in I}$ and let $f \in R[X_I]$. Then

$$f = \sum_{n\in\mathbb{N}_I} f_n x^n$$

for a unique almost zero family $(f_n)_{n\in\mathbb{N}_I}$ in R.

If $I = \{x_1, \dots, x_m\}$ this becomes

$$f = \sum_{(n_1,\dots,n_m)\in\mathbb{N}^m} f_{n_1\dots n_m} x_1^{n_1} \dots x_m^{n_m}$$

Lemma 2.2.19. *Let R, S be rings and $s = (s_i)_{i\in I}$ a commuting family of elements in S. Let $\beta : R \to S$ be a ring homomorphism and suppose that*

$$\beta(r)s_i = s_i\beta(r)$$

for all $r \in R$, $i \in I$.

(a)

$$\phi : R \times \mathbb{N}_I, (r, n) \to \beta(r)s^n$$

is a sesquihomomorphism.

(b)

$$\beta_s : R[X_I] \to S, \quad \sum_{n\in\mathbb{N}^I} r_n x^n \ \to \ \sum_{n\in\mathbb{N}_I} \beta(r_n)s^n$$

is the unique homomorphism from $R[X_I] \to S$ with $\beta_s(ri) = \beta(r)s_i$ for all $r \in R$, $i \in I$.

Proof. (a) Since $(s_i)_{i\in I}$ is commuting,

$$\gamma : \mathbb{N}_I^\sharp \to S, n \to s^n$$

is a homomorphism. Applying 2.2.8 we see that the restriction of γ to $R \times \mathbb{N}_I^\sharp$ is a sesquihomomorphism.

Since $\phi(a, 0) = \beta(a)$ is an additive homomorphism, ϕ is a additive homomorphism in the first coordinate.

$$\phi(a,n)\phi(b,0) = \beta(a)s^n\beta(b) = \beta(a)\beta(b)s^n = \beta(ab)s^n = \beta(ab)s^{n+0} = \phi(ab,n+0)$$

and similarly $\phi(a,0)\phi(b,n) = \phi(ab,0+n)$. Finally

$$\phi(a,0)\phi(b,0) = \beta(a)\beta(b) = \beta(ab) = \phi(ab,0+0)$$

and so ϕ is a multiplicative homomorphism.

(b) follows from (a) and 2.2.6(a). □

Notation 2.2.20. *With the notation and assumption from 2.2.19:*

If $f \in R[X_I]$ we write $f_\beta(s)$ for $\beta_s(f)$. In the special case $R \subseteq S$ and $\beta = \mathrm{id}_R$, we write $f(s)$ for $\beta_{\mathrm{id}_R}(f)$.

Remark 2.2.21. *(a) With the notation and assumption from 2.2.20:*

$$(f+g)_\beta(s) = f_\beta(s) + g_\beta(s) \text{ and } (fg)_\beta(s) = f_\beta(s)g_\beta(s)$$

for all $f,g \in R[X_I]$.

(b) Suppose R is a ring with identity and I is set. View R is a subset of r by identifying r with $r1$ and view I is a subset of $R[X_I]$ by identifying i with $1i$. Note that $x = (i)_{i\in I}$ is a commuting family in $R[X_I]$ and $ri = ri$ for all $r \in R$. Then $f(x) = f$ for all $f \in R[X_I]$.

Proof. (a) holds since β_s is a homomorphism.

(b) Put $\beta = \mathrm{id}_R$. By definition β_x is the unique homomorphism from $R[X_I] \to R[X_I]$ with $\beta_x(ri) = \beta(r)x_i$, that is with $\beta_x(ri) = ri$. Hence $\beta_x = \mathrm{id}_{R[X_I]}$ and so $f(x) = \beta_x(f) = f$. □

Lemma 2.2.22. *Let R and S be rings and I a set. Suppose R has an identity and $\phi : R \times \mathbb{N}_I \to S$ is a sesquihomomorphism. Define*

$$\beta : R \to S, r \to \phi(r,0) \quad \text{and} \quad \text{for } i \in I,\ s_i = \phi(1,i)$$

Then

(a) β is a homomorphism of rings.

(b) $(s_i)_{i\in I}$ is commuting family of elements in S.

(c) $\beta(r)s_i = s_i\beta(r)$ for all $r \in R$, $i \in I$.

(d) $\phi(r,n) = \beta(r)s^n$ for all $r \in R$, $n \in \mathbb{N}_I$.

Proof. For $n \in \mathbb{N}$ define $\gamma(n) = \phi(1,n)$. By 2.2.9 β is a ring homomorphism, $\gamma : (N_I, +) \to (S, \cdot)$ is a homomorphism and

$$\beta(r)\gamma(n) = \phi(r,n) = \gamma(n)\beta(n)$$

for all $r \in R$, $n \in N$. In particular, (a) holds.

Note that $\gamma(i) = s_i$ and so also (c) holds.

Since $i + j = j + i$, $s_i s_j = \gamma(i + j) = \gamma(j + i) = s_j s_i$ and (b) is proved.

Since γ is a homomorphism, $\gamma(n) = \gamma\big(\sum_{i\in I} n_i i\big) = \prod_{i\in I} \gamma(i)^{n_i} = s^n$ and so (d) holds. □

2.3 Elementary Properties of Rings

Definition 2.3.1. *Let R be a ring and $a \in R$.*

(a) $R^{\#} = R \smallsetminus \{0\}$.

(b) a is left (right) zero divisor *if $a \neq 0_R$ and there there exists $b \in R^{\#}$ with $ab = 0$ (resp. $ba = 0$). a is a zero divisor if a is a left or a right zero divisor.*

Suppose now that R has an identity.

(c) a is called (left,right,) invertible if it is (left,right,) invertible in $(R, \cdot)$. An invertible element is also called a unit.

(d) $\mathrm{U}(R)$ *is the set of units in R.*

(e) R is called an integral domain *if R is commutative, $1_R \neq 0_R$ and R has no zero-divisors.*

(f) R is called a division ring *if $1_R \neq 0_R$ and all it non-zero elements are invertible. A* field *is a commutative division ring.*

Note that a ring with identity is a zero ring (that is $R = \{0_R\}$ if and only if $1_R = 0_R$. So in (e) and (f) the condition $1_R \neq 0_R$ can be replaced by $R \neq \{0_R\}$.

Lemma 2.3.2. *Let R be a ring. Then the following statements are equivalent:*

(a) R has no right zero-divisors.

(b) If $a, b \in R$ with $ab = 0_R$, then $a = 0_R$ or $b = 0_R$.

(c) R has no left zero-divisors.

(d) The Right Cancellation Law *holds, that is*

$a = b$ for all $a, b, c \in R$ with $c \neq 0$ and $ac = bc$

(e) The Left Cancellation Law *holds, that is*

$a = b$ for all $a, b, c \in R$ with $c \neq 0$ and $ca = cb$

Clearly (a) and (b) are equivalent and similarly (b) and (c) are equivalent.

Suppose that R has no left zero-divisors and $a, b, c \in R$ with $c \neq 0_R$ and $ab = ac$. Then

$$0_R = ac - bc = (a - b)c$$

Since R has no left zero-divisors this implies $a-b = 0_R$ and so $a = b$. Thus the Right Cancellation Law holds.

Suppose the Right Cancellation Law holds and let $a, b \in R$ with $b \neq 0_R$ and $ab = 0_R$. Then $ab = 0_R = 0_R \cdot b$ and so by the Right Cancellation Law, $a = 0_R$. So R has no left zero-divisors. Thus (c) and (d) are equivalent. Similarly (a) and (e) are equivalent.

Example 2.3.3. 1. $\mathbb{R}, \mathbb{Q}$ and $\mathbb{C}$ are fields. $\mathbb{Z}$ is an integral domain.

2. For which $n \in \mathbb{Z}^+$ is $\mathbb{Z}_n$ an integral domain? If $n = 1$, then $\mathbb{Z}_1$ is a zero ring and so not an integral domains. So suppose $n \geq 2$. Then $1 \neq 0$ in $\mathbb{Z}_n$ and thuas Z_n is an integral domain if and only,

$$n \mid kl \Longrightarrow n \mid k \text{ or } n \mid l$$

and so if and only if n is a prime. The following lemma implies that $\mathbb{Z}/p\mathbb{Z}$ is a field for all primes p.

3. Let R is be an integral domain and G an abelian monoid. Is $R[G]$ an integral domain?

We will first show:

1°. *Suppose there exists $a, b, c \in G$ and $n \in \mathbb{Z}^+$ with $a \neq b$ and $a^n c = b^n c$. Then c or $a - b$ is a zero divisor. In particular, $R[G]$ is not an integral domain.*

Assume first that $a^n \neq b^n$. Then $a^n - b^n \neq 0$ in $R[G]$ and

$$(a^n - b^n)c = a^n c - b^n c = 0$$

so c is a zero divisor.

Assume next that $a^n = b^n$ and choose k minimal with $a^k = b^k$. Let $0 \leq m < k$ and define

$$\tau(m) = \sum_{i=0}^{m} a^i b^{m-i}$$

Then

$$(a - b)\tau(m) = (a - b)\sum_{i=0}^{m} a^i b^{m-i} = a^{m+1} - b^{m+1}$$

and so

$$(a-b)\tau(k-1)=0$$

If $\tau(k-1)\neq 0$, $a-b$ is a zero divisor.

So suppose that $\tau(k-1)=0$. Then we choose $l\in\mathbb{N}$ minimal with $a^j\tau(l)=0$ for some $j\in\mathbb{N}$. Looking at the coefficients of a^{j+l} in $a^j\tau(l)$ we see that $a^{j+l}=a^{j+l-i}b^i$ for some $1\leq i\leq l$. Hence $a^{j+l-i}a^i=a^{j+l-i}b^i$. Put $t=j+l-i$. Then $a^ta^i=a^tb^i$ and so and

$$0=a^ta^i-a^lb^i=a^t(a^i-b^i)=a^t\tau(i-1)(a-b)$$

Note that $i-1<i\leq l$ and so by minimality of l, $a^t\tau(i-1)\neq 0$. Thus $a-b$ is a zero divisor.

2°. *Suppose that*

$$(*) \qquad a^nc\neq b^nc$$

for all $a,b,c\in G$ and $n\in\mathbb{Z}^+$ with $a\neq b$. Then $R[G]$ is an integral domain.

We will only outline a proof (and use a couple of result proven later).

The special case $n=1$ in (*) shows that the cancellation law holds in G. So by 2.7.1 there G can be embedded an abelian group H such that $H=\{ab^{-1}\mid a,b\in G\}$. H is a group. If $(ab^{-1})^n=1$ for some $a,b\in G$ and $n\in\mathbb{Z}^+$, then $a^n=b^n$, and (*) applied with $c=1$, gives $a=b$ and $ab^{-1}=1$. Thus H has no-nontrivial elements of finite order and since H is a group we conclude that (*) holds for H. So we may assume from now on that G is a group.

Let $r,s\in R[G]$ with $r\neq 0$ and $s\neq 0$. We need to show that $rs\neq 0$. Let $F=\langle g,h\in G\mid r_g\neq 0, s_h\neq 0\rangle$. Replacing G by F we may assume that G is finitely generated. Since G has no non-trivial elements of finite order a theorem proved sometime later will show that $G\cong\mathbb{Z}^m$ for some $m\in\mathbb{N}$. So we may assume that $G=\mathbb{Z}^m$. Since $\mathbb{Z}^{m+1}=\mathbb{Z}^m\times\mathbb{Z}$, $R[\mathbb{Z}^{m+1}]\cong R[\mathbb{Z}^m][\mathbb{Z}]$ (see Homework 5) and so by induction we may assume that $m=1$. Let $x=1\in G$. Then $r=\sum_{i=k}^n r_ix^i$ for some $k\leq n\in\mathbb{Z}$ and $r_i\in R$ with $r_n\neq 0_R$ and $s=\sum_{j=l}^m s_jx^j$ for some $l\leq m\in\mathbb{Z}$ and $s_j\in R$ with $s_m\neq 0_R$. Then the coefficient of x^{n+m} in rs is r_ns_m and since R is an integral domain $r_ns_m\neq 0$ and so also $xy\neq 0$.

Lemma 2.3.4. *All finite integral domains are fields*

Proof. Let R be a finite integral domain and $a\in R^\#$. As R is an integral domain, multiplication by a is a one to one map from $R^\#\to R^\#$. As R is finite, this map is onto. Thus $ab=1_R$ for some $b\in R$. Since R is commutative $ba=1-R$ and so all non-zero elements are invertible. □

For a ring R we define the *opposite ring* R^{op} by $(R^{\mathrm{op}},+^{\mathrm{op}})=(R,+)$, and $a\cdot^{\mathrm{op}}b=b\cdot a$. If R and S are rings then a map $\phi:R\to S$ is called an *anti-homomorphism* if $\phi:R\to S^{\mathrm{op}}$ is ring homomorphism. So $\phi(a+b)=\phi(a)+\phi(b)$ and $\phi(ab)=\phi(b)\phi(a)$.

Let $\mathrm{End}(R)$ be the set of ring homomorphism. Then $\mathrm{End}(R)$ is monoid under composition. But as the sum of two ring homomorphisms usually is not a ring homomorphism, $\mathrm{End}(R)$ has no natural structure as a ring.

The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \quad m \to m + n\mathbb{Z}$ is a ring homomorphism.

For $r \in R$ let $\mathcal{R}_r : R \to R, s \to sr$ and $\mathcal{L}_r : R \to R, s \to rs$. By definition of a ring $\mathcal{R}_a$ and $\mathcal{L}_r$ are homomorphisms of $(R, +)$. But left and right multiplication usually is not a ring homomorphism. The map $\mathcal{L} : R \to \mathrm{End}((R, +)), r \to \mathcal{L}_r$ is a homomorphism but the map $\mathcal{R} : R \to \mathrm{End}((R, +)), r \to \mathcal{R}_r$ is an anti-homomorphism. Note that if R has an identity, then both $\mathcal{R}$ and $\mathcal{L}$ are one to one.

Definition 2.3.5. *(a) Let G be a group We say that G has finite* exponent *of there exists $n \in \mathbb{Z}^+$ with $g^n = e$ for n for all $g \in G$. If G has finite exponent then exponent* $\exp(G)$ *of G is the smallest positive integer m with $g^m = 1$ for all $g \in G$, otherwise* $\exp(G) = \infty$.

(b) Let R be a ring. If $(R, +)$ is has finite exponent then the characteristic $\mathrm{char} R$ *of R is the exponent of $(R, +)$. If $(R, +)$ has infinite exponent then* $\mathrm{char} R = 0$.

Lemma 2.3.6. *Let R be a ring with identity.*

(a) Let $n \in \mathbb{Z}$ then $n1_R = 0_R$ if and only if $nr = 0_R$ for all $r \in R$.

(b) Suppose $1_R \neq 0_R$ and that R has no zero-divisors. Then $\mathrm{char} R$ *is 0 or a prime.*

Proof. (a) If $nr = 0_R$ then clearly $n1_R = 0_R$. So suppose $n1_R = 0_R$. Then for all $r \in R$

$$nr = n(1_R r) = (n1_R)r = 0_R r = 0_R$$

(b) Suppose $n := \mathrm{char} R \neq 0$. If $n = 1$, then $0_R = 1 \cdot 1_R = 1_R$, contrary to the assumptions. So $n > 1$. Let $n = st$ with $s, t \in \mathbb{Z}^+$. Then

$$0_R = n1_R = (st)1_R = st1_R 1_R = (s1_R)(t1_R)$$

Since R has no zero divisors we conclude that $s1_R = 0_R$ or $t1_R = 0_R$. The minimality n implies $s = n$ or $t = n$. Hence n is a prime. □

Let $r \in R$. If R has an identity we define $r^0 = 1$. If R does not have an identity we will use the convention $r^0 s = s$ for all $s \in R$.

Lemma 2.3.7 (Binomial Theorem). *Let R be ring, $a_1, a_2 \ldots, a_n \in R$ and $m \in \mathbb{Z}^+$.*

(a)

$$(\sum_{i=1}^{n} a_i)^m = \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} \ldots \sum_{i_m=1}^{n} a_{i_1} a_{i_2} \ldots a_{i_m}$$

(b) If $a_i a_j = a_j a_i$ for all $1 \leq i, j \leq n$, then

$$(\sum_{i=1}^{n} a_i)^m = \sum_{\{(m_i) \in \mathbb{N}^n \mid \sum_{i=1}^{n} m_i = m\}} \binom{m}{m_1, m_2, \ldots, m_n} a_1^{m_1} a_2^{m_2} \ldots a_n^{m_n}$$

Proof. (a) Follows form 2.1.5e and induction on m.

For (b) notice that $a_{i_1}\dots a_{i_m} = a_1^{m_1}a_2^{m_2}\dots a_n^{m_n}$, where $m_k = |\{j \mid i_j = k\}|$. So (b) follows from (b) and a simple counting argument. □

Lemma 2.3.8. *Let $n, m, k \in \mathbb{Z}^+$.*

(a) If $\gcd(m,k) = 1$ *or* $\gcd(n,m) = 1$*, then* $\gcd(f,k) = 1$ *for some $f \in \mathbb{Z}$ with $f \equiv n \pmod{m}$.*

(b) There exists $f \in \mathbb{Z}$ so that $\gcd(f,k) = 1$ *and* $fn \equiv \gcd(n,m) \pmod{m}$

Proof. (a) Suppose first that $\gcd(m,k) = 1$. Then $1 - n = lm + sk$ for some integers l, s. Thus $1 = (n + lm) + sk$. Put $f = n + lm$, then $\gcd(n + lm, k) = 1$.

Suppose next that $gcd(n,m) = 1$. Write $k = k_1k_2$ where $\gcd(k_1,m) = 1$ and all primes dividing k_2 also divide m. By the first part there exists $l \in \mathbb{Z}$ with $\gcd(n+lm, k_1) = 1$. Now any prime dividing k_1, divides m and (as $\gcd(n,m) = 1$), does not divide m. Hence it also does not divide $m + lm$. Thus $\gcd(n + lm, k) = \gcd(n + lm, k_1) = 1$.

(b) Let $d = \gcd(n,m)$. Replacing n be $\frac{n}{d}$ and m by $\frac{m}{d}$ we may assume that $d = 1$. Then $n^*n \equiv 1 \pmod{m}$ for some $n^* \in \mathbb{Z}$. Since $\gcd(n^*, m) = 1$ we can apply (a) to n^*, m and k. So there exists f with $\gcd(f,k) = 1$ and $f \equiv n^* \pmod{m}$. Then also $fn \equiv 1 \pmod{m}$. □

Lemma 2.3.9. *Let R be a ring with $(R,+)$ cyclic. Then R is isomorphic to exactly one of the following rings:*

1. *$\mathbb{Z}$ with regular addition but zero-multiplication.*

2. *$(n\mathbb{Z}/nm\mathbb{Z}, +, \cdot)$, where $m \in \mathbb{N}, n \in \mathbb{Z}^+$ and n divides m.*

Proof. Let $m \in \mathbb{N}$ so that $(R,+) \cong (\mathbb{Z}/m\mathbb{Z}, +)$ and let a be generator for $(R,+)$. So $a \cdot a = na$ for some $n \in \mathbb{Z}$. Then for all $k, l \in \mathbb{Z}$, $(ka)\cdot(la) = klna$ and so the multiplication is uniquely determine by n. Note that $(-a)(-a) = na = (-n)(-a)$. So replacing a be $-a$ we may assume that $n \in \mathbb{N}$. Also if $m > 0$ we may choose $0 < n \leq m$.

Suppose first that $n = 0$. Then by our choice $m = 0$ as well. So $(R,+) \cong (\mathbb{Z},+)$ and $rs = 0$ for all $r, s \in R$.

Suppose next that $n > 0$. Then the map

$$n\mathbb{Z}/nm\mathbb{Z} \to R, \quad nk + nm\mathbb{Z} \to ka$$

is an isomorphism. If $m = 0$, these rings are non-isomorphic for different n. Indeed $R^2 = nR$ and so $|R/R^2| = n$. Therefore n is determined by the isomorphism type R.

For $m > 0$, various choices of n can lead to isomorphic rings. Namely the isomorphism type only depends on $d = \gcd(n,m)$. To see this we apply 2.3.8 to obtain $f \in \mathbb{Z}$ with $\gcd(f,m) = 1$ and $fn \equiv d \pmod{m}$. Then $1 = ef + sm$ for some $e, s \in \mathbb{Z}$ and so $f + m\mathbb{Z}$ is invertible. Hence also fa is a generator for $(R,+)$ and

$$(fa)\cdot(fa) = f^2na = (fn)(fa) = d(fa).$$

Also $R^2 = dR$ and $|R/R^2| = \frac{m}{d}$. So d is determined by the isomorphism type of R. □

2.4 Ideals and homomorphisms

Definition 2.4.1. *Let $(R,+,\cdot)$ be ring.*

(a) A subring of R is a ring $(S,\triangle,\Box)$ such that $S\subseteq R$, and

$$s\triangle t = s+t \quad \textit{and} \quad s\,\Box\, r = s\cdot t$$

for all $s,t\in S$

(b) A left (right) ideal *in R is a subring I of R so that $rI\subseteq I$ $(Ir\subseteq I)$ for all $r\in R$.*

(c) An ideal in R is a subring of R which is left and right ideal in R.

Lemma 2.4.2. *Let $(R,+,\cdot)$ be a ring and $S\subseteq R$. The $(S,+,\cdot)$ is a subring of R if and only if*

(i) $0_R\in S$.

(ii) $a+b\in S$ *for all* $a,b\in S$.

(iii) $-a\in S$ *for all* $a\in S$.

(iv) $ab\in S$ *for all* $a,b\in S$.

Proof. Straightforward and we leave the few details to the reader. □

Example 2.4.3. 1. Let $n\in\mathbb{Z}$. Then $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

2. Let V be a vector space over $\mathbb{R}$. Let W be any subset Define

$$\mathrm{Ann}(W)=\{\alpha\in\mathrm{End}_{\mathbb{R}}(V)\mid\alpha(w)=0_V \text{ for all } w\in W\}.$$

Ann(W) is called the annihilator of W in End(W). We will show that Ann(W) is left ideal in End$_{\mathbb{R}}(V)$.

Let $\alpha,\beta\in\mathrm{Ann}(W)$, $\gamma\in\mathrm{End}_{\mathbb{R}}(V)$ and $w\in W$, then

$$0_{\mathrm{End}_{\mathbb{R}}(V)}(w)=0_W$$
$$(\alpha+\beta)(w)=\alpha(w)+\beta(w)=0_V+0_V=0_V$$
$$(\gamma\circ\alpha)(w)=\gamma(\alpha(w)=\gamma(0_V)=0_V$$

and so by 2.4.2 Ann(W) is an ideal.

Lemma 2.4.4. *Let $\phi: R\to S$ be a ring homomorphism.*

(a) If T is a subring of R, $\phi(T)$ is a subring of S.

(b) If T is a subring of S then $\phi^{-1}(T)$ is a subring of R.

(c) $\ker\phi$ *an ideal in R.*

(d) If I is an (left,right) ideal in R and ϕ is onto, $\phi(I)$ is a (left,right) ideal in S.

(e) If J is a (left,right) ideal in S, then $\phi^{-1}(J)$ is an (left,right) ideal on R.

Proof. Straight forward. □

Example 2.4.5. Let (R,G) be a sesquiring with $G \neq \emptyset$.

(a) By Example 2.2.7

$$\alpha : R[G] \to R, \sum r_g g \to \sum r_g.$$

is an onto ring homomorphism. The kernel of α is

$$R^\circ[G] := \left\{\sum r_g g \mid \sum r_g = 0\right\}$$

$R^\circ[G]$ is called the *augmentation ideal* of $R[G]$.

(b) Let $\beta : R \to S$ be a ring homomorphism and $\gamma : G \to H$ a semigroup homomorphism. Then by 2.2.8

$$\alpha : R[G] \to S[H], \quad \sum_{g\in G} r_g g \to \sum_{g\in G} \beta(r_g)\gamma(g)$$

is a ring homomorphism. What is the image and the kernel of γ? Clearly $\alpha(R[G]) = \beta(R)[\gamma(G)]$. Let $I = \ker\beta$. To compute $\ker\alpha$ note that

$$\alpha\left(\sum_{g\in G} r_g g\right) = \sum_{h\in H} \beta\left(\sum_{g\in\gamma^{-1}(h)} r_g\right) h$$

and so

$$\sum_{g\in G} r_g g \in \ker\alpha \qquad \iff \qquad \sum_{g\in\gamma^{-1}(h)} r_g \in I \quad \text{for all } h \in \gamma(G).$$

If γ is a group homomorphism we can describe $\ker\alpha$ just in terms of $I = \ker\beta$ and $N := \ker\gamma$. Indeed the $\gamma^{-1}(h)$'s ($h \in \gamma(G)$) are just the cosets of N and so

$$\sum_{g\in G} r_g g \in \ker g \qquad \iff \qquad \sum_{g\in T} r_g \in I \quad \text{for all } T \in G/N.$$

Definition 2.4.6. *Let R be a ring and $A, B \subseteq R$. Then*

(a) $\langle A\rangle$ *is subgroup of* $(R,+)$ *generated by A.*

(b)

$$\llbracket A\rrbracket = \bigcap\{I \mid I \textit{ is an ideal in } R, A \subseteq I\}$$
$$\llbracket A) = \bigcap\{I \mid I \textit{ is a left ideal in } R, A \subseteq I\}$$
$$(A\rrbracket = \bigcap\{I \mid I \textit{ is right ideal in } R, A \subseteq I\}$$

$\llbracket A\rrbracket$, $\llbracket A)$, $\langle A\rrbracket$ *are called the ideal, left ideal and right ideal, respectively, in R generated by A.*

Lemma 2.4.7. *Let R be a ring, $A, B, C \subseteq R$ and $r \in R$.*

(a) $\langle A, B\rangle = \langle A\rangle + \langle B\rangle$.

(b) $r\langle A\rangle = \langle rA\rangle$ *and* $\langle A\rangle r = \langle Ar\rangle$.

(c) $\langle AB\rangle = \big\langle A\langle B\rangle\big\rangle = \big\langle\langle A\rangle\langle B\rangle\big\rangle = \big\langle\langle A\rangle B\big\rangle$.

(d) If A is a left ideal, then $\langle AB\rangle$ *is a left ideal.*

(e) If B is a right ideal, then $\langle AB\rangle$ *is a right ideal.*

(f) If A is a left ideal in R and B is right ideal, then $\langle AB\rangle$ *is an ideal in R.*

(g) If $(A_i)_{i\in I}$ *be a family of (left,right,) ideals of R, then* $\langle A_i, i \in I\rangle$ *is a (left,right,) ideal.*

(h) Let $(A_i)_{i\in I}$ *be a family of (left,right,) ideals of R, then* $\bigcap_{i\in I} A_i$ *is a (left,right) ideal.*

(i) $\llbracket A)$ *is a left ideal in R,* $\llbracket A) = \langle RA, A\rangle$ *and if R has a left identity then* $\llbracket A) = \langle RA\rangle$.

(j) $(A\rrbracket$ *is a right ideal in R,* $(A\rrbracket = \langle AR, A\rangle$ *and if R has a right identity then* $(A\rrbracket = \langle AR\rangle$.

(k) $\llbracket A\rrbracket$ *is an ideal in R,* $\llbracket A\rrbracket = \langle RAR, RA, AR, A\rangle$ *and R has an identity, then* $\llbracket A\rrbracket = \langle RAR\rangle$.

(l) If R is commutative $\big\langle\llbracket A\rrbracket\llbracket B\rrbracket\big\rangle = \llbracket AB\rrbracket$.

Proof. Let $r \in R, a \in A$ and $b \in B$.

(a) Since + is commutative, $\langle A\rangle + \langle B\rangle$ is an additive subgroup of R and so (a) holds.

(b) Since left and right multiplication by r are additive homomorphism, (d) follow from conclude from 1.8.5(c).

(c) By (b) $a\langle B\rangle = \langle aB\rangle \leq \langle AB\rangle$ and so

$$(*) \qquad \big\langle A\langle B\rangle\big\rangle = \langle AB\rangle$$

(*) applied to opposite ring gives $\big\langle\langle A\rangle B\big\rangle = \langle AB\rangle$.

(*) applied to $\langle A\rangle$ in place of A yields $\big\langle\langle A\rangle\langle B\rangle\big\rangle = \langle\langle A\rangle B\rangle$ and so (c) holds.

(d) Since A is a left ideal $RA \subseteq A$. So using (c)

$$R\langle AB\rangle \subseteq \langle RAB\rangle \subseteq \langle AB\rangle$$

and so $\langle AB\rangle$ is left ideal.

(e) Apply (d) to the opposite ring.

(f) Follows from (d) and (e).

(g) Suppose $(A_i)_{i\in I}$ is a family of left ideal in R. Then by (c)

$$R\langle A_i, i\in I\rangle \subseteq \langle RA_i, i\in I\rangle \subseteq \langle A_i, i\in I\rangle$$

and so $\langle A_i, i\in I\rangle$ is a left ideal. Applying this statement to the opposite ring completes the proof of (g).

(h) Suppose each A_i is an left ideal. By 1.8.3 $\bigcap_{i\in I} A_i$ is subgroup of $(R,+)$. Let $a\in\bigcap_{i\in I} A_i$. Then $a\in A_i$ and so $ra_i\in A_i$ for all $i\in I$. Thus $ra_i\in\bigcap_{i\in I} A_i$ and so $\bigcap_{i\in I} A_i$ is a left ideal. Applying this statement also to the opposite ring completes the proof of (g).

(i) Clearly $\langle RA, A\rangle$ is contained in every left ideal containing A, and so also $(\!|A)$. So it suffices to show that $\langle RA, A\rangle$ is left ideal. We have

$$R(RA\cup A) = RRA\cup RA = RA$$

and so by (c), $R\langle RA, A\rangle\subseteq\langle RA\rangle\subseteq\langle RA, A\rangle$.

If R has an left identity l, , then $A = lA\subseteq RA$ and so $\langle RA, A\rangle = \langle RA\rangle$

(j) Apply (i) to the opposite ring.

(k) By definition $(\!|A|\!)$ is an intersection of ideals and so by (h), is an ideal.

$$(**)\qquad \langle RAR, AR, RA, A\rangle = \langle R(AR\cup A), (AR\cup A)\rangle$$

and so by (i) $\langle RAR, AR, RA, A\rangle$ is a left ideal and so (after applying this to the opposite ring) is an ideal in R. $\langle RAR, AR, RA, A\rangle$ is contained in any ideal containing A and the first statement in (k) holds.

If R has an identity, $A\cup AR\cup A\cup RAR = 1A1\cup 1AR\cup 1A1\cup RAR = RAR$ and also the second statement holds.

(l) Since R is commutative $(\!|A|\!) = \langle A, RA\rangle$ and so using (c)

$$\big\langle (\!|A|\!)(\!|B|\!)\big\rangle = \big\langle\langle A, RA\rangle\langle B, RB\rangle\big\rangle = \langle AB, RAB, ARB, RARB\rangle = \langle AB, RAB, RRAB\rangle = \langle AB, RAB\rangle = (\!|AB|\!)$$

□

Lemma 2.4.8. *Let I be an ideal in the ring R.*

(a) The binary operations

$$\begin{aligned} +_{\cdot R/I} &: R/I\times R/I\to R/I, & (a+I, b+I) &\to (a+b)+I \quad \textit{and}\\ \cdot_{R/I} &: R/I\times R/I\to R/I, & (a+I, b+I) &\to ab+I \end{aligned}$$

are well-defined.

(b) $(R/I, +_{R/I}, \cdot_{R/I})$ *is a ring.*

(c) The map

$$\pi : R \to R/I, \quad r \to r + I$$

is a ring homomorphism with kernel I.

Proof. (a) That $+_{R/I}$ is well-defined follows from 1.6.10. $i, j \in I$. Then $(a+i)(b+j) = ab+ib+aj+ij$. As I is an ideal, $ib + aj + ij \in I$ and so $(a + i)(b + j) + I = ab + I$. Thus also $\cdot_{R/N}$ is well-defined.

(b) By 1.6.10 $(R/I, +)$ is a group. The remaining axiom of a ring are readily verified.

(c) By 1.6.10 is a well-defined homomorphism of abelian groups with $\ker\pi = I$. Since

$$\phi(ab) = ab + I = (a + I) \cdot_{R/I} (b + I) = \pi(a) \cdot_{R/I} \pi(b)$$

and so π is ring homomorphism. □

Remark 2.4.9. *(a) Let $A, B \in R/I$. Note that A, B is are subsets of R and so $A \cdot B = \{a \cdot b \mid a \in A, b \in B\}$. In general, $A \cdot_{R/I} B$ is not equal to $A \cdot B$.*

(b) If a, b are elements of R/I denoted by lower case letters, then ab is understood to mean $a \cdot_{R/I} b$ and not $a \cdot b$.

Consider for example $R = \mathbb{Z}$ and $A = B = I = 2\mathbb{Z}$. Then

$$2\mathbb{Z} \cdot 2\mathbb{Z} = 4\mathbb{Z} \text{ and } 2\mathbb{Z} \cdot_{Z/2\mathbb{Z}} 2\mathbb{Z} = (0 + 2\mathbb{Z}) \cdot_{\mathbb{Z}/2\mathbb{Z}} (0 + 2\mathbb{Z}) = 0 + 2\mathbb{Z} = 2\mathbb{Z}$$

Theorem 2.4.10 (The Isomomorphism Theorem for Rings)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then the map*

$$\overline{\phi} : R/\ker\phi \to \phi(R), \quad r + \ker\phi \to \phi(r)$$

is a well-defined isomorphism of rings.

Proof. By the Isomorphism Theorem for groups 1.6.11, this is a well-defined isomorphism for the additive groups. We have

$$\overline{\phi}((a + \ker\phi)(b + \ker\phi)) = \overline{\phi}(ab + \ker\phi) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(a + \ker\phi)\overline{\phi}(b + \ker\phi)$$

and $\overline{\phi}$ is a ring isomorphism. □

We will see below that any ring R can be embedded into a ring S with an identity. This embedding is somewhat unique. Namely suppose that $R \leq S$ and S has an identity. Then for $n, m \in \mathbb{Z}$ and $r, s \in R$ we have $(n1+r)+)(m1+s) = (n+m)1+(r+s)$ and $(n1+r)(m1+s) = (nm)1+(mr+ns+rs)$. So already $\mathbb{Z}1 + R$ is a ring with 1, contains R and the addition and multiplication on $\mathbb{Z}1 + R$ is uniquely determined. But there is some degree of freedom. Namely $\mathbb{Z}1 + R$ does not have to be a direct sum.

Let $\hat{R} = \mathbb{Z} \times R$ as abelian groups. We make $\hat{R}$ into a ring by defining

$$(n, r) \cdot (m, s) = (nm, ns + mr + rs).$$

Then $(1,0)$ is an identity in $\hat{R}$. The map $\phi : \hat{R} \to S, (n,r) \to n1 + r$ is a homomorphism with image $\mathbb{Z}1 + R$. Let us investigate $\ker\phi$. $(n,r) \in \ker\phi$ iff $r = -n1$. Let $k\mathbb{Z}$ be the inverse image of $\mathbb{Z}1 \cap R$ in $\mathbb{Z}$. Also put $t = k1$ and $D_{k,t} = \{(lk, -lt) \mid l \in \mathbb{Z}\}$. Then $\ker\phi = D_{k,t}$. Hence $\hat{R}/D_{k,t} \cong \mathbb{Z}1 + R$.

Now which choices of $k \in \mathbb{Z}$ and $t \in R$ can really occur? Note that as $t = -n1$, $tr = kr = rt$. This necessary condition on k and t turns out to be sufficient:

Let $k \in \mathbb{Z}$. $t \in R$ is called a k-element if $tr = rt = kr$ for all $r \in R$. Note that a 1-element is an identity, while a 0-element is an element with $tR = Rt = 0$. Also if a and b are k-elements, then $a - b$ is a 0-element. So if a k-elements exists it unique modulo the zero elements.

Suppose now that t is a k-element in R. Define $D_{t,k}$ has above. We claim that $D_{k,t} = \mathbb{Z}(k, -t)$ is an ideal in R. For this we compute(using $rt = kr$)

$$(n,r)\cdot(k,-t) = (nk, kr - nt - rt) = (nk, kr - nt - kr) = (nk, -nt) = n(k,-t).$$

So $D_{k,t}$ is a left ideal. Similarly, $D_{t,k}$ is a right ideal. Put $R_{k,t} = \hat{R}/D_{k,t}$. Then $R_{k,t}$ is a ring with identity, contains R (via the embedding $r \to (0,r) + D_{k,t}$) and fulfills $\mathbb{Z}1 \cap R = k\mathbb{Z}1 = \mathbb{Z}t$.

Note that if t is an k-element and s an l-element, then $-t$ is an $-k$ element and $t + s$ is an $(k+l)$-element. Therefore the sets of $k \in \mathbb{Z}$ for which there exists a k-element is a subgroup of $\mathbb{Z}$ and so of the form $i\mathbb{Z}$ for some $i \in \mathbb{N}$. Let u be a i-element. $R_{i,u}$ is in some sense the smallest ring with a identity which contains R. Also if R has no 0-elements, u and so $R_{i,u}$ is uniquely determined.

For example if $R = n\mathbb{Z}$, then $i = n = u$ and $R_{i,u} \cong \mathbb{Z}$. Indeed $\hat{R} = \mathbb{Z}\times n\mathbb{Z}$, $D_{nn} = \{(jn, -jn) \mid j \in \mathbb{Z}\}$, $\hat{R} = \mathbb{Z}(1,0)\mathrm{op}lusD_{n,n}$ and the map $R_{n,n} \to \mathbb{Z}$, $(j,r) + D_{n,n} \to j + r$ is an isomorphism between $R_{n.n}$ and $\mathbb{Z}$.

Next we will show that R can be embedded into a ring with identity which has same characteristic as R. Put $n = \mathrm{char} R$, then 0 is an n-element. Also $D_{n,0} = n\mathbb{Z} \times \{0\}$ and $R_{n,0} \cong \mathbb{Z}/n\mathbb{Z} \times R$ as abelian groups. So $R_{n,0}$ has characteristic n. On the other hand $\hat{R} = R_{0,0}$ always has characteristic 0.

Definition 2.4.11. *Let I be an ideal in the ring R with $I \neq R$.*

(a) I is prime ideal *if for all ideals A, B in R*

$$AB \subseteq I \qquad \Longrightarrow \qquad A \leq I \text{ or } B \leq I$$

(b) I is a maximal ideal *if for each ideal A of R.*

$$I \subseteq A \subseteq R \qquad \Longrightarrow \qquad A = I \quad or \quad A = R.$$

Example 2.4.12. Let I be an ideal in $\mathbb{Z}$ with $I \neq \mathbb{Z}$. Then I is a subgroup of $\mathbb{Z}$ and so $I = n\mathbb{Z}$ for some $n \in \mathbb{N}$ with $n \neq 1$. Let $A = a\mathbb{Z}$ and $B = b\mathbb{Z}$ with $a, b \in \mathbb{N}$. Then $AB = ab\mathbb{Z}$ and so $AB \leq I$ if and only if $n \mid ab$. Also $n\mathbb{Z} \leq a\mathbb{Z}$ if and only if $n \mid a$. Thus I is a prime ideal if and only if

$$n \mid ab \Longrightarrow n \mid a \text{ or } n \mid a$$

This is this is case if and only if $n = 0$ or n is a prime. So the prime ideals in $\mathbb{Z}$ are $\{0\}$ and $p\mathbb{Z}$, p a prime.

I is a maximal ideal if and only if $n\mathbb{Z} \leq a\mathbb{Z}$ implies $n\mathbb{Z} = a\mathbb{Z}$ or $a\mathbb{Z} = \mathbb{Z}$. So if and only if $a \mid n$ implies $n = a$ or $n = 1$. This is the case if and only if n is a prime. So the maximal ideals in $\mathbb{Z}$ are $p\mathbb{Z}$, p a prime.

Lemma 2.4.13. *Let P be an ideal in the ring R with $P \neq R$. Suppose that for all $a, b \in R$,*

$$ab \in P \qquad \Longrightarrow \qquad a \in P \quad or \quad b \in P$$

then P is a prime ideal

Proof. Let A and B are ideals in R with $AB \leq P$. We need to show that $A \leq P$ or $B \leq P$. So suppose $A \nleq P$ and pick $a \in A \setminus P$. Since $ab \in P$ for all $b \in B$ we conclude $b \in P$ and $B \leq P$. □

Lemma 2.4.14. *Let P be an ideal in the commutative ring R with $P \neq R$. Then the following statements are equivalent:*

(a) R is a prime ideal.

(b) For all $a, b \in R$,

$$ab \in P \qquad \Longrightarrow \qquad a \in P \quad or \quad b \in P$$

(c) R/P has no zero divisors.

Proof. (a) $\Longrightarrow$ (b): Suppose that P is prime ideal and let $a, b \in R$ with $ab \in P$. By 2.4.7(l)

$$\left\langle \llparenthesis a \rrparenthesis \llparenthesis b \rrparenthesis \right\rangle = \llparenthesis ab \rrparenthesis \subseteq P$$

As P is prime ideal, $\llparenthesis a \rrparenthesis \subseteq P$ or $\llparenthesis b \rrparenthesis \subseteq P$. Hence $a \in P$ or $b \in P$.

By 2.4.13 (b) implies (a).
Since (b) and (c) are clearly equivalent, the lemma is proved. □

Lemma 2.4.15. *Let R be a non-zero commutative ring with identity and P an ideal in R. Then P is prime ideal if and only if R/P is an integral domain.*

Proof. If P is a prime ideal or if R/P is an integral domain we have that $R \neq P$. So the lemma follows from 2.4.13c. □

Lemma 2.4.16. *Let R be a ring and $\mathcal{M}$ be chain of ideal in R. (So $\mathcal{M}$ is a set of ideal and if $A, B \in \mathcal{M}$, then $A \subseteq B$ or $B \subseteq A$). Then $\bigcup \mathcal{M}$ is an ideal in R.*

Proof. Put $M = \bigcup \mathcal{M}$. Since $\mathcal{M} \neq \varnothing$, there exists $C \in \mathcal{M}$. Hence $0 \in C \subseteq M$. Let $a, b \in M$. Then there exist $A, B \in \mathcal{C}$ with $a \in A$ and $B \in \mathcal{C}$. Since $\mathcal{C}$ is chain, $A \subseteq B$ or $B \subseteq A$. Say $A \subseteq B$. Then both a and b are contained in B and so $a + b \in B \subseteq M$. Also if $r \in R$, then $-a, ra$ and ar all are in A and so in M. Thus M is an ideal in R. □

Remark 2.4.17. *A similar argument show that the union of a chain of subgroups is a subgroup and the union of a chain of subrings is a subring. See A.6.6 in the appendix for a common proof of these facts.*

Theorem 2.4.18. *Let R be a ring with identity and I an ideal in R with $I \neq R$. Then I is contained in a maximal ideal. In particular, every non-zero ring with identity has a maximal ideal.*

Proof. The second statement follows from the first applied to the zero ideal.

To prove the first statement we apply Zorn's lemma A.3.8. For this let $\mathcal{M}$ be the set of ideals J of R with $I \subseteq J \subsetneq R$. Order $\mathcal{M}$ by inclusion and let $\mathcal{C}$ be a nonempty chain in $\mathcal{M}$. So $\varnothing \neq \mathcal{C} \subseteq \mathcal{M}$ and if $A, B \in \mathcal{C}$, then $A \subseteq B$ or $B \subseteq A$. Let $M = \bigcup \mathcal{C}$. By 2.4.16 M is an ideal

Since $\mathcal{C} \neq \varnothing$ we can choose $C \in \mathcal{C}$. Since $I \subseteq C$, $I \subseteq M$. Since $\llbracket 1 \rrbracket = R$, $1 \notin C$ for all $C \in \mathcal{C}$ and so $1 \notin M$. Hence $M \neq R$ and $M \in \mathcal{M}$. Since $C \subseteq M$ for all $C \in \mathcal{M}$, M is an upper bound for $\mathcal{M}$. Thus by Zorn's Lemma $\mathcal{M}$ has a maximal element J. If $J \subseteq A$ for some ideal $A \neq R$, then $I \subseteq A$, $A \in \mathcal{M}$ and so by maximality of M in $\mathcal{M}$, $A = J$. Thus J is a maximal ideal of R containing I. □

Theorem 2.4.19. *Let M be a maximal ideal in the ring R. Then M is a prime ideal if and only $R^2 \nsubseteq M$. In particular if R is a ring with $\langle R^2 \rangle = R$ or a ring with identity then every maximal ideal is a prime ideal.*

Proof. We will show that $R^2 \subseteq M$ if and only if M is not a prime ideal.

Suppose $R^2 = RR \subseteq M$. Since R is an ideal in R and $R \nsubseteq M$, we conclude that M is not a prime ideal.

Suppose that M is not a prime ideal. Then $AB \subseteq M$ for some ideals A and B with $A \nsubseteq M$ and $B \nsubseteq M$. By 2.4.7(g), $A + M$ and $B + M$ are ideals in R. So the maximality of M implies $R = A + M = B + M$. Thus $R^2 = (A + M)(B + M) \subseteq AB + M \subseteq M$.

If R has an identity, then $\langle R^2 \rangle = R$ and if $\langle R^2 \rangle = R$, then $R^2 \nsubseteq M$. So the second statement follows from the first. □

Definition 2.4.20. *Let R be a ring.*

(a) A subring of S of R is called proper, if $S \neq 0$ and $S \neq R$.

(b) R is called simple *if $R^2 \neq 0$ and R has no proper ideals.*

Lemma 2.4.21. *(a) Let R be a division ring. Then R has no proper left or right ideals. In particular, R is simple.*

(b) Let R be commutative ring. Then R is simple if and only if R is a field.

Proof. (a) Let I be an non-zero left ideal in R and pick $0 \neq i \in I$. Then $1 = i^{-1}i \in Ri \subseteq R$ and so $R = R1 \subseteq I$. Similarly R has no proper right ideals. Since $0 \neq 1 = 1^2 \in R^2$, $R^2 \neq 0$ and so R is simple.

(b) Let R be simple commutative ring. Then $R^2 \neq 0$ and we can choose $a \in R$ with $Ra \neq 0$. Since R is commutative, Ra is an ideal in R and so $R = Ra$. Hence any $r \in R$ there exists $r_a \in R$ with $r = r_a a$. Then $ra_a = (r_a a)(a_a) = r_a(aa_a) = r_a a = r$ and so $1 = a_a$ is an identity in R. Note that 1_a is an inverse of a and so a is invertible. We proved that any element in $a \in R$ with $Ra \neq 0$ is a unit. Since $1b = b \neq 0$ for all $0 \neq b \in R$, this shows that all non-zero elements are units. Since $R \neq 0$, $1 \neq 0$ and so R is a field.

If R is a field, then by (a), R is simple. □

Lemma 2.4.22. *Let R be a ring and M an ideal in R. Then R/M is simple if and only if M is a maximal ideal with $R^2 \nsubseteq M$.*

Proof. In both cases $M \neq R$ and so we may assume $M \neq R$. We have $(R/M)^2 \neq 0_{R/M}$ if and only if $R^2 \nsubseteq M$. R/M has no proper ideals if and only if there does not exist an ideal J with $I \subsetneq J \subsetneq R$ and so if and only if M is a maximal ideal. □

If I is an ideal we will write $a \equiv b \pmod I$ if $a+I = b+I$, that is if $a-b \in I$. If $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ then $a \equiv b \pmod{n\mathbb{Z}}$ is the same as $a \equiv b \pmod n$.

Theorem 2.4.23 (Chinese Remainder Theorem)**.** *Let $(A_i, i \in I)$ be a family of ideals in the ring R.*

(a) The map θ :

$$R/\bigcap_{i\in I} A_i \to \prod_{i\in A_i} R/A_i$$

$$r + \bigcap_{i\in I} A_i \to (r + A_i)_{i\in I}$$

is a well defined monomorphism.

(b) Suppose that I is finite, $R = R^2 + A_i$ and $R = A_i + A_j$ for all $i \neq j \in I$. Then

(a) If $|I| > 1$, then $R = A_i + \bigcap_{i\neq j\in I} A_j$.

(b) θ is an isomorphism.

(c) For $i \in I$ let $b_i \in R$ be given. Then there exists $b \in R$ with

$$b \equiv b_i \pmod{A_i} \textit{ for all } i \in I$$

Moreover, b is unique $\pmod{\bigcap_{i\in I} A_i}$.

Proof. (a) The map $r \to (r+A_i)_{i\in I}$ is clearly a ring homomorphism with kernel $\bigcap_{i\in I} A_i$. So (a) holds.

(b:a) For $\varnothing \neq J \subseteq I$ put $A_J = \bigcap_{j\in J} A_j$. We will show by induction on $|J|$ that

$$R = A_i + A_J$$

for all $\varnothing \neq J \subseteq I \smallsetminus \{i\}$. Indeed if $|J| = 1$ this is part of the assumptions. So suppose $|J| > 1$, pick $j \in J$ and put $K = J \smallsetminus \{j\}$. Then by induction $R = A_i + A_K$ and $R = A_i + A_j$. Note that as A_j and A_K are ideals, $A_jA_K \subseteq A_j \cap A_K = A_J$ Thus

$$R^2 = (A_i + A_j)(A_i + A_K) \subseteq A_i + A_jA_K \subseteq A_i + A_J$$

Hence $R = A_i + R^2 = A_i + A_J$.

(b:b) By (a) we just need to show that θ is onto. For $|I| = 1$, this is obvious. So suppose $I| \geq 2$. Let

$$x = (x_i)_{i\in I} \in \prod_{i\in A_i} R/A_i.$$

We need to show that $x = \theta(b)$ for some $b \in R$. Let $x_i = b_i + A_i$ for some $b_i \in R$. By (ba), we may choose $b_i \in \bigcap_{j \in i \neq I} A_j$. So $b_i \in A_j$ for all $j \neq i$. Thus

$$\theta(b_i)_j = \begin{cases} x_i & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}$$

Put $b \sum_{i \in I} b_i$. Then $\theta(b)_j = x_j$ and so $\theta(b) = x$.

(b:c) This is clearly equivalent to (b:b) □

The special case $R = \mathbb{Z}$ is an elementary result from number theory which was know to Chinese mathematicians in the first century A.D. To state this result we first need to observe a couple of facts about ideals in $\mathbb{Z}$.

Let n, m be positive integers. $\gcd(n, m)$ denotes the greatest common divisor and $\operatorname{lcm}(n, m)$ the least common multiple of n and m. Then

$$n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{lcm}(n, m)\mathbb{Z}$$

and

$$n\mathbb{Z} + m\mathbb{Z} = \gcd(n, m)\mathbb{Z}$$

In particular n and m are relatively prime if and only if $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$. So part (b:c) of the Chinese Remainder Theorem translates into:

Corollary 2.4.24. *Let $m_1, \dots m_n$ be positive integers which are pairwise relatively prime. Let $b_1, \dots, b_n$ be integers. Then there exists an integer b with*

$$b \equiv b_i \pmod{m_i} \textit{ for all } 1 \leq i \leq n$$

Moreover, b is unique $\pmod{m_1 m_2 \dots m_n}$

2.5 Factorizations in commutative rings

Definition 2.5.1. *Let R be a commutative ring and $a, b \in R$.*

(a) We say that a divides *b and write $a \mid b$, if $\llbracket b \rrbracket \subseteq \llbracket a \rrbracket$.*

(b) We say that a and b are associate *and write $a \sim b$, if $\llbracket a \rrbracket = \llbracket b \rrbracket$*

(c) We say that a is proper if $0 \neq \llbracket a \rrbracket \neq R$.

(d) a is a generator (of R) if $\llbracket a \rrbracket = R$.

Lemma 2.5.2. *Let R be a commutative ring and $a, b \in R$.*

(a) $a \sim b \iff a \mid b$ and $b \mid a$.

(b) The relation $\mid$ on R is reflexive and transitive.

(c) The relation $\sim$ on R is an equivalence relation.

(d) $a \mid b$ if and only if $b \in \llparenthesis a \rrparenthesis$.

(e) If a is a generator of R, then b is a generator if and only if $a \sim b$,

(f) If R has an identity, then $a \mid b$ if and only if $b = ra$ for some $r \in R$.

Proof. Obvious. □

Lemma 2.5.3. *Let R be a commutative ring and $u \in R$. The following are equivalent*

(a) $u \mid r$ for all $r \in R$.

(b) u is a generator of R.

(c) $u \mid r$ for some generator r of R.

Proof. (a) $\Longleftrightarrow$ (b) : u is a generator if and only if $\llparenthesis u \rrparenthesis = R$ if and only if $r \in \llparenthesis u \rrparenthesis$ for all $r \in R$ and if only if $r \mid u$ for all $r \in R$.

(b) $\Longrightarrow$ (c): Just observe that $u \sim u$.

(c) $\Longrightarrow$ (b): If $u \mid r$ for some generator r, then $R = \llparenthesis r \rrparenthesis \subseteq \llparenthesis u \rrparenthesis$ and so $R = \llparenthesis u \rrparenthesis$. □

Lemma 2.5.4. *Let R be a commutative ring with identity. Let $u \in R$. Then the following statements are equivalent*

(a) u is a generator.

(b) $Ru = R$.

(c) u is unit.

(d) $ur \mid r$ for all $r \in R$.

(e) $ur \sim r$ for all $r \in R$.

(f) u is not contained in any maximal ideals of R.

Proof. (a) $\Longleftrightarrow$ (b) : Since R is a commutative ring with identity, $\llparenthesis u \rrparenthesis = Ru$. So u is a generator if and only $Ru = R$.

(b) $\Longrightarrow$ (c): Since $Ru = R$, $1 = ru$ for some $r \in R$. Since R is commutative, $ur = 1$ and so u is a unit.

(c) $\Longrightarrow$ (d): Since R is a unit, $su = 1$ for some $s \in R$. Hence $r = 1r = (su)r = s(ur)$ and so $ur \mid r$.

(d) $\Longrightarrow$ (e): Note that $r \mid ur$ and so $ur \mid r$ implies $ur \sim r$.

(e) $\Longrightarrow$ (f): Using $r = 1$ in (e) we get $u \sim 1$. Thus $\llparenthesis u \rrparenthesis = \llparenthesis 1 \rrparenthesis = R$ and so u is not contained in any maximal ideal of R.

(f) $\Longrightarrow$ (a): If $\llparenthesis u \rrparenthesis \neq R$, 2.4.18 shows that $\llparenthesis u \rrparenthesis$ is contained in a maximal ideal, contrary the assumption. So $\llparenthesis u \rrparenthesis = R$ and u is a generator. □

Lemma 2.5.5. *Let R be a commutative ring with identity and $a, b \in R^\sharp$. Suppose b is not a zero-divisor.*

(a) Let $b = ua$. Then $a \sim b$ if and only if u is a unit.

(b) Let $a, b \in R$. Then $a \sim b$ if and only if $b = ua$ for a unit u in R.

Proof. (a) The "if" part follows from 2.5.4(d).

So suppose that $b \sim a$. Then $a = vb$ for some $v \in R$. Thus $1b = b = ua = u(vb) = (uv)b$ and so $(1 - uv)b = 0$. Since b is not a zero-divisor, $uv = 1$. So u is a unit.

(b) Suppose $a \sim b$. Then $a \mid b$ and so $b = ua$ for some $u \in R$. Thus (a) shows $a \sim b$.

The converse follows directly from (a). □

Corollary 2.5.6. *Let R be an integral domain. The equivalence classes of $\sim$ are the orbits of* $\mathrm{U}(R)$ *on R with respect to action by left multiplication.*

Proof. Note first that by 1.2.3(e), $(\mathrm{U}(R), \cdot)$ is a group and since $(R, \cdot)$ is associative $\mathrm{U}(R)$ acts on R by left multiplication. The corollary now follows from 2.5.5(b). □

Definition 2.5.7. *Let R be a ring.*

(a) An ideal I is called a principal ideal *if its generated by one element, that is $I = \llparenthesis r \rrparenthesis$ for some $r \in R$.*

(b) R is called a principal ideal ring *if every ideal is a principal ideal.*

(c) R is principal ideal domain *(*PID*), if R is an integral domain and a principal ideal ring.*

(d) An ideal I in R s called finitely generated if $I = \llparenthesis F \rrparenthesis$ for some finite subset F of R.

Definition 2.5.8. *Let R be a commutative ring and c a proper element. c is called a* prime *if for all $a, b \in R$*

$$c \mid ab \quad \Longrightarrow \quad c \mid a \quad or \quad c \mid b.$$

Lemma 2.5.9. *Let p be proper element in the commutative ring R. Then following are equivalent:*

(a) p is a prime

(b) $\llparenthesis p \rrparenthesis$ is a prime ideal

(c) $R/\llparenthesis p \rrparenthesis$ has no zero-divisor.

Proof. Let $d \in R$. Then $p \mid d$ if and only if $\llparenthesis d \rrparenthesis \subseteq \llparenthesis p \rrparenthesis$ and so if and only if $d \in \llparenthesis p \rrparenthesis$. Thus for all $a, b \in R$

$$p \mid ab \quad \Longrightarrow \quad p \mid a \quad \text{or} \quad p \mid b$$

if and only if

$$ab \in \llparenthesis p \rrparenthesis \quad \Longrightarrow \quad a \in \llparenthesis p \rrparenthesis \quad \text{or} \quad b \in \llparenthesis p \rrparenthesis$$

Thus the lemma follows from 2.4.14 □

Definition 2.5.10. *Let R be a commutative ring and c a proper element in R.*

(a) c is called irreducible *if for all $a,b\in R$*

$$c\sim ab \qquad \Longrightarrow \qquad a \text{ is a generator} \quad \text{or} \quad b \text{ is a generator}$$

(b) c is called weakly irreducible *if for all $a,b\in R$*

$$c\sim ab \qquad \Longrightarrow \qquad a\sim c \quad \text{or} \quad b\sim c$$

(c) c is called divisor simple *if for all a in R*

$$a \mid c \qquad \Longrightarrow \qquad a\sim c \quad \text{or} \quad a \text{ is a generator}$$

Remark 2.5.11. *Let R be a commutative ring and $c\in R$. Then c is divisor simple if and only if $\llbracket c\rrbracket$ is a maximal element in the set of proper principal ideal of R.*

Proof. Both statement just say that if $a\in R$ then

$$\llbracket c\rrbracket \subseteq \llbracket a\rrbracket \qquad \Longrightarrow \qquad \llbracket c\rrbracket = \llbracket a\rrbracket \quad \text{or} \quad \llbracket a\rrbracket = R.$$

□

Remark 2.5.12. *Let R be a commutative ring and a,b associate elements in R. Then a is a prime (irreducible,weakly irreducible,divisor-simple, proper) if and only if b is.*

Proof. A glance at the definitions of these terms show that they only depended on $\llbracket a\rrbracket$. □

Example 2.5.13. For any proper $(a,b)\in\mathbb{Z}_2\times\mathbb{Z}$ determine whether a is a prime, irreducible, weakly irreducible and/or divisor simple.

(a,b)	irreducible	divisor-simple	weakly irreducible	prime
$(1,p)$	Yes	Yes	Yes	Yes
$(0,1)$	No	Yes	Yes	Yes
$(1,0)$	No	No	Yes	Yes
otherwise	No	No	No	No

here p is a prime integer.

Lemma 2.5.14. *Let c be a proper element in the commutative ring R*

(a) If c is divisor-simple, then c is irreducible or $c\sim c^2$.

(b) If c is divisor simple, then c is weakly irreducible or R has a generator and $\llbracket c\rrbracket = \langle R^2\rangle \neq R$.

(c) If c is a prime, then c is weakly irreducible.

Proof. (a) Suppose c is divisor simple and c is not irreducible. Then there exists $a, b \in R$ such that $c \sim ab$ and neither a nor b is a generator. Note that $a \mid c$ and $b \mid c$. Since c is divisor simple and neither a and b are generators, $a \sim c$ and $b \sim c$. Thus $\llbracket a \rrbracket = \llbracket c \rrbracket = \llbracket b \rrbracket$ and so

$$\llbracket c \rrbracket = \llbracket ab \rrbracket = \langle \llbracket a \rrbracket \llbracket b \rrbracket \rangle = \langle \llbracket c \rrbracket \llbracket c \rrbracket \rangle = \llbracket c^2 \rrbracket$$

So indeed $c \sim c^2$.

(b) Suppose c is divisor simple and c is not weakly irreducible. Then there exists $a, b \in R$ such that $c \sim ab$ and neither a nor b is associated to c. Note that $a \mid c$ and $b \mid c$. Since c is divisor simple and neither a and b are associated to c, a and b are generators. Thus $\llbracket a \rrbracket = R = \llbracket b \rrbracket$ and so

$$\llbracket c \rrbracket = \llbracket ab \rrbracket = \langle \llbracket a \rrbracket \llbracket b \rrbracket \rangle = \langle R^2 \rangle$$

Since c is proper, $\llbracket c \rrbracket \neq R$ and so (b) is proved

(c) Let $a, b \in R$ with $p \sim ab$. Since $p \mid p = ab$ and p is a prime, $p \mid a$ or $p \mid b$. Since $a \mid p$ and $b \mid p$, $p \sim a$ or $p \sim b$. So p is weakly irreducible. □

Lemma 2.5.15. *Let c be a proper element in the commutative ring R with identity.*

(a) c is irreducible if and only if c is divisor-simple and $c \nsim c^2$.

(b) If c is divisor simple, then c is weakly irreducible.

(c) If c is weakly irreducible and not a zero-divisor, then c is irreducible.

Proof. (a) Suppose c is irreducible Let $a \in R$ with $a \mid c$. Then $c = ab$ for some $a, b \in R$ Since c is irreducible a or b is a generator. If b is a generator, then by 2.5.4, $c = ab \sim a$. So $a \sim c$ or a is a generator. Thus c is divisor simple.

Suppose that $c \sim c^2$. Since c is irreducible, c is a generator, a contradiction since c is proper.

Thus $c \nsim c^2$ and the forward direction of (a) is proved. The backwards direction follows from 2.5.14(a).

(b) Since R has an identity, $R = R^2$ and so (b) follows from 2.5.14(a).

(c) Suppose c is weakly irreducible and not a zero-divisor. Let $a, b \in R$ with $c \sim ab$. Since c is weakly irreducible, $c \sim a$ or $c \sim b$. Say, $c \sim b$. Then $b = rc$ and $c = sab$ for some $r, s \in R$. So $1c = sab = sarc = (sra)c$. Since c is not a zero divisor, $sra = 1$ and so a is a unit and thus a generator. Hence c is irreducible.

□

Lemma 2.5.16. *Let R be commutative ring with identity and $c \in R$ a proper non-zero divisor.*

(a) c is irreducible if and only if c is divisor-simple, if and only if c is weakly irreducible and if and only if $\llbracket p \rrbracket$ is a maximal proper principal ideal.

(b) If c is a prime, c is irreducible.

Proof. (a) Since c is not a zero-divisor and not a unit 2.5.5 shows that $c \nsim c^2$. So (a) follows from 2.5.15 and 2.5.11

(b) By 2.5.14 the prime c is weakly irreducible and so by (b) c is irreducible. □

Lemma 2.5.17. *Let R be principal ideal domain. Then the following are equivalent*

(a) p is a prime

(b) p is irreducible.

(c) $(\!(p)\!)$ is a maximal ideal.

(d) $R/(\!(p)\!)$ is a field.

Proof. (a) $\Longrightarrow$ (b): This is 2.5.16(b)

(b) $\Longrightarrow$ (c): By 2.5.16(a) $(\!(p)\!)$ is a maximal proper principal ideal. Since every ideal in a PID is a principal ideal, $(\!(p)\!)$ is a maximal ideal. So (c) holds.

(c) $\Longrightarrow$ (d): This follows from 2.4.22.

(d) $\Longrightarrow$ (a): By 2.4.19, $(\!(p)\!)$ is a prime ideal. So by 2.5.9 p is a prime. □

Proposition 2.5.18. *Let R be an commutative ring with identity and $a \in R$. Suppose that*

$$a = p_1 \cdot \ldots \cdot p_m \quad \textit{and} \quad a = q_1 \cdot \ldots \cdot q_n$$

where $m, n \in \mathbb{Z}^+$, p_i is a non-zero-dividing prime for $1 \le i \le m$ and q_j is divisor-simple for $1 \le j \le n$. Then $n = m$ and there exists $\pi \in \mathrm{Sym}(m)$ with $p_i \sim q_{\pi(i)}$ for all $1 \le i \le m$.

Proof. Note that $p_m \mid a$. Since p_m is a prime, $p_m \mid q_j$ for some $1 \le j \le n$. Since q_j is divisor-simple e and p_m is not a unit, $q_j \sim p_m$ and so $uq_j = p_m$ for some unit $u \in R$. Without loss, $j = n$.

Suppose $n = 1$. If $m = 1$ we are done. So suppose for a contradiction that $m > 1$. Then

$$(p_1 \ldots p_{m-1})p_m = a = q_m \sim p_m.$$

Thus by 2.5.5(a), $p_1 \ldots p_{m-1}$ is a unit and so divides 1. Hence also p_1 divides 1 and so p_1 is a unit, a contradiction.

Suppose $n > 1$. Then $p_{m-1}p_m = p_{m-1}(uq_n) = (up_{m-1})q_n$. By 2.5.5(a) $up_{m-1} \sim p_{m-1}$. Also $q_n \sim p_m$ and so by 2.5.16, up_{m-1} and q_n are non-zero-dividing primes. So replacing p_m by q_n and p_{m-1} by up_{m-1} we may assume that $q_n = p_m$.

Put $b = p_1 \ldots p_{m-1}$ if $m > 1$ and $b = 1$ if $m = 1$. Then

$$(q_1 \ldots q_{n-1})p_m = (q_1 \ldots q_{n-1})q_n = a = (p_1 \ldots p_{m-1})p_m = bp_m.$$

Since p_m is not a zero-divisor this implies

$$q_1 \ldots q_{n-1} = b$$

Suppose that $m = 1$. Then $b = 1$ and so q_1 is a unit, a contradiction.

Thus $m > 1$ and

$$q_1 \ldots q_{n-1} = p_1 \ldots p_{m-1}$$

So by induction on n, $n-1 = m-1$ and there exists $\mu \in \mathrm{Sym}(m-1)$ with $p_i \sim q_{\mu(i)}$ for all $1 \le i \le m-1$. Defining $\pi \in \mathrm{Sym}(m)$ by $\pi(m) = m$ and $\pi(i) = \mu(i)$ for $1 \le i \le m-1$ we see that the lemma holds. □

Definition 2.5.19. *A* unique factorization domain *(*UFD*) is an integral domain in which every proper element is a product of primes.*

Lemma 2.5.20. *Let R be a UFD and $r \in R$. Then r is a prime if and only if r is irreducible.*

Proof. By 2.5.16 each prime in R is irreducible. Now let r be irreducible. Then by definition of a UFD, $r = p_1 \dots p_n$ where each p_i is a prime. Then by 2.5.18 $n = 1$ and so $r = p_1$ is a prime. □

Our next goals is to show that every PID is a UFD. For this we need a couple of preparatory lemmas.

Lemma 2.5.21. *Let $\mathcal{I}$ be chain of ideals in the ring R. If $\bigcup \mathcal{I}$ is finitely generated as an ideal, then $\bigcup \mathcal{I} \in \mathcal{I}$.*

Proof. Suppose that $\bigcup \mathcal{I} = \llbracket F \rrbracket$ for some finite $F \subseteq \bigcup \mathcal{I}$. For each $f \in F$ there exists $I_f \in \mathcal{I}$ with $f \in I_f$. Since $\mathcal{I}$ is totally ordered, the finite set $\{I_f \mid f \in F\}$ has a maximal element I. Then $I \in \mathcal{I}$, $F \subseteq I$ and so

$$\bigcup \mathcal{I} = \llbracket F \rrbracket \subseteq I \subseteq \bigcup \mathcal{I}.$$

Thus $\bigcup \mathcal{I} = I \in \mathcal{I}$. □

Lemma 2.5.22. *Let R be an integral domain and $\mathcal{I}$ a non-empty set of principal ideals. Then one of the following holds:*

1. *$\bigcap \mathcal{I} = 0$ and there exists a family $(I_k)_{k \in \mathbb{N}}$ in $\mathcal{I}$ such that*

$$I_0 \supsetneq I_1 \supsetneq \dots \supsetneq I_k \supsetneq I_{k+1} \supsetneq \dots$$

   with $\bigcap_{k \in \mathbb{N}} I_k = 0$.

2. *$\mathcal{I}$ has a minimal element.*

3. *There exists a family $(J_k)_{k \in \mathbb{N}}$ of principal ideal in R such that*

$$J_0 \subsetneq J_1 \subseteq \dots \subsetneq J_k \subsetneq J_{k+1} \subsetneq \dots$$

   and $\bigcup_{k \in \mathbb{N}} J_k$ is not finitely generated.

Proof. Assume that (2) does not hold. Then by A.4.10 (applied to the ordering on $\mathcal{I}$ by reverse inclusion) there exists a family $(I_k)_{k \in \mathbb{N}}$ in $\mathcal{I}$ such that

$$I_0 \supsetneq I_1 \supseteq \dots \supsetneq I_k \supsetneq I_{k+1} \supsetneq \dots$$

If $\bigcap_{k \in \mathbb{N}} I_k = 0$, also $\bigcap \mathcal{I} = 0$ and so (1) holds. So we may assume that there exists $0 \neq a \in \bigcap_{k \in \mathbb{N}} I_k$. Since each I_n is a principal ideal, $I_n = \llbracket a_n \rrbracket$ for some $a_n \in R$. Since $a \in I_n$, $a = r_n a_n$ for some $r_n \in R$. Since

$$\llbracket a_{n+1} \rrbracket = I_{n+1} \subsetneq I_n = \llbracket a_n \rrbracket),$$

$a_{n+1} = s_n a_n$ for some non-unit s_n in R. Thus

$$r_n a_n = a = r_{n+1}a_{n+1} = r_{n+1}s_n a_n = r_{n+1}s_n a_n$$

Since R is an integral domain,

$$r_n = r_{n+1}s_n$$

Since s_n is not a unit, this gives

$$\llbracket r_n \rrbracket \subsetneq \llbracket r_{n+1} \rrbracket$$

Put $J_n = \llbracket r_n \rrbracket$. Then $J_n \subsetneq J_{n+1}$ and 2.5.21 shows that $\bigcup_{n\in\mathbb{N}} J_n$ is not finitely generated. So (3) holds. □

Lemma 2.5.23. *Let R be a ring in which every ideal is finitely generated.*

(a) Any nonempty set of ideals in R has a maximal member.

(b) Suppose in addition that R is an integral domain. Then every non-empty set of principal ideals with nonzero intersection has a minimal member.

Proof. (a) Otherwise A.4.10 implies that there exists an infinite strictly ascending chain of ideals

$$J_0 \subsetneq J_1 \subseteq \ldots \subsetneq J_k \subsetneq J_{k+1} \subsetneq \ldots$$

in R. But then 2.5.21 shows that $\bigcup_{k=1}^{\infty} J_k$ is not finitely generated, a contradiction.

(b) Let $\mathcal{I}$ be a non-empty set principal ideal in R with $\bigcap \mathcal{I} \neq 0$. By 2.5.22, $\bigcap \mathcal{I} = 0$, $\mathcal{I}$ has a minimal element or 2.5.22 as an infinite ascending chain of ideals. By assumption the first possibility does not holds. By (a), the last possibility does not holds and so $\mathcal{I}$ has a minimal element. □

Lemma 2.5.24. *Every principal ideal domain is a unique factorization domain.*

Proof. Let S be the set of proper elements in R which can be written as a product of primes. Let a be proper in R. We will first show

1°. *a is divisible by a prime.*

By 2.5.23(a) there exists a maximal ideal I with with $\llbracket a \rrbracket \subset I$. Since R is a PID, $I = \llbracket s \rrbracket$ for some $s \in R$. Then by 2.5.17 s is a prime. Since $\llbracket a \rrbracket \subseteq \llbracket s \rrbracket$, $s \mid a$ and (1°) holds.

2°. *Put $\mathcal{S} = \{\llbracket s \rrbracket \mid s \in S, s \mid a\}$. Then $\mathcal{S} \neq \varnothing$ and $\llbracket a \rrbracket \subseteq \bigcap \mathcal{S} \neq 0$.*

By (1°) there exists a prime s with $s \mid a$. Then $s \in S$ and so (2°) holds.

By (2°) and 2.5.23b, $\mathcal{S}$ has a minimal member, say $\llbracket b \rrbracket$ with $b \in S$. Since $b \mid a$, $a = ub$ for some $u \in R$.

Suppose that u is not a unit. Then by (1°) applied to u, there exists a prime p dividing a. Then pb divides a and $pb \in S$. Thus $\llbracket pb \rrbracket \in \mathcal{S}$ and since p is not a unit $\llbracket pb \rrbracket \subsetneq \llbracket b \rrbracket$, a contradiction to the minimal choice of $\llbracket b \rrbracket$

Thus u is a unit and $a \sim b$. Since b is a product of primes and any associate of a prime is a prime, we conclude that a is a product of primes. □

2.6 Euclidean Rings

Definition 2.6.1. *Let R be a ring.*

(a) A pre-Euclidean *function on R is a function $d : R \to \Lambda$, where Λ is a well-ordered set* [2]*, such that for all $a, b \in R$ with $b \neq 0$*

(i) $d(0) < d(b)$ and

(ii) if $d(b) \leq d(a)$, then there exists $t \in \llparenthesis b \rrparenthesis$ with $d(a - t) < d(a)$

(b) R is called an Euclidean domain *if R is an integral domain and there exists an pre-Euclidean function on R.*

Example 2.6.2. 1. Let $d : \mathbb{Z} \to \mathbb{N}, m \to |m|$ be the absolute value function. Let $a, b \in \mathbb{Z}$ and $0 < |b| \leq |a|$. If a and b are both positive or both negative, then $|a - b| < |a|$. If one of a, b is positive and the other negative, then $|a + b| > |a|$. So d is a pre-Euclidean function. Thus $\mathbb{Z}$ is an Euclidean domain.

2. Let $\mathbb{F}$ be any field, $\Lambda = \{-\infty\} \cup \mathbb{N}$. Let $0 \neq f, g \in \mathbb{F}[x]$ of degree n and m respectively. Suppose that $n < m$. Let a and b be the leading coefficients of f and g, respectively. $ba^{-1}x^{m-n}f$ is a polynomial of degree m and leading coefficient b. Thus $g - ba^{-1}x^{m-n}f$ has degree less than g and so d is a pre-Euclidean function.

Note also that fg is a polynomial of degree x^{n+m} with leading coefficient ab. Thus $fg \neq 0$ and so $\mathbb{F}[x]$ is an integral domain. Hence $\mathbb{F}[x]$ is a Euclidean domain.

Lemma 2.6.3. *Let $d : R \to \Lambda$ be a pre-Euclidean function on a ring R. Let $a, b \in R$ with $b \neq 0$. Then there exist $s \in \llparenthesis b \rrparenthesis$ and $r \in R$ and*

$$a = s + r \text{ and } d(r) < d(b).$$

Proof. Since Λ is well-ordered we can choose $s \in \llparenthesis b \rrparenthesis$ with

$$(*) \qquad d(a - s) = \min\{d(a - t) \mid t \in \llparenthesis b \rrparenthesis\}$$

Put $r = a - s$ and suppose that $d(r) \geq d(b)$. Then $r \neq 0$ and by the definition of a pre-Euclidean function there exists $t \in \llparenthesis b \rrparenthesis$ such that $d(r - t) < d(r)$. But $r - t = (a - s) - t = a - (s + t)$. Since $s + t \in \llparenthesis b \rrparenthesis$ and we obtain a contradiction (*). Hence $d(r) < d(b)$ and the lemma is proved. □

Definition 2.6.4. *Let R be an ring, Λ a well-ordered set and $d : R \to \Lambda$ a function such that for all $a, b \in R$ with $b \neq 0$:*

(i) $d(0) < d(b)$.

(ii) If $0 \neq a \in \llparenthesis b \rrparenthesis$, then $d(b) \leq d(a)$.

[2] see A.3.9 in the appendix for the definition of a well ordered set

(iii) There exist $s \in \llparenthesis b \rrparenthesis$ *and* $r \in R$ *with*

$$a = s + r \text{ and } d(r) < d(b).$$

Then d is called a Euclidean function

Lemma 2.6.5. *Let R be a ring and d a pre-Euclidean function on R. Let* $b \in R$*. If* $b = 0$ *define* $d^*(b) = d(b)$*, otherwise put*

$$d^*(b) = \min\{d(s) \mid 0 \neq s \in \llparenthesis b \rrparenthesis\}.$$

Then d^* *is a Euclidean function.*

Proof. We need to verify the conditions (i)- (iii) in the definition of an Euclidean function.

Let $a \in R$. Since $a \in \llparenthesis a \rrparenthesis$:

$$(1) \qquad d^*(a) \leq d(a)$$

For any $x \in R$, choose $x^* \in \llparenthesis x \rrparenthesis$ with $x^* \neq 0$ and

$$(2) \qquad d^*(x) = d(x^*)$$

Note that $x^* = 0$ if and only if $x = 0$. Let $0 \neq b \in R$.

(i): By definition of a pre-Euclidean function $d(0) < d(b^*)$ and so $d^*(0) < d^*(b)$.

(ii): Let $0 \neq a \in \llparenthesis b \rrparenthesis$. Then $a^* \in \llparenthesis a \rrparenthesis \subseteq \llparenthesis b \rrparenthesis$ and so by definition of d^*,

$$d^*(a) = d(a^*) \geq d(b^*) = d^*(b).$$

(iii): By 2.6.3 there exists $s \in \llparenthesis b^* \rrparenthesis$ and $r \in R$ with

$$a = s + r \text{ and } d(r) < d(b^*).$$

Since $b^* \in \llparenthesis b \rrparenthesis$, $s \in \llparenthesis b^* \rrparenthesis \subseteq \llparenthesis b \rrparenthesis$.

$$d^*(r) \leq d(r) < d(b^*) = d^*(b)$$

and so d^* is indeed an Euclidean function. □

Theorem 2.6.6. *Let d be a pre-Euclidean function on the ring R and I a non-zero left ideal in R. Let* $0 \neq b \in I$ *with* $d(b)$ *minimal, then* $I = \llparenthesis b \rrparenthesis$*. In particular every Euclidean domain is a PID.*

Proof. Let $0 \neq b \in I$ with $d(b)$ minimal. Let $a \in I$. By 2.6.3 there exist $s \in \llparenthesis b \rrparenthesis$ and $r \in R$ such that $a = s + r$ and

$$d(r) < d(b)$$

Since $r = a - s$ and both a, s are in I we get $r \in I$. So the minimal choice of $d(b)$ implies $r = 0$. Thus $a = s \in \llparenthesis b \rrparenthesis$ and so $I = \llparenthesis b \rrparenthesis$. □

Definition 2.6.7. *Let R be a commutative ring, $r \in R$ and $A \subseteq R$.*

(a) We say that r is a common divisor *of A and write $r \mid A$ if $r \mid a$ for all $a \in A$.*

(b) We say that r is a greatest common divisor *and write $r \sim \gcd A$ if r is common divisor of A and $s \mid r$ for all common divisor s of A.*

(c) We say that A is relatively prime *if all commons divisors of A are units.*

We remark that in a general commutative ring a given set of elements might not have a greatest common divisor.

Lemma 2.6.8. *Let R be a commutative ring, $r \in R$ and $A \subseteq R$.*

(a) $r \mid A$ if and only if $\llparenthesis A \rrparenthesis \subseteq \llparenthesis r \rrparenthesis$.

(b) r is a gcd of A if and only if for all $s \in R$

$$s \mid A \quad \Longleftrightarrow \quad s \mid r.$$

Proof. (a) By definition of dividing, $r \mid a$ if and only if $\llparenthesis a \rrparenthesis \subseteq \llparenthesis r \rrparenthesis$. Since $\llparenthesis r \rrparenthesis$ is an ideal, $\llparenthesis a \rrparenthesis \subseteq \llparenthesis r \rrparenthesis$ for all $a \in A$ if and only if $\llparenthesis A \rrparenthesis \subseteq \llparenthesis r \rrparenthesis$. Thus (a) holds.

(b) Suppose r is a gcd. If $s \mid A$, then $s \mid r$ by definition of a gcd. If $s \mid r$, then since $r \mid A$ also $s \mid A$.

Suppose for all $s \in R$ we have $s \mid A \Longleftrightarrow s \mid r$. Since $r \mid r$ we get $r \mid A$. Also $s \mid r$ for all s with $s \mid A$ and so r is a gcd of A. □

Lemma 2.6.9. *Let R be a commutative ring and $A \subseteq R$*

(a) A has a common divisor in R if and only if A is contained in a principal ideal of R.

(b) Suppose that A has a common divisor in R and let I be the intersection of the principal ideal containing A. Then A has a greatest common divisor if and only if I is principal ideal. In the case the greatest common divisor are exactly the generators of I. In particular, greatest common divisors are unique up to associates.

Proof. Let $r \in R$.

(a) This holds since r is a common divisor of A if and only if $A \subseteq \llparenthesis r \rrparenthesis$.

(b) Let $\mathcal{K}$ be the set of principal ideal containing A. r is a greatest common divisors of A if and only if $A \subseteq \llparenthesis r \rrparenthesis$ and $\llparenthesis r \rrparenthesis \subseteq \llparenthesis s \rrparenthesis$ for all common divisor s of A. So r is a greatest common divisor if and only if $\llparenthesis r \rrparenthesis \in \mathcal{K}$ and $\llparenthesis r \rrparenthesis \subseteq K$ for all $K \in \mathcal{K}$. Thus if and only if $\langle r \rangle = I$. □

Lemma 2.6.10. *Let R be a commutative ring, $A \subseteq R$ and $r \in \llparenthesis A \rrparenthesis$. Then the following are equivalent.*

(a) r is a common divisor of A.

(b) $\llparenthesis A \rrparenthesis = \llparenthesis r \rrparenthesis$.

(c) r is a greatest common divisor of A.

Proof. (a) $\Longrightarrow$ (b): Suppose r is a common divisor of A. Then $\llparenthesis A\rrparenthesis \subseteq \llparenthesis r\rrparenthesis$. Since $r \in \llparenthesis A\rrparenthesis$ we have $\llparenthesis r\rrparenthesis \subseteq \llparenthesis A\rrparenthesis$ and $\llparenthesis r\rrparenthesis = \llparenthesis A\rrparenthesis$.

(b) $\Longrightarrow$ (c): If $\llparenthesis A\rrparenthesis = \llparenthesis r\rrparenthesis$, $\llparenthesis A\rrparenthesis$ is the intersection of the principal ideal containing $\llparenthesis A\rrparenthesis$ and (c) follows from 2.6.9

(c) $\Longrightarrow$ (a): is obvious. □

Lemma 2.6.11. *Let R be an integral domain Let $\mathcal{P}$ a set of representatives for the primes in R, that is $\mathcal{P}$ is a set of primes and each prime in R is associate to exactly one element in $\mathcal{P}$. Put $\mathbb{p} = (p)_{p\in\mathcal{P}}$. Recall that*

$$\mathbb{N}_{\mathcal{P}} = \bigoplus_{p\in\mathcal{P}} \mathbb{N} \quad \textit{and} \quad \mathbb{p}^n = \prod_{p\in\mathcal{P}} p^{n_p},$$

where $n = (n_p)_{p\in\mathcal{P}} \in \mathbb{N}_{\mathcal{P}}$. The function

$$\mathrm{U}(R) \times \mathbb{N}_I \to R^\sharp, \ (u,n) \to u\mathbb{p}^n$$

is 1-1 homomorphism from the semigroup $(\mathrm{U}(R),\cdot) \times (\mathbb{N}_I,+)$ to the semigroup $(R^\sharp,\cdot)$. The function is onto if and only if R is a UFD.

Proof. The function is clearly a homomorphism. If $u\mathbb{p}^n = v\mathbb{p}^m$, the uniqueness of prime factorization shows that $n = m$. So $\mathbb{p}^n = \mathbb{p}^m$ and since R is an integral domain, $u = v$. So the map is 1-1.

If the function is onto each proper element is associated to a product or primes and so is a product of primes.

Suppose R is a UFD and let $a \in \mathbb{R}^\sharp$. If a is a unit, $a = a\mathbb{p}^0$. Suppose a is not a unit. Since R is a UFD, $a = q_1 \dots q_m$ for some primes $q_1,\dots,q_m$. Choose $p_i \in \mathcal{P}$ with $p_i \sim q_i$. Then $q_i = u_i p_i$ for some unite u_i. Put $u = \prod_{i=1}^m u_i$ and for $p \in \mathcal{P}$ let $n_p = \{1 \le i \le m \mid p_i = p\}$ and $n = (n_p)_{p\in\mathcal{P}}$. Then $a = u\mathbb{p}^n$ and so the map is onto. □

Lemma 2.6.12. *Let R be a UFD and P a set of representatives for the primes in R, that is P is a set of primes and each prime in R is associate to exactly one element in P. Put $\mathbb{p} = (p)_{p\in P}$. Let $a,b \in R^\sharp$ and $B \subset R^\sharp$ with $B \neq \emptyset$. Let $\big(u(a),n(a)\big) \in U(R) \times \mathbb{N}_P$ be defined by*

$$a = u(a)\mathbb{p}^{n(a)}.$$

For $n,m \in \mathbb{N}_I$ define

$$n \le m \qquad \textit{if} \quad n_p \le m_p \quad \textit{for all } p \in P$$

Define

$$n(B) = \inf_{b\in B} n(b) \qquad \textit{that is} \qquad n_p(B) = \inf_{b\in B} n_p(b) \quad \textit{for all } p \in P.$$

(a) $a \mid b$ if and only if $n(a) \le n(b)$.

(b) $a \mid B$ if and only if $n(a) \le n(B)$.

(c) Let $p \in P$. Then

$$n_p(b) = \max\{k \in \mathbb{N} \mid p^k \mid b\} \quad \textit{and } n_p(B) = \max\{k \in \mathbb{N} \mid p^k \mid B\}$$

(d) $\mathbb{p}^{n(B)} \sim \gcd(B)$.

Proof. (a) a divides b if and only if $b = ad$ for some $d \in R$. Since $b \neq 0$, $d \neq 0$ and so $d = v\mathbb{p}^m$ for some $v \in \mathrm{U}(R)$ and $m \in \mathbb{N}_I$. Thus $a \mid b$ if and only if there exist $v \in \mathrm{U}(R)$ and $m \in \mathbb{N}_I$ with $u(b) = u(a)v$ and $n(b) = n(a) + m$. Since $u(b)$ and $u(a)$ are units, there exists a unique $v \in \mathrm{U}(R)$ with $u(b) = u(a)v$, namely $v = u(b)^{-1}u(a)$. There exists $m \in \mathbb{N}_I$ with $n(b) = n(a) + m$ if and only if $n(b) - n(a) \in \mathbb{N}_I$, that is $n(a) \leq n(b)$.

(b) $a \mid B$ if and only if $a \mid b$ for all $b \in B$. By (a) this holds if and only if $n(a) \leq n(b)$ for all $b \in B$ and so if and only if $n(a) \leq n(B)$.

(c) Let $q \in P$. Then $n_q(p^k) = 0$ for $q \neq p$ and $n_p(p^k) = k$. Thus by (a) and (b), $p^k \mid b$ if only if $k \leq n_p(b)$ and $p^k \mid B$ if and only if $k \leq n_p(B)$. Thus (c) holds.

(d) Note that $n\left(\mathbb{p}^{n(B)}\right) = n(B)$. Thus by (a) and (b) $a \mid \mathbb{p}^{n(B)}$ if and only if $n(a) \leq n(B)$ and if and only if $a \mid B$. So (d) follows from 2.6.8(b).

□

Here are a couple of concrete examples which might help to understand some of the concepts we developed above.

First let $R = \mathbb{Z}[i]$, the subring of $\mathbb{C}$ generated by i. R is called the ring of *Gauian integers*.

Note that $R = \mathbb{Z} + \mathbb{Z}i$. We will first show that R is an Euclidean ring. Indeed, put $\phi(a_1 + a_2 i) = a_1^2 + a_2^2$. Then $\phi(xy) = \phi(x)\phi(y)$ and $\phi(x) \in \mathbb{Z}^+$. So $(ER1)$ holds. Let $x, y \in R$ with $x \neq 0$. Put $z = \frac{y}{x} \in \mathbb{C}$. Then $y = zx$. Also there exists $d = d_1 + d_2 i \in \mathbb{C}$ with $q := z - d \in R$ and $|d_i| \leq \frac{1}{2}$. In particular, $\phi(d) \leq \frac{1}{2}^2 + \frac{1}{2}^2 = \frac{1}{2}$. Put $r = y - qx$ then $r = zx - qx = (z - q)x = dx$. So $\phi(r) = \phi(d)\phi(x) \leq \frac{1}{2}\phi(x)$. Hence also $(ER2)$ holds.

Let a be a prime in R and put $P = (a)$. Since $\phi(a) = \bar{a}a \in P$, $P \cap \mathbb{Z} \neq 0$. Also $1 \notin P$ and so $P \cap Z$ is a proper ideal in $\mathbb{Z}$. Since R/P has no zero divisors, $\mathbb{Z} + P/P \cong \mathbb{Z}/P \cap \mathbb{Z}$ has no zero divisors. Thus $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime integer p. Let $Q = pR$. Then $Q \leq P \leq R$. We will determine the zero divisors in R/Q. Indeed suppose that $ab \in Q$ but neither a nor b are in Q. Then p^2 divides $\phi(ab)$. So we may assume that p divides $\phi(a)$. Hence $a_1^2 = -a_2^2 \pmod{p}$. If p divides a_1 it also divides a_2, a contradiction to $a \notin Q$. Therefore we can divide by $a_2 \pmod{p}$ and conclude that the equation $x^2 = -1$ has a solution in $\mathbb{Z}/p\mathbb{Z}$. Conversely, if $n^2 \equiv -1 \pmod{p}$ for some integers n we see that (up to associates) $n + i + Q$ and $n - i + Q$ are the only zero divisors.

Suppose that no integer n with $n^2 \equiv -1 \pmod{p}$ exists. Then R/Q is an integral domain and so a field. Hence $Q = P$ and $a \sim p$ in this case.

Suppose that n is an integer with $n^2 \equiv -1 \pmod{p}$. As P is a prime ideal and $(n + i)(n - i) \in Q \leq P$, one of $n \pm i$ is in P. We conclude that $a \sim n \pm i$.

Next let $R = \mathbb{Z}[\sqrt{10}]$. We will show that R has some irreducible elements which are not primes. In particular, R is neither UFD, PID or Euclidean. Note that $R = \mathbb{Z} + \mathbb{Z}\sqrt{10}$. For $r \in R$ define $r_1, r_2 \in \mathbb{Z}$ by $r = r_1 + r_2\sqrt{10}$. Define $\tilde{r} = r_1 - r_2\sqrt{10}$ and $N(r) = r\tilde{r} = r_1^2 - 10r_2^2$. $N(r)$ is called the *norm* of r. We claim that $r \to \tilde{r}$ is a ring automorphism of R. Clearly it is an automorphism of $(R,+)$. Let $r, s \in R$. Then

$$rs = (r_1 + r_2\sqrt{10})(s_1 + s_2\sqrt{10}) = (r_1s_1 + 10r_2s_2) + (r_1s_2 + r_2s_2)\ \sqrt{10}$$

It follows that $\widetilde{rs} = \tilde{r}\tilde{s}$. In particular,

$$N(rs) = rs\widetilde{rs} = rs\tilde{r}\tilde{s} = r\tilde{r}s\tilde{s} = N(r)N(s)$$

and $N : R \to \mathbb{Z}$ is a multiplicative homomorphism. Let r be a unit in R. Since $N(1) = 1$, we conclude that $N(r)$ is unit in $\mathbb{Z}$ and so $N(r) = \pm 1$. Conversely, if $N(r) = \pm 1$, then $r^{-1} = \frac{\tilde{r}}{N(r)} = N(r)\tilde{r} \in R$ and r is a unit. For example $3 + \sqrt{10}$ is unit with inverse $-3 + \sqrt{10}$. As $\sqrt{10}$ is not rational, $N(r) \neq 0$ for $r \in R^{\#}$.

We claim that all of $2, 3$, $f := 4 + \sqrt{10}$ and $\tilde{f}$ are irreducible. Indeed suppose that ab is one of those numbers and neither a nor b are units. Then $N(a)N(b) \in \{4, 9, 6\}$ and so $N(a) \in \{\pm 2, \pm 3\}$ and

$$N(a) \equiv 2, 3 \pmod 5$$

But for any $x \in R$ we have

$$N(a) \equiv a_1^2 \equiv 0, 1, 4 \pmod 5$$

So indeed $2, 3, f$ and $\tilde{f}$ are primes. Note that $2 \cdot 3 = 6 = -f\tilde{f}$. Hence 2 divides $f\tilde{f}$ but (as f and $\tilde{f}$ are irreducible) 2 divides neither f nor $\tilde{f}$. So 2 is not a prime. With the same argument none of 3, f and $\tilde{f}$ are not primes.

We claim that every proper element in R is a product of irreducible. Indeed let a be proper in R and suppose that a is not irreducible. Then $a = bc$ with neither b nor c units. Then as $N(a) = N(b)N(c)$ both b and c have smaller norm as a. So by induction on the norm, both b and c can be factorized into irreducible.

Since R has irreducibles which are not primes, we know that R can not be a PID. But let us verify directly that $I = (2, f) = 2R + fR$ is not a principal ideal. First note that $f\tilde{f} = -6 \in 2R$. Since also $2f \in 2R$ we $I\tilde{f} \in 2R$. Since 4 does not divide $N(f)$, $f \notin 2R$ and so I does not contain a unit. Suppose now that h is a generator for I. Then h is not a unit and divides f. So as f is irreducible, $h \sim f$ and $I = (f)$. But every element in (f) has norm divisible by $N(f) = 6$, a contradiction to $2 \in I$ and $N(2) = 4$.

2.7 Localization

Let R be a commutative ring and $\emptyset \neq S \subseteq R$.In this section we will answer the following question:

Does there exists a commutative ring with identity R' so that R is a subring of R' and all elements in S are invertible in R ?

Clearly this is not possible if $0 \in S$ or S contains zero divisors. It turns out that this condition is also sufficient. Note that if all elements in S are invertible in R', also all elements in the subsemigroup of $(R, \cdot)$ generated by S are invertible in R'. So we may assume that S is closed under multiplication.

Lemma 2.7.1. *Let X be non-empty multiplicatively closed subset of the commutative ring R. For $r \in R$ and $x \in S$ denote the element $rx \in R[X]$ by ${}^{r}\!/_{x}$. Put*

$$I = \llbracket\, {}^{rz}\!/_{xz} - {}^{r}\!/_{x} \mid r \in R, x, z \in X \,\rrbracket$$

Let $r, s \in R$ and $x, y \in X$. Put

$$X^{-1}R = R[X]/I \qquad \textit{and} \qquad \frac{r}{x} = {}^{r}\!/_{x} + I.$$

(a) $\frac{r}{x}\frac{s}{y} = \frac{rs}{xy}$.

(b) $\frac{r}{x} + \frac{s}{y} = \frac{ry+sx}{xy}$.

(c) $X^{-1}R = \{\frac{r}{x} \mid r \in R, x \in X\}$.

(d) $\frac{x}{x}$ *is an identity in* $X^{-1}R$.

(e) $\frac{y}{x}$ *is an inverse of* $\frac{x}{y}$ *in* $X^{-1}R$.

(f) *The map* $\phi = \phi_X^R : R \to X^{-1}R$, $r \to \frac{rx}{x}$ *is a ring homomorphism and independent of* x.

(g) $\frac{r}{x} = \phi(x)^{-1}\phi(r)$.

(h) *Let S be a commutative ring with identity and $\beta : R \to S$ a ring homomorphism such that $\beta(x)$ is invertible for all $x \in X$. Then*

$$\beta_X : X^{-1}S \to S,\ \frac{a}{x} \to \beta(x)^{-1}\beta(a)$$

is a well defined function and is the unique homomorphism from $X^{-1}R$ to S with $\beta = \beta_X \circ \phi$.

(i) $\frac{r}{x} = \frac{s}{y}$ *if and only if there exists* $z \in X$ *with* $ryz = sxz$.

(j) $\ker\phi = \{r \in R \mid rx = 0$ *for some* $x \in X\}$. *In particular, if* $R \neq 0$, ϕ *is 1-1 if and only if no element of X is zero or a zero-divisor.*

Proof. Let $r, s \in R$ and $x, y, z \in X$. By definition of $R[X]$,

$${}^{r}\!/_{x}\,{}^{s}\!/_{y} = {}^{rs}\!/_{xy} \quad \text{and} \quad {}^{r}\!/_{x} + {}^{s}\!/_{x} = {}^{r+s}\!/_{x}$$

and so also

$$\frac{r}{x}\frac{s}{y} = \frac{rs}{xy} \quad \text{and} \quad \frac{r}{x} + \frac{s}{x} = \frac{r+s}{x}$$

In particular (a) holds. By definition of $\frac{r}{x}$ and I,

$$\frac{rz}{xz} = \frac{r}{x}.$$

Thus

$$\frac{r}{x}+\frac{s}{y}=\frac{ry}{xy}+\frac{sx}{yx}=\frac{ry}{xy}+\frac{sx}{xy}=\frac{ry+sx}{xy}$$

and (b) is proved.

(c) Put

$$W=\{{}^{r}\!/_{x}\mid r\in R, x\in X\}\quad\text{ and }\quad T=\{w+I\mid w\in W\}=\left\{\frac{r}{x}\;\middle|\; r\in R, x\in X\right\}.$$

Note that $R[X]=\langle W\rangle$ and so $X^{-1}R=\langle T\rangle$. By (c), T is closed under addition. It also closed under negatives and so $X^{-1}R=T$.

(d) $\frac{b}{y}\frac{x}{x}=\frac{bx}{yx}=\frac{b}{y}$.

(e) $\frac{x}{y}\frac{y}{x}=\frac{xy}{xy}$, which by (d) is an identity in $X^{-1}R$.

(f) $\frac{rx}{x}=\frac{rxy}{xy}=\frac{ry}{y}$ and so ϕ is independent of the choice of r. ϕ is the composition of the additive homomorphisms $r\to rx$, $s\to {}^{s}\!/_{x}$ and $a\to a+I$. Thus ϕ is an additive homomorphism.

$$\phi(r)\phi(s)=\frac{rx}{x}\frac{sx}{x}=\frac{rsxx}{xx}=\phi(rs)$$

and so ϕ is also a multiplicative homomorphism.

(g)

$$\frac{r}{x}=\frac{rxx}{xxx}=\frac{rx}{x}\frac{x}{x^2}=\phi(r)\phi(x)^{-1}$$

(h) Define $\gamma: X\to S, x\to\beta(x)^{-1}$. Then γ is multiplicative homomorphism and so 2.2.8 there exits a unique homomorphism $\delta: R[X]\to S$ with

$$\delta\left({}^{r}\!/_{x}\right)=\beta(r)\gamma(x)=\beta(r)\beta(x)^{-1}$$

Note that

$$\delta\left({}^{ry}\!/_{xy}\right)=\beta(ry)\beta(xy)^{-1}=\beta(r)\beta(y)\big(\beta(x)\beta(y)\big)^{-1}=\beta(r)\beta(y)\beta(y)^{-1}\beta(x)^{-1}=\beta(r)\beta(x)^{-1}=\delta\left({}^{r}\!/_{x}\right)$$

and so ${}^{ry}\!/_{xy}-{}^{r}\!/_{x}\in\ker\delta$. Since $\ker\delta$ is an ideal in R this gives $I\subseteq\ker\delta$. Defining $\alpha(a+I)=\delta(a)$ we see that α is well-defined homomorphism. Moreover

$$\alpha(\phi(r))=\alpha\left({}^{rx}\!/_{x}\right)=\beta(rx)\beta(x)^{-1}=\beta(r)\beta(x)\beta(x)^{-1}=\beta(r)$$

and so $\beta=\alpha\circ\phi$.

Conversely suppose that $\rho: X^{-1}R\to S$ is a homomorphism from $X^{-1}R$ with $\beta=\rho\circ\phi$. Define $\mu=\rho\circ\pi_I$. So $\mu(a)=\rho*a+I)$. Since $\phi(x)$ and $\rho(\phi(x))=\beta(x)$ are invertible, 1.6.7 shows that

$$\rho(\phi(x)^{-1})=(\rho(\phi(x))^{-1}=\beta(x)^{-1}$$

Thus

$$\mu\left({}^{r}\!/_{x}\right) = \rho\left(\pi_I\left({}^{r}\!/_{x}\right)\right) = \rho\left(\frac{r}{x}\right) = \rho\left(\phi(r)\phi(x)^{-1}\right) = \rho\big(\phi(r)\big)\rho\big(\phi(x)\big)^{-1} = \beta(r)\beta(x)^{-1}$$

So $\mu = \delta$. Hence $\rho(a + I) = \mu(a) = \delta(a) = \alpha(a + I)$ and thus $\rho = \alpha$.

(i) Suppose first that there exist $z \in X$ with $ryz = sxz$. Then

$$\frac{r}{x} = \frac{r(yz)}{x(yz)} = \frac{sxz}{xyz} = \frac{s(xz)}{y(xz)} = \frac{s}{y}$$

For the converse we will first determine exactly when an element of $R[X]$ is contained in I. Let J consists of all $a \in R[X]$ such that there exists $d \in X$ and $n = (n_x)_{x\in X} \in X^X$ with

(i) $xn_x = d$ for all $x \in X$ with $a_x \neq 0$, and

(ii) $\sum_{x\in X} a_x n_x = 0$.

Let $a, a' \in J$ and choose d, d' and n, n' according the definition of J.
Then

$$a + I = \left(\sum_{x\in X} {}^{a_x}\!/_{x}\right) + I = \sum_{a\in X} \frac{a_x}{x} = \sum_{x\in X} \frac{a_x n_x}{x n_s x} = \sum_{x\in X} \frac{a_x n_x}{d} = \frac{\sum_{x\in X} a_x n_x}{d} = \frac{0}{d} = I$$

and so $a \in I$. Thus $J \subseteq I$.

Define

$$m_x = \begin{cases} n_x d' & \text{if } a_x \neq 0 \\ n'_x d & \text{if } a_x = 0 \end{cases}$$

If $a_x \neq 0$ and $a'_x \neq 0$, then $n_x d' = n_x x n'_x = n'_x d$. In particular, the setup is symmetric in a and a'.

If $a_x \neq 0$, then $xm_x = xn_x d' = dd'$. By symmetry, $xm_x = dd'$ if $a'_x \neq 0$ and so $xm_x = dd'$, whenever $a_x + a'_x \neq 0$. We compute

$$\sum_{x\in X}(a_x + a'_x)m_x = \sum_{\substack{x\in X\\ a_x\neq 0}} a_x m_x + \sum_{\substack{x\in X\\ a'_x\neq 0}} a'_x m_x = \left(\sum_{x\in X} a_x n_x\right) d' + \left(\sum_{x\in X} a'_x n_x\right) d = 0d' + 0d = 0$$

and so $a + a' \in J$.

Put $V = \{{}^{rz}\!/_{xz} - {}^{r}\!/_{x} \mid r \in R, x, z \in X\}$. We will show that $V \subseteq J$.

If $x \neq xz$, choose $d = xxz$, $n_x = xz$ and $n_{xz} = x$. Then $xn_x = d = xzn_{xz}$ and

$$rzn_{xz} - rn_x = rzx - rxz = 0$$

and so ${}^{rz}\!/_{xz} - {}^{r}\!/_{x} \in J$.

If $x = xz$, then ${}^{rz}\!/_{xz} - {}^{r}\!/_{x} = {}^{rz}\!/_{x} - {}^{r}\!/_{x} = {}^{rz-r}\!/_{x}$. Put $n_x = x$ and $d = x^2 = n_x x$. Then

$$(rz - r)x = rzx - rx = rx - rx = 0$$

and so again ${}^{rz}\!/_{xz} - {}^{r}\!/_{x} \in J$. Thus $V \subseteq J$. Note that

$$ {}^{s}\!/_{y}\left({}^{rz}\!/_{xz} - {}^{r}\!/_{x}\right) = {}^{rsz}\!/_{xyz} - {}^{rs}\!/_{xy} $$

and so $WV \subseteq V \subseteq J$. Using that J is an additive subgroup of $R[X]$ we get

$$ I = \langle R[X]V, V\rangle = \langle\langle W\rangle V, V\rangle = \langle WV, V\rangle = \langle V\rangle \leq J $$

Since $J \subseteq I$, this proves $J = I$.

Now suppose that $\frac{r}{x} = \frac{s}{y}$. Then $\frac{r}{x} - \frac{s}{y} = 0$, $\frac{rx-sy}{xy} = 0$ and ${}^{rx-sy}\!/_{xy} \in I = J$. Thus there exists $n_{xy} \in X$ with $(rx - sy)n_{xy} = 0$ and so $rxn_{xy} = syn_{xy}$. Thus (i) holds.

(g) If $rx = 0$ for some $r \in X$, then $\phi(r) = \frac{rx}{x} = 0$. If $r \in \ker\phi$ then $\frac{r}{x}x = 0$ and so $rxy = 0$ for some $y \in X$. Since $xy \in X$, this gives shows

$$ \ker\phi = \{r \in R \mid rx = 0 \text{ for some } x \in X\} $$

ϕ is not 1-1 if and only if there exists $0 \neq r \in R$ with $r \in \ker\phi$ and so if and only if there exists $0 \neq r \in R$ and $x \in X$ with $rx = 0$. This holds if and only if $0 \in X$ or X contains a zero divisor.

□

Corollary 2.7.2. *Let G be a commutative semigroup and X a non-empty semisubgroup of G. Let R be a commutative ring with identity $1 \neq 0$. Identify $g \in G$ with $1g \in R[G]$.*

(a) Put

$$ X^{-1}G = \left\{ \frac{g}{x} \;\middle|\; g \in G, x \in X \right\} \subseteq X^{-1}(R[G]) $$

Then $X^{-1}G$ is multiplicatively closed subgroup of $X^{-1}(R[G])$ and so a semigroup. This semigroup is (up to isomorphism) independent of the ring R.

(b) There exists a homomorphism

$$ \alpha : R[X^{-1}G] \to X^{-1}(R[G]) \quad \textit{with} \quad \alpha\left(r\frac{g}{x}\right) = \frac{rg}{x} $$

for all $r \in R, g \in G$ and $x \in X$.

(c) There exists a homomorphism

$$ \beta : X^{-1}(R[G]) \to R[X^{-1}G] \quad \textit{with} \quad \beta\left(\frac{rg}{x}\right) = r\frac{g}{x} $$

for all $r \in R, g \in G$ and $x \in X$.

(d) α and β are inverse to each other and so are isomorphism.

Proof. (a) $\frac{g}{x}\frac{h}{y} = \frac{gh}{xy}$ for all $g,h \in G$, $x,y \in X$. So $X^{-1}G$ is multiplicatively closed and the multiplication on $X^{-1}G$ is completely determined by the multiplication of G and independent of R. . Since $\frac{g}{x} = \frac{h}{y}$ if and only if $gyz = hxz$ for some $z \in X$, also the set $X^{-1}G$ is independent of R.

(b) Fix $x \in X$ and define

$$\rho : R \to X^{-1}(R[G]), \quad r \to \frac{rx}{x}$$

Then

$$\rho(r+s) = \frac{(r+s)x}{x} = \frac{rx+sx}{x} = \frac{rx}{x} + \frac{sx}{x} = \rho(r) + \rho(s)$$

and

$$\rho(rs) = \frac{(rs)x}{x} = \frac{(rs)xx}{xx} = \frac{(rx)(sx)}{xx} = \frac{rx}{x}\frac{sx}{s} = \rho(r)\rho(s)$$

and ρ is ring homomorphism. $\mathrm{id}_{X^{-1}G}$ is a multiplicative homomorphism from $X^{-1}G$ to $X^{-1}(R[G])$ and so by 2.2.8 there exist a ring homomorphism

$$\alpha : R[X^{-1}G] \to X^{-1}(R[G]), \quad \text{with} \quad \alpha(ru) = \rho(r)u$$

for all $r \in R$, $u \in X^{-1}G$. Thus

Note that $\frac{rx}{x} = \frac{rxy}{xy} = \frac{ry}{y}$ for $y \in R$ and so ρ is independent of x. We have

$$\alpha\left(r\frac{g}{x}\right) = \rho(r)\frac{g}{x} = \frac{rx}{x}\frac{g}{x} = \frac{rgx}{xx} = \frac{rg}{x}$$

and so (b) holds.

(c) $\phi_|G$ is a homomorphism for G to $X^{-1}G$. id_R is a homomorphism from R to R and so by 2.2.11 thee exists a unique homomorphism

$$\gamma : R[G] \to R[X^{-1}G] \text{ with } \gamma(rg) = r\phi(g)$$

Since $\gamma(x) = \gamma(1x) = 1\phi(x) = \phi(x)$ is invertible in $R[X^{-1}G]$ we conclude that there exists a unique homomorphism

$$\beta : X^{-1}(R[G]) \to R[X^{-1}G]$$

with $\beta(\phi(a)) = \gamma(a)$ for all $a \in R[G]$. Moreover, $\beta\left(\frac{a}{x}\right) = \gamma(a)\gamma(x)^{-1}$. So

$$\beta(\left(\frac{rg}{x}\right) = \gamma(rg)\gamma(x)^{-1} = r\phi(g)\phi(x)^{-1} = r\frac{g}{x}$$

and (c) holds.

(d) Note that $(\alpha \circ \beta)\left(\frac{rg}{x}\right) = \frac{rg}{x}$ and since $X^{-1}(R[G])$ is generated by these elements $\alpha \circ \beta$ is the identity function in $X^{-1}(R[G]$. Similarly $\beta \circ \alpha$ is the identity function on $R[X^{-1}G]$. □

Definition 2.7.3. *Let G be a magma. We say that the left cancellation law holds for $g \in G$ if for all $a,b \in G$:*

$$ga = gb \Longrightarrow a = b$$

Note that if R is a ring and $0 \neq r \in R$ then the left cancellation holds for r if and only if r is not a left zero divisor.

Lemma 2.7.4. *Let G be semigroup and let S be the set of elements in G for which the left cancellation law holds. Then S is a subsemigroup of G.*

Proof. Let $s, t \in S$. Define $l_s : G \to G, g \to sg$. Then l_s and l_t are 1-1. Since G is associative $l_s \circ l_t = l_{st}$. Since compositions of 1-1 functions are 1-1, $st \in S$.

□

Definition 2.7.5. *Let R be a commutative ring.*

(a) *$\check{R}$ is the set of all non-zero, non zero divisors.*

(b) *Suppose that $\check{R} \neq \emptyset$. $\check{R}^{-1}R$ is called the* complete ring of fraction *of R*[3].

(c) *If R has no zero divisors, then $R\sharp^{-1}R$ is called the* field of fraction *of R and is denoted by $\mathbb{F}_R$.*

Example 2.7.6. *(a)* $\mathbb{F}_{\mathbb{Z}} = \mathbb{Q}$.

(b) *Let $0 \neq n \in \mathbb{Z}$. Then $\mathbb{F}_{n\mathbb{Z}} = \mathbb{Q}$.*

(c) *Let $\mathbb{F}$ be a field. Let I be a set and let (X_I, id_I) be a free abelian monoid. Then the field of fraction of $\mathbb{F}[X_I]$ is denoted by $\mathbb{F}(X_I)$. So*

$$\mathbb{F}(X_I) = \left\{ \frac{f}{g} \;\middle|\; f, g \in \mathbb{F}[X_I], g \neq 0 \right\}$$

If R is a commutative ring without zero divisors, then $\mathbb{F}_R(X_I)$ is the field of fractions of $R[X_I]$.

We will now spend a little but of time to investigate the situation where S does contain some zero divisors.

Define

$$\phi^* : S^{-1}R \to \phi(S)^{-1}\phi(R), \quad \frac{r}{s} \to \frac{\phi(r)}{\phi(s)}$$

We claim that ϕ^* is a well defined isomorphism. For this we prove the following lemma.

Lemma 2.7.7. *Let $\alpha : R \to R'$ be a homomorphism of commutative rings and S and S' multiplicative subsets of R and R' respectively. Suppose that $\alpha(S) \subseteq S'$.*

(a) *$\alpha(S)$ is a multiplicative subset of R'.*

(b)

$$\alpha^* : S^{-1}R \to S'^{-1}R', \quad \frac{r}{s} \to \frac{\alpha(r)}{\alpha(s)}$$

is a well defined homomorphism.

[3] Note that by 2.7.4 $\check{R}$ is a multiplicatively closed

(c) Suppose that $S' = \alpha(S)$. Then

$$\ker\alpha^* = \{\frac{r}{s} \mid r \in R, s \in S, Sr \cap \ker\alpha \neq \emptyset\} \textit{ and } \alpha^*(S^{-1}R) = \alpha(S)^{-1}\alpha(R)$$

Proof. (a) Just note that $\alpha(s)\alpha(t) = \alpha(st)$ for all $s, t \in S$.

(b) Note that $\phi_{S'}(\alpha(s))$ is invertible. Hence α^* is nothing else as the homomorphism given by **??** applied to the homomorphism:

$$\phi_{S'} \circ \alpha : R \to S'^{-1}R'$$

(c) Let $\frac{r}{s} \in \ker\alpha^*$. As seen above this means $t'\alpha(r) = 0$ for some $t' \in S'$. By assumption $t' = \alpha(t)$ for some $t \in T$. Thus $\frac{r}{s} = 0$ if and only if $tr \in \ker\alpha$ for some $t \in S$.

That $\alpha^*(S^{-1}R) = \alpha(S)^{-1}\alpha(R)$ is obvious. □

Back to the map ϕ^*. By the previous lemma ϕ^* is a well defined homomorphism and onto. Let $\frac{r}{s} \in \ker\phi^*$. Then $tr \in \ker\phi$ for some and $t \in S$. As $\ker\phi = R_S$, $\tilde{t}tr = 0$ for some $\tilde{t} \in S$. Hence $r \in R_S$ and $\frac{r}{s} = 0$. Therefore ϕ^* is one to one and so an isomorphism.

Note also that $\phi(R) \cong R/R_S$. Let $\bar{R} = R/R_S$ and $\bar{S} = S + R_S/R_S$. As ϕ^* is an isomorphism we get

$$S^{-1}R \cong \bar{S}^{-1}\bar{R}$$

We have $\bar{R}_{\bar{S}} = 0$. So in some sense we can always reduce to the case where S has no zero divisors.

Definition 2.7.8. *Let R be a commutative ring, X a multiplicatively closed subset of R and I be an ideal in R.*

(a) $A \subseteq R$ and $Y \subseteq X$. Then $\frac{A}{Y} = \{\frac{a}{y} \mid a \in A, y \in Y\} \subseteq X^{-1}R$.

(b)

$$\{r \in R \mid rx \in I \textit{ for some } x \in X\}$$

is called the X^{-1}-closure of I

(c) I is called X^{-1}-closed if $r \in I$ for all $r \in R$ with $rX \cap I \neq \emptyset$.

Note that $rx \in I$ for some $x \in X$ if and only if $rX \cap I \neq \emptyset$. So I is X^{-1} closed if and only if I is equal to the X^{-1}-closure of I.

Proposition 2.7.9. *Let X be a multiplicative subset of the commutative ring R and $\phi = \phi^R_X$. Let I be an ideal in R and J an ideal in $X^{-1}R$.*

(a) $\frac{I}{X}$ is an ideal in $X^{-1}R$

(b) Put $K = \phi^{-1}(J)$. Then K is an ideal in R with $J = \frac{K}{X}$. Moreover, for $r \in R$ and $x \in X$,

$$r \in K \iff \frac{r}{x} \in J$$

(c) $\phi^{-1}\left(\frac{I}{X}\right)$ *is the* X^{-1}*-closure of* I*.*

(d) $\phi^{-1}(J)$ *is* X^{-1}*-closed.*

(e) The X^{-1}*-closure of* X *is* X^{-1}*-closed.*

(f) The map

$$I \to \frac{I}{X}$$

is a bijection from the set of X^{-1}*-closed ideals in* I *to the set of ideals to* $X^{-1}R$*. The inverse is given by*

$$J \to \phi^{-1}(J)$$

(g) If $I \neq R$ *and* I *is* X^{-1}*-closed then* $I \cap X = \varnothing$*.*

(h) If I *is a prime ideal, then is* X^{-1}*-closed if an only if* $I \cap X = \varnothing$*.*

(i) $I \to \frac{I}{X}$ *is a bijection between the prime ideals* I *of* R *with* $I \cap X = \varnothing$ *and the prime ideals in* $X^{-1}R$*.*

Proof. (a) Let $i, j \in I$, $x, y \in X$ and $r \in R$. Then $0 = \frac{0}{x} \in \frac{I}{X}$. $\frac{i}{x} + \frac{j}{y} = \frac{iy+jx}{xy} \in \frac{I}{X}$ and $\frac{r}{x}\frac{i}{y} = \frac{ri}{xy} \in \frac{I}{X}$.

(b) Inverse images of ideals under homomorphism are ideal and so K is ideal.

Since $\phi(r)$ is associated to $\phi(r)\phi(x)^{-1}$ in $X^{-1}R$,

$$\phi(r) \in J \qquad \Longleftrightarrow \qquad \phi(r)\phi(x)^{-1} \in J$$

and so

$$r \in K \qquad \Longleftrightarrow \qquad \frac{r}{x} \in J$$

In particular, $J = \frac{K}{X}$ and (b) holds.

(c) Put $E = \phi^{-1}\left(\frac{I}{X}\right)$. Let $x \in X$. By (b) $r \in E$ if and only if $\frac{r}{x} \in \frac{I}{X}$ and so if and only if $\frac{r}{x} = \frac{i}{y}$ for some $i \in I$, $y \in X$. This holds if and only if $ryz = ixz$ for some $i \in I, y, z \in X$.

If $rxz = iyz$ for some $i \in I, y, z \in X$, then $xz \in X$ and $iyz \in I$. Hence $r(xz) \in I$ and so r is in the X^{-1}-closure of I.

Conversely, if $rx = i$ for some $x \in X$ and $i \in I$, then $rxxx = ixx$. Choose $y = xx$ and $z = x$ we see that $r \in E$.

(d) By (b) $\frac{K}{X} = \frac{I}{X}$ and so $\phi^{-1}\left(\frac{K}{X}\right) = K$. So by (c) K is equal to its X^{-1}-closure.

(e) Follows from (c) and (d)

(f) Follows from (a) to (e).

(g) Since $I \neq R$ and $I \to \frac{I}{X}$ is a bijection, $\frac{I}{X} \neq R^{-1}X$. Thus $\frac{I}{X}$ contains no units and so $I \cap X = \varnothing$.

(h) The forward direction follows from (g). So suppose $I \cap X = \varnothing$ and suppose $r \in R$ and $x \in X$ with $rx \in I$. Since $I \cap X = \varnothing$, $x \notin I$ and since I is a prime ideal we conclude that $r \in I$. Thus I is X^{-1}-closed.

(i) By (h) we can replace the conditions $I \cap X = \varnothing$ by I is X^{-1}-closed. Let I be an X^{-1}-closed ideal in R. Since $I \to \frac{I}{X}$ is a bijection, $I = R$ if and only if $\frac{I}{X} = X^{-1}R$. Let $r, s \in R$ and $x, y \in X$. Since I is X^{-1}-closed, we can apply (b) with $K = I$ and $J = \frac{I}{X}$. Thus

$$\begin{array}{ccc} r \in I & \Longleftrightarrow & \dfrac{r}{x} \in \dfrac{I}{X} \\ s \in I & \Longleftrightarrow & \dfrac{s}{y} \in \dfrac{I}{X} \\ sr \in I & \Longleftrightarrow & \dfrac{rs}{xy} \in \dfrac{I}{X} \end{array}$$

Hence

$$rs \in I \quad \Longrightarrow \quad r \in I \quad \text{or} \quad s \in I$$

if and only if

$$\frac{r}{x}\frac{s}{y} \in \frac{X}{I} \quad \Longrightarrow \quad \frac{r}{x} \in \frac{I}{X} \quad \text{or} \quad \frac{s}{y} \in \frac{I}{X}$$

Hence I is a prime ideal in R if and only if $\frac{I}{X}$ is a prime ideal in $X^{-1}R$.

□

Definition 2.7.10. *Let R be a commutative ring and P a prime ideal in R. The ring*

$$(R \setminus P)^{-1}R$$

is called is called the localization *of R at the prime P and is denoted by R_P. For $A \subseteq R$ we write A_P for $\frac{A}{P}$.*

Note here that by 2.4.13 $R \setminus P$ is a multiplicatively closed. So $(R \setminus P)^{-1}R$ is defined.

Recall that R_P also denotes $\bigoplus_{p \in P} R$. But hopefully it will always be clear from the context what is meant.

If S is a subring of R with $P \subsetneq S$, then P is also a prime ideal in S. Then $S_P = \frac{S}{P} \subseteq R_P$ should not be confused with $S_P = (S \setminus P)^{-1}S$.

Theorem 2.7.11. *Let P be a prime ideal in the commutative ring.*

(a) The map $Q \to Q_P$ is a bijection between the prime ideals of R contained in P and the prime ideals in R_P.

(b) P_P is the unique maximal ideal in R_P.

Proof. (a) Put $X = R \smallsetminus P$ and let Q a prime ideal in R. Then $Q \cap X = \varnothing$ if and only if $Q \subseteq P$. Thus (a) follows from 2.7.9(i).

(b) Let I be a maximal ideal in R_P. Since R_P has an identity, 2.4.19 I is prime ideal. Thus by (a) $I = Q_P$ for some $Q \subseteq P$. Since $I \subseteq P_P$ and I is maximal we get $I = P_P$. □

Definition 2.7.12. *A* local ring *is a commutative ring with identity and an ideal $M \neq R$ such that $I \subseteq M$ for all proper ideals I of M.*

Remark 2.7.13. *A commutative ring with identity is a local ring if and only if its has a unique maximal ideal M.*

Proof. Suppose R is a local ring. Then the ideal M is the definition of a local ring is the unique maximal ideal of R.

Suppose R has a unique maximal ideal M. Let I be a proper ideal in R. Then by 2.4.18 I is contained in a maximal ideal of R and so $I \subseteq M$. □

Lemma 2.7.14. *Let R be a commutative ring and M an ideal in R with $M \neq R$. Then the following statements are equivalent:*

(a) $I \subseteq M$ for all ideal I of R with $I \neq R$.

(b) M contains all proper elements.

(c) M is the set of non-generators.

Proof. (a) $\Longrightarrow$ (b): Let $r \in R$ be proper. Then $\llparenthesis r \rrparenthesis \neq R$ and so $\llparenthesis r \rrparenthesis \subseteq M$.

(b) $\Longrightarrow$ (c): The elements in $R \smallsetminus M$ are neither proper nor zero and so are generators. Since $M \neq R$, M does not contain any generators and so M is the set of non-units in R.

(c) $\Longrightarrow$ (a): Let I be an ideal in R with $I \neq R$. Let $i \in I$. Then $\llparenthesis i \rrparenthesis \subseteq I$ and so i is not a generator. Hence $i \in M$ and $I \subseteq M$. □

Example 2.7.15. *Let R be a UFD and p a prime in R. Determine the ideals in $R_{\llparenthesis p \rrparenthesis}$.*

Let $X = R \smallsetminus \llparenthesis p \rrparenthesis$. Then for $r \in R$, $r \in X$ if and only if $p \nmid r$. Thus
Then

$$R_{\llparenthesis p \rrparenthesis} = \left\{ \frac{r}{x} \in \mathbb{F}_R \;\middle|\; r, x \in \mathbb{R}, p \nmid x \right\}$$

Let I be a non-zero ideal in R. Put $n = n_p(I)$, so $n \in \mathbb{N}^+$ is maximal with $p^n \in I$. We claim that I is X^{-1}-closed if and only if $I = \llparenthesis p^n \rrparenthesis$.

Suppose first that I is X^{-1}-closed and choose $0 \neq i \in I$ with $n_p(i) = n$. Then $i = ap^n$ for some $a \in R$ with $p \nmid a$. Then $a \in X$ and $ap^n \in I$ and since I is X^{-1} closed, $p^n \in I$. So also $\llparenthesis p^n \rrparenthesis \subseteq I$. Since $p^n \mid I$, $I \subseteq \llparenthesis p^n \rrparenthesis$ and thus $I = \llparenthesis p^n \rrparenthesis$.

Suppose next that $I = \llparenthesis p^n \rrparenthesis$. So $r \in I$ if and only if $p^n \mid i$. Let $x \in X$ and $r \in R$ with $xr \in I$. Then $p^n \mid xr$ and since $p \nmid x$, $p^n \mid r$. Thus $r \in I$ and I is X^{-1}-closed.

So the non-zero ideal in $R_{\llparenthesis p \rrparenthesis}$ are $\llparenthesis p^n \rrparenthesis_{\llparenthesis p \rrparenthesis}$, $n \in n\mathbb{N}$. Note that this is just the ideal in $R_{\llparenthesis p \rrparenthesis}$ generate by $\frac{p^n}{1}$. Thus $R_{\llparenthesis p \rrparenthesis}$ is a PID with a unique prime $\frac{p}{1}$.

2.8 Polynomials rings, power series and free rings

Let R be a ring and G a semigroup. In the definition of the semigroup ring $R[G]$ we had to use the direct sum rather than the direct product since otherwise the definition of the products of two elements would involve infinite sums. But suppose G has the following property

$$\text{(FP)} \qquad |\{(a,b)\in G\times G \mid ab=g\}| \text{ is finite for all } g\in G$$

Then we can define the *power semigroup ring* of G over R, $R[[G]]$by

$$(R[[G]],+) = (\prod_{g\in G} R,+)$$

and

$$(r_g)_{g\in G}\cdot(s_g)_{g\in G} = (\sum_{(h,k)\in G\times G|hk=g} r_h s_k)_{g\in G}$$

If G is a group then it fulfills (FP) if and only if G is finite. So we do not get anything new. But there are lots of infinite semigroups with (FP). For example $G=\mathbb{N}$. $R[[\mathbb{N}]]$ is isomorphic to $R[[x]]$ the ring of formal power series. Other semigroups with (FP) are the free (abelian) monoids (or semigroups) over a set

Let I be a set. Then the power semigroup ring

$$R[[\bigoplus_{i\in I}\mathbb{N}]]$$

is called the ring of *formal power series* over R in the variables I and is denoted by $R[[I]]$. The elements of $R[[I]]$ are called formal power series. We use the same exponential notation as for the ring of polynomials. Every formal power series can be uniquely written as a formal sum

$$f=\sum_{\alpha\in\square} f_\alpha x^\alpha$$

Here $f_\alpha\in R$. But in contrast to the polynomials we do not require that almost all f_α are zero.

If $I=\{1\}$ the formal power series have the form:

$$f=\sum_{n=0}^{\infty} f_n x^n = f_0+f_1x+f_2x^2\ldots f_nx^n\ldots$$

with $f_n\in R$. Note that there does not exist an analog for **??** for formal power series, since the definition of $\Phi_y(f)$ involves an infinite sum.

Lemma 2.8.1. *Let R be ring with identity and $f\in R[[x]]$.*

(a) f is a unit if and only if f_0 is.

(b) If R is commutative and f_0 is irreducible, then f is irreducible.

Proof. (a) Note that $(fg)_0 = f_0 g_0$ and $1_0 = 1$ so if f is a unit so is f_0. Suppose now that f_0 is a unit. We define $g \in R[[x]]$ by defining its coefficients inductively as follows $g_0 = f_0^{-1}$ and for $n > 0$,

$$g_n = -f_0^{-1} \sum i = 0^{n-1} f_{n-i} g_i$$

. Note that this just says $\sum_{i=0}^{n} f_{n-i} g_i = 0$ for all $n > 0$. Hence $fg = 1$. Similarly f has a left inverse h by1.2.3 $g = h$ is a left inverses.

(b) Suppose that $f = gh$. Then $f_0 = g_0 h_0$. So as f_0 is irreducible, one of g_0, f_0 is a unit. Hence by (a) g or h is a unit. □

As an example we see that $1 - x$ is a unit in $R[[x]]$. Indeed

$$(1 - x)^{-1} = 1 + x + x^2 + x^3 + \dots .$$

Lemma 2.8.2. *Let $\mathbb{D}$ be a division ring.*

(a) $(x) = \{f \in \mathbb{D}[[x]] \mid f_0 = 0\}$

(b) The elements of (x) are exactly the non-units of $\mathbb{D}[[x]]$.

(c) Let I be a left ideal in $\mathbb{D}[[x]]$. Then $I = x^k\mathbb{D}[[x]] = (x^k)$ for some $k \in \mathbb{N}$.

(d) Every left ideal in $\mathbb{D}[[x]]$ is a right ideal and $\mathbb{D}[[x]]$ is a principal ideal ring.

(e) (x) is the unique maximal ideal in $\mathbb{D}[[x]]$.

(f) If $\mathbb{D}$ is a field, $\mathbb{D}[[x]]$ is a PID and a local ring.

Proof. (a) is obvious and (b) follows from 2.8.1.

(c) Let $k \in \mathbb{N}$ be minimal with $x^k \in I$. Let $f \in I$ and let n be minimal with $f_n \neq 0$. Then $f = x^n g$ for some $g \in \mathbb{D}[[x]]$ with $g_0 \neq 0$. Hence g is unit and $x^n = g^{-1} f \in I$. So $k \leq n$ and $f = (x^{n-k} g) x^k \in \mathbb{D}[[x]] x^k = (x^k)$. Thus $I = (x^k)$.

(d),(e) and (f) follow immediately form (c). □

2.9 Factorizations in polynomial rings

Definition 2.9.1. *Let R be a ring and I a set, (X_I, id_I) a free abelian monoid on I and $J \subseteq I$. Define*

$$\deg_J : R[I] \to \mathbb{N} \cup \{-\infty\}, \quad f \to \max_{\substack{n \in \mathbb{N}_I \\ f_n \neq 0}} \sum_{j \in J} n_j$$

with $\deg_J f = -\infty$ *if* $f = 0$. $\deg f = \deg_I(f)$.

If $I = J \uplus K$, then $X_I = X_J \times X_K$ and so $R[X_I]$ is canonical isomorphic to $R[X_K][X_J]$ and $\deg_J(f)$ is the degree of f viewed as polynomial in the variables J with coefficients in $R[X_K]$.

Lemma 2.9.2. *Let R be a ring, I a set and $f, g \in R[I]$.*

(a) $\deg(f+g) \le \max(\deg f, \deg g)$ *with equality unless* $h(g) = -h(f)$.

(b) If f *and* g *are homogeneous, then* fg *is homogeneous. Also either* $\deg(fg) = \deg(f) + \deg(g)$ *or* $fg = 0$.

(c) $h(fg) = h(f)h(g)$ *unless* $h(f)h(g) = 0$.

(d) $R[I]$ *has no zero divisors if and only if* R *has no zero divisors.*

(e) $\deg fg \le \deg f + \deg g$ *with equality if* R *has no zero divisors.*

Proof. (a),(b) and (c) are readily verified.

(d) If R has zero divisors, then as R is embedded in $R[I]$, $R[I]$ has zero divisors.

Suppose next that R has no zero divisors. Let $f, g \in R[I]^\#$. We need to show that $fg \neq 0$. By (c) we may assume that f and g are homogeneous.

Consider first the case that $|I| = 1$. Then $f = ax^n$, $g = bx^m$ and $fg = (ab)x^{n+m}$. Here $a, b \in R^\#$ and so $ab \neq 0$. Thus also $fg \neq 0$. If I is finite, $R[I] = R[I \setminus \{i\}][i]$ and so by induction $R[I]$ has no zero divisors.

For the general case just observe that $f, g \in R[J]$ for some finite subset J of I.

(e) If R has no zero divisors, (d) implies $h(f)h(g) \neq 0$. Thus by (b) and (c),

$$\deg f = \deg h(fg) = \deg h(f)h(g) = \deg h(f) + \deg h(g) = \deg f + \deg g.$$

□

Lemma 2.9.3. *Let* R *be a ring,* P *an ideal in* R *and* I *a set.*

(a) Let $P[I] = \{f \in R[I] \mid f_\alpha \in P$ *for all* $\alpha \in \mathbb{I}\}$. *Then* $P[I]$ *is an ideal in* $R[I]$ *and*

$$R[I]/P[I] \cong (R/P)[I]$$

(b) If R *has an identity,* $P[I] = P \cdot R[I]$ *is the ideal in* $R[I]$ *generated by* P.

Proof. (a) Define $\phi : R[I] \to (R/P)[I], \sum_{\alpha\in\mathbb{I}} f_\alpha x^\alpha \to \sum_{\alpha\in\mathbb{I}} (f_\alpha + P)x^\alpha$. By **??** ϕ is a ring homomorphism. Clearly ϕ is onto and $\ker\phi = P[I]$ so (a) holds.

(b) Let $p \in P$ then $px^\alpha \in P \cdot R[I]$. Thus $P[I] \le P \cdot R[I]$. The other inclusion is obvious. □

Corollary 2.9.4. *Let* R *be a commutative ring with identity,* I *a set and* $p \in R$. *Then* p *is a prime in* R *if and only if* p *is a prime in* $R[I]$.

Proof. R is a prime if and only if R/pR is an integral domain. So by 2.9.2d if and only if $(R/pR)[I]$ is an integral domain. So by 2.9.3 if and only if $R[I]/pR[I]$ is a prime ideal and so if and only if p is a prime in $R[I]$. □

Theorem 2.9.5 (Long Divison)**.** *Let* R *be a ring and* $f, g \in R[x]$. *Suppose that the leading coefficient of* g *is a unit in* R. *Then there exist uniquely determined* $q, r \in R$ *with*

$$f = qg + r \text{ and } \deg r < \deg g$$

Proof. Let $h(f) = ax^n$ and $h(g) = bx^m$. If $n < m$, we conclude that $q = 0$ and $r = f$ is the unique solution.

So suppose that $m \leq n$. Then any solution necessarily has $h(f) = h(q)h(g)$ and so $s(q) = ab^{-1}x^{n-m}$. Now $f = qg - r$ if and only if

$$f - ab^{-1}x^{n-m}g = (q - ab^{-1}x^{n-m})g + r$$

So uniqueness and existence follows by induction on $\deg f$. □

Let R be a ring and $f \in R[x]$. Define the function

$$f^r : R \to R, c \to \sum_{\alpha \in \mathbb{N}} f_\alpha c^\alpha$$

The function f^r is called the *right evaluation* of f. Note here that as R is not necessarily commutative , $f_\alpha c^\alpha$ might differ from $c^\alpha f^\alpha$. If R is commutative $f^r = f^{\mathrm{id}}$.

The map $f \to f^r$ is an additive homomorphism but not necessarily a multiplicative homomorphism. That is we might have $(fg)^r(c) \neq f^r(c)g^r(c)$. Indeed let $f = rx$ and $g = sx$. Then $fg = (rs)x^2$, $(fg)^r(c) = rsc^2$ and $f^r(c)g^r(c) = rcsc$.

Lemma 2.9.6. *Let R be a ring, $f, g \in R[x]$ and $c \in R$. If $g^r(c)c = cg^r(c)$ then*

$$(fg)^r(c) = f^r(c)g^r(c).$$

Proof. As $f \to f^r$ is a additive homomorphism we may assume that $f = rx^m$ for some $r \in R$, $m \in \mathbb{N}$. Thus

$$fg = \sum_{\alpha \in \mathbb{N}} rg_\alpha x^{\alpha+m}$$

and so

$$(fg)^r(c) = \sum_{\alpha \in \mathbb{N}} rg_\alpha c^{\alpha+m} =$$

$$= r(\sum_{\alpha \in \mathbb{N}} g_\alpha c^\alpha)c^m = rg^r(c)c^m = rc^m g^r(c) = f^r(c)g^r(c)$$

□

Corollary 2.9.7. *Let R be a ring with identity, $c \in R$ and $f \in R[x]$.*

(a) Then there exists a unique $q \in R[x]$ with

$$f = q(x - c) + f^r(c).$$

(b) $f^r(c) = 0$ if and only if $f = q(x - c)$ for some $q \in R[x]$.

Proof. (a) By2.9.5 $f = q \cdot (x - c) + r$ with $\deg r < \deg(x - c) = 1$. Thus $r \in R$. By 2.9.6

$$f^r(c) = q^r(c)(c - c) + r = r$$

Hence $r = f^r(c)$. The uniqueness follows from 2.9.5

(a) follows from (b). □

Corollary 2.9.8. *Let R be an commutative ring with identity and $c \in R$.*

(a) $R[x]/(x - c) \cong R$.

(b) $x - c$ is a prime if and only R is an integral domain.

Proof. Proof. Consider the ring homomorphism $\mathrm{id}_c : R[x] \to R, f \to f(c)$ (see **??** Clearly id_c is onto. By 2.9.7b $\ker \mathrm{id}_c = (x - c)$ so (b) follows from the Isomorphism Theorem for rings.

(b) Note that $x - c$ is a prime if and only if $R[x]/(x - c)$ has non-zero divisors. Thus (a) follows from (b). □

Corollary 2.9.9. *Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is an Euclidean domain. In particular, $\mathbb{F}[x]$ is a PID and a UFD. The units in $\mathbb{F}[x]$ are precisely the nonzero elements in $\mathbb{F}$.*

Proof. Just note that by 2.9.5 $\mathbb{K}[x]$ is a Euclidean domain. □

Let R be a subring of the commutative ring S. Write $R \to S$ for the inclusion map from R to S. Let I be a set, $f \in R[I]$ and $c \in S^I$. We say that c is a *root* of f if

$$f^{R \to S}(c) = 0.$$

Let R be any ring, $f \in R[x]$ and $c \in R$. We say that c is a root of f if $f^r(c) = 0$. Note that for R commutative this agrees with previous definition of a root for f in R.

Theorem 2.9.10. *Let D be an integral domain contained in the integral domain E. Let $0 \neq f \in D[x]$. Let $m \in \mathbb{N}$ be maximal so that there exists $c_1, \ldots c_m \in E$ with*

$$\prod_{i=1}^{m} x - c_i \quad | \quad f$$

in $E[x]$. Let c be any root of f in E. Then $c = c_i$ for some i. In particular, f has at most $\deg f$ *distinct roots in E.*

Proof. Let $f = g \prod_{i=1}^{m} x - c_i$ with $g \in E[x]$. By maximality of m, $x - c \nmid g$. By 2.9.8 $x - c$ is a prime in $E[x]$ and so

$$x - c \mid \prod_{i=1}^{m} x - c_i$$

By 2.5.18, $x - c \sim x - c_i$ for some i. Thus $x - c = x - c_i$ and $c = c_i$. □

We remark that the previus theorem can be false for non-commuative divison rings. For example the polynomial $x^2 + 1 = 0$ has at infinitely many roots in the division ring $\mathbb{H}$ of quaternions, namely any $ai + bj + ck$ with $a^2 + b^2 + c^2 = 1$.

Let R be a ring, $f \in R[x]$ and c b a root of f in D. Then by 2.9.10 We can write f has $f = g(x-c)^m$ with $m \in \mathbb{Z}^+$, $g \in R[x]$ and so that c is not a root of g. m is called the *multiplicity* of the root g. If $m \geq 2$ we say that c is a *multiple root*

As a tool to detect multiple roots we introduce the formal *derivative* f' of a polynomial $f \in R[x]$.

$$f' := \sum_{\alpha \in \mathbb{Z}^+} n f_\alpha x^{\alpha - 1}$$

Put $f^{[0]} = f$ and inductively, $f^{[k+1]} = (f^{[k]})'$ for all $k \in \mathbb{N}$.

Lemma 2.9.11. *Let R be a ring, $f, g \in R[x]$ and $c \in R$. Then*

(a) $(cf)' = cf'$

(b) $(f + g)' = f' + g'$.

(c) $(fg)' = f'g + fg'$.

(d) If $ff' = f'f$, $(f^n)' = nf^{n-1}f'$.

Proof. (a) and (b) are obvious.

(c) By (b) we may assume that $f = rx^m$ and $g = sx^n$ are monomials. We compute

$$(fg)' = (rsx^{n+m})' = (n+m)rsx^{n+m-1}$$
$$f'g + fg' = mrx^{m-1}sx^n + rx^m nsx^{n-1} = (n+m)rsx^{m+n-1}$$

Thus (c) holds.

(d) follows from (c) and induction on n. □

Lemma 2.9.12. *Let R be a ring with identity, $f \in R[x]$ and $c \in R$ a root of f.*

(a) Suppose that $f = g(x-c)^n$ for some $n \in \mathbb{N}$ and $g \in R[x]$. Then

$$f^{[n]}(c) = n!g(c).$$

(b) c is a multiple root of f if and only if $f'(c) = 0$.

(c) Suppose that $(\deg f)!$ is neither zero nor a zero divisor in R. Then the multiplicity of the root c is smallest number $m \in \mathbb{N}$ with $f^{[m]}(c) \neq 0$.

Proof. (a) We will show that for all $0 \leq i \leq n$, there exists $h_i \in R[x]$ with

$$f^{[i]} = \frac{n!}{(n-i)!} g(x-c)^{n-i} + h_i(x-c)^{n-i+1}$$

For $i = 0$ this is true with $h_0 = 0$. So suppose its true for i. Then using 2.9.11

$$f^{[i+1]} = (f^{[i]})' = \frac{n!}{(n-i)!}(g'(x-c)^{n-i} + g(n-i)(x-c)^{n-i-1}) + h_i'(x-c)^{n-i+1} + h_i(n-i+1)x^{n-i}$$

This is of the form $\frac{n!}{(n-i-1)!}g(x-c)^{n-i-1}$ plus a left multiple of $(x-c)^{n-i}$. So the statements holds for $i+1$.

For $i = n$ we conclude $f^{[n]} = n!g + h_n(x-a)$ Thus (a) holds.

(b) Since c is a root, $f = g(x-a)$ for some $g \in R[x]$. So by (a) applied to $n = 1$, $f'(c) = g(c)$. Thus (b) holds.

(c) Let m the multiplicity of c has a root of f. So $f = g(x-c)^m$ for some $g \in R[x]$ with $g(c) \neq 0$. Let $n < m$. Then $f = (g(x-c)^{m-n})(x-c)^n$ and (a) implies $f^{[n]}(c) = 0$. Suppose that $f^{[m]}(c) = 0$. Then by (a), $m!g(c) = 0$. As $m \leq \deg f$ we get $(\deg f)!\,g(c) = 0$. Thus by assumption $g(c) = 0$, a contradiction. This $f^{[m]}(c) \neq 0$ and (c) holds. □

Consider the polynomial x^p in $\mathbb{Z}/p\mathbb{Z}[x]$. Then $(x^p)' = px^{p-1} = 0$. This shows that the condition on $(\deg f)!$ in part (c) of the previous theorem is necessary.

Let D be an UFD, I a set and $f \in D[I]$. We say that f is *primitive* if 1 is a greatest common divisor of the coefficents of f.

Lemma 2.9.13. *Let D be a UFD, $\mathbb{F}$ its field of fractions and I a set. Let $f \in \mathbb{F}[I]$. Then there exists $a_f, b_f \in D$ and $f^* \in \mathbb{D}[I]$ so that*

(a) f^* is primitive in $D[I]$.

(b) a_f and b_f are relatively prime.

(c) $f = \frac{a_f}{b_f}f^*$.

Moreover a_f, b_f and f^* are unique up to associates in D.

Proof. We will first show the existence. Let $f = \sum_{\alpha\in\square} f_\alpha x^\alpha$ with $f_\alpha \in \mathbb{F}$. Then $f_\alpha = \frac{r_\alpha}{s_\alpha}$ with $r_\alpha, s_\alpha \in D$. Here we choose $s_\alpha = 1$ if $f_\alpha = 0$. Let $s = \prod_{\alpha\in\square} s_\alpha$. Then $sf \in D[I]$. Let $r = \gcd_{\alpha\in\square} sf_\alpha$ and $f^* = r^{-1}sf$. Then $f^* \in D[I]$, f^* is primitive and $f = \frac{r}{s}f^*$. Let e the a greates common divisor of r and s and put $a_f = \frac{r}{e}$ and $b_f = \frac{s}{e}$. Then (a),(b) and (c) hold.

To show uniqueness suppose that $f = \frac{a}{b}\tilde{f}$ with $a, b \in D$ relative prime and $\tilde{f} \in D[I]$ primitive. Then

$$ba_f^* = b_f a\tilde{f}$$

Taking the greatest common divisor of the coefficents on each side of this equation we see that ba_f and $b_f a$ are associate in D. In particular, a divides ba_f and as b is realtively prime to a, a divides a_f. By symmetry a_f divides a and so $a = ua_f$ for some unit u in D. Similarly $b = vb_f$ for some unit $v \in D$. Thus $vb_f a_f f^* = ub_f a_f \tilde{f}$. As D is an integral domain we conclude $\tilde{f} = u^{-1}vf^*$. □

Let f be as in the previuos theorem. The fraction $c_f = \frac{a_f}{b_f}$ is called the content of f. Note that $c_f \in \mathbb{F}$ and $f = c_f f^*$.

Lemma 2.9.14. *Let D be a UFD, $\mathbb{F}$ its field of fraction, I a set and $f, g \in \mathbb{F}[I]^\#$.*

(a) $c_{fg} = uc_f c_g$ for some unit $u \in D$.

(b) $(fg)^* = u^{-1} f^* g^*$

(c) The product of primitive polynomials is primitive.

(d) If $f \mid g$ in $\mathbb{F}[I]$, then $f^* \mid g^*$ in $D[I]$.

(e) Suppose f is primitive. Then f is irreducible in $D[I]$ if and only if its irreducible in $\mathbb{F}[I]$

(f) Suppose f is primitive.Then f is a prime in $D[I]$ if and only if it is a prime in $\mathbb{F}[I]$.

Proof. Note that $fg = c_f c_g f^* g^*$. So (a), (b) and (c) will follow once the show that the product of two primitive polynomials is primitive. Suppose not. Then there exist primitive $f, g \in D[I]$ and a prime p in D dividing all the coefficients of fg. But then $p \mid fg$ in $D[I]$. By 2.9.4 p is prime in $D[I]$ and so p divides f or g in $D[I]$. A contradiction as f and g are primitive.

(d) Suppose that $f \mid g$. Then $g = fh$ for some $h \in \mathbb{F}[I]$. By (b) $g^* = f^* h^*$ and so (d) holds.

(e) Suppose that f is irreducible in $\mathbb{F}[I]$ and $f = gh$ with $g, h \in D[x]$ Then by (a) both g and h are primitive. On the other hand since f is irreducible in $\mathbb{F}[I]$, one of g or h is a unit in $F[I]$ and so in $\mathbb{F}$. It follows that one of g and h is a unit in D. So f is also irreducible in $D[I]$.

Suppose that f is irreducible in $D[I]$ and $f = gh$ for some $g, h \in \mathbb{F}[x]$. Then $f = f^* \sim g^* h^*$ and as f is irreducible in $D[I]$, one of g^*, h^* is a unit in D. But then one of g and h is in $\mathbb{F}$ and so a unit in $\mathbb{F}[I]$.

(f) Suppose that f is prime in $D[I]$ and that $f \mid gh$ in $\mathbb{F}[I]$. By (d) $f = f^* \mid g^* h^*$ and as f is a prime in $D[I]$ we may assume $f \mid g^*$. As g^* divides g in $F[I]$ f does too. So f is a prime in $F[I]$.

Suppose that f is a prime in $F[I]$ and $f \mid gh$ in $D[I]$ for some $g, h \in D[I]$. Then as f is a prime in $F[I]$ we may assume that $f \mid g$ in $F[I]$. But (d) $f = f^* \mid g^*$ in $D[I]$. As g^* divides g in $D[I]$, f does too . So f is a prime in $D[I]$. □

Theorem 2.9.15. *Let D be a UFD and I a set, then $D[I]$ is a UFD.*

Proof. Let f be in $D[I]$. We need to show that f is the product of primes. Now $f \in D[J]$ for some finite f and by 2.9.4 a prime factorization in $D[J]$ is a prime factorization in $D[I]$. So we may assume that J is finite and then by induction that $|I| = 1$.

Note that $f = c_f f^*$ with $f^* \in D[x]$ primitive and $c_f \in D$. As D is a UFD, c_f is a product of primes in D and by2.9.4 also a prodcut of primes in $D[x]$. So we may assume that f is primitive. Suppose that $f = gh$ with $g, h \in D[x]$ with neither g nor h a unit. As f is primitive, g and h both have positive degree smaller than f. So by induction on $\deg f$ both g and h are a product of primes. So we may assume that f is irreducible. Let $\mathbb{F} = \mathbb{F}_D$. By 2.9.13 f is irreducible in $\mathbb{F}[x]$. As $\mathbb{F}[x]$ is Euclidean, f is a prime in $\mathbb{F}[x]$. Hence by 2.9.13 f is a prime in $D[x]$. □

Chapter 3

Modules

3.1 Modules and Homomorphism

In this section we introduce modules over a ring. It corresponds to the concept of group action in the theory of groups.

Definition 3.1.1. *Let $(R, +, \cdot)$ be a ring and $(M, +)$ an abelian group. A* ring action *of R on M is a function $*$ with $R \times M \subseteq \mathrm{Dom}(*)$ such that such that for all $r, s \in R$ and $a, b \in M$:*

(M0) $r * a \in M$.

(M1) $r * (a + b) = ra + rb$.

(M2) $(r + s) * a = ra + sa$.

(M3) $r * (s * a) = (r \cdot s)a$.

*In this case $(M, +, *)$ is called an R-*module.

Abusing notation we will call M an R-module and write ra for $r * a$.

Lemma 3.1.2. *Let R be a ring, M an abelian group, $* \in \mathrm{Fun}(R \times M)$ and $*_R : R \to \mathrm{Fun}(M)$ the associated function on R. Then $*$ is ring action of R on M if and only if $*_R$ is ring homomorphism from R to* $\mathrm{End}(M)$.

Proof. (M0) holds if and only if r^* is a function from M to M for all $r \in R$, that is if and only if $*_R$ is a function from R to $\mathrm{Fun}(M.M)$.

Assuming that (M0) holds:

(M1) holds if and only if r^* is a homomorphism for all $r \in R$, that is if and only if $*_R$ is a function from R to $\mathrm{End}(M)$.

Suppose now that (M0) and (M1) hold:

(M2) holds if and only if $(r + s)^* = r^* + s^*$ and (M3) holds if and only if $(rs)^* = r^* \circ s^*$ for all $r, s \in R$. So (M2) and (M3) holds if and only of $*_R$ is ring homomorphism from R to $\mathrm{End}(M)$.

□

Example 3.1.3. Let R be a ring and A an abelian group.

1. A is a $\mathbb{Z}$-module via $n * a = na$ for all $n \in \mathbb{Z}$ and $a \in A$.

2. A is an $\mathrm{End}(A)$-module via $\phi m = \phi(m)$ for all $\phi \in \Phi$, $m \in M$.

3. A is an R-module via, $ra = 0_R$ for all $r \in R$, $a \in A$.

4. R is an R-module via left multiplication.

5. Let $(M_i)_{i\in I}$ be a family of R-modules. Then $\bigtimes_{i\in I} M_i$ and $\bigoplus_{i\in I} M_i$ are R-modules via

$$r * (m_i)_{i\in I} = (r *_i m_i)_{i\in I}$$

Definition 3.1.4. *Let (R,G) be a sesquiring. An (R,G)-sesquimodule is triple $(M,+,*)$, where $(M,+)$ is an abelian group and $*$ is a function with $R \times G \times M \subseteq \mathrm{Dom}(*)$, such that the following holds for all $a, a' \in R$, $g, g' \in G$ and $m, m' \in M$:*

*(*SM 0) $a * g * m \in M$.

*(*SM 1) $a * g * (m + m') = a * g * m + a * g * m'$.

*(*SM 2) $a * g * (a' * g' * m) = (aa') * (gg') * m$.

*(*SM 3) $(a + a') * g * m = a * g * m + a' * g * m,$

Lemma 3.1.5. *Let (R,G) be a sesquiring and M an abelian group.*

(a) Let $* \in \mathrm{Fun}(R \times G \times M)$ and $*_{R\times G} : R \times G \to \mathrm{Fun}(M)$ the associated function on $R \times G$. Then $(M,*)$ is an (R,G)-sesquimodule if and only if $*_{R\times G}$ is a sesquihomomorphism from $R \times G$ to $\mathrm{End}(M)$.

(b) There exist natural 1-1 correspondences between the class of (R,G)-sesquimodules, the class of sesquihomomorphisms from (R,G) to endomorphism rings of abelian groups, the class of homomorphisms from $R[G]$ to endomorphism rings of abelian groups and the class $R[G]$-modules.

Proof. (a) Observe that (SM0) holds if and only if $*_{R\times G}$ is function from $R \times G$ to $\mathrm{Fun}(M,M)$.

Assume that (SM0) holds.

Note that (SM1) holds if and only if each $(a,g)^*$ is an homomorphism, that is if and only if $*_{R\times G}$ is a function from $R \times G$ to $\mathrm{End}(M,M)$.

Assume that (SM0) and (SM1) holds.

(SM2) holds if and only if $(aa', gg')^* = (a,g)^* \circ (a',g')^*$ and so if and only if $*_{R\times G}$ is a multiplicative homomorphism.

(SM3) holds if and only if $(a + a', g)^* = (a,g)^* + (a',g)^*$, that is $*_{R\times G}$ is an additive homomorphism in the first coordinate.

(b) (a) provides a 1-1 correspondence between the class of (R,G)-sesquimodules and the class of sesquihomomorphisms from (R,G) to endomorphismrings of abelian groups.

2.2.6 provides a 1-1 correspondence between class of sesquihomomorphisms from (R, G) to endomorphism rings of abelian groups and the class of homomorphisms from $R[G]$ to endomorphism rings of abelian groups.

3.1.2 provides a 1-1 correspondence between class of homomorphisms from $R[G]$ to endomorphism rings of abelian groups and the class $R[G]$-modules.

□

Example 3.1.6. *Let R be a ring, M an R-module and G a group acting on the set Ω. Define*

$$* : R \times G \times M^{\Omega} \to M^{\Omega}$$

by

$$(r * g * f)(\omega) = r \cdot f(g^{-1}\omega)$$

for all $r \in R, g \in G, f \in M^{\omega}$. Then $(M, *)$ is an (R, G) sesquimodule. So M is also an $R[G]$ module via

$$\Big(\big(\sum_{g \in G} r_g g\big) f\Big)(\omega) = \sum_{g \in G} r_g \cdot f(g^{-1}\omega)$$

Definition 3.1.7. *Let $\mathcal{C}$ be class, R a ring and I and J sets.*

(a) An $I \times J$-matrix is an $I \times J$-tuple. An $I \times J$-matrix in $\mathcal{C}$ is an $I \times J$-tuple in $\mathcal{C}$. $\mathrm{M}^{IJ}(\mathcal{C})$ is the class of all $I \times J$ matrix in $\mathcal{C}$.

(b) Let $i \in I$, $j \in J$ and A an $I \times J$-matrix. Then $A_{i,j} = A(i, j)$. $A_{i,}$ is the J-tuple $(A_{i,j})_{j \in J}$. $A_{i,}$ is called Row i of A. $A_{,j}$ is the I-tuple $(A_{i,j})_{j \in J}$. $A_{,j}$ is called Column j of A. We will also write A_{ij} for $A_{i,j}$ and A_i for $A_{i,}$.

(c) Let A be an $I \times J$-matrix. We will use any of the following to denote A:

$$[A_{ij}]_{i \in I, j \in J} \qquad [A_{ij}]_{\substack{i \in I \\ j \in J}} \qquad [A_{ij}]_{i,j} \qquad [A_{ij}] \qquad [A_{i,}]_{i \in I} \qquad [A_{,j}]_{,j \in J}$$

Definition 3.1.8. *Let R be a ring, I, J, K sets, A an $I \times J$-matrix in R, B an $J \times K$-matrix in R, $x, y \in R^J$ and $r \in R$.*

(a) We say that A has almost trivial rows A, if $A_i \in R_J$ for all $i \in I$. A has almost trivial columns if $A_{,j} \in R_I$ for all $j \in J$. $M^I{}_J(R)$ is the set of $I \times J$-matrices in R with almost trivial row. $M_I{}^J(R)$ is the set of $I \times J$-matrices in R with almost trivial columns, M_{IJ} is the set of $I \times J$-matrices in R with almost trivial rows and almost trivial columns.

(b) $rx := (rx_j)_{j \in J}$, $xr := (x_j r)_{j \in J}$, $rA = [rA_{ij}]_{\substack{i \in I \\ j \in J}}$ and $Ar = [A_{ij} r]_{\substack{i \in I \\ j \in J}}$.

(c) If $x \in R_J$ or $y \in R_J$, then $x \bullet y := \sum_{j \in J} x_j y_j$ and so $x \cdot y \in R$,

(d) If $A \in M^I{}_J(R)$ or $x \in R_J$, then $Ax := (A_i \bullet x)_{i \in I}$ and so $Ax \in R^I$.

(e) If $x \in R^J$ or $B \in M_J{}^K(R)$ then $xB := (x \bullet B_{,k})_{k\in K}$ and so $xB \in R^K$.

(f) If $A \in M^I{}_J(R)$ or $B \in M_J{}^K(R)$ then $AB := [A_i \bullet B_{,k}]_{\substack{i\in I\\ k\in K}}$ and so $AB \in \mathrm{M}^{IK}(R)$

Lemma 3.1.9. *Let R be a ring, I, J, K sets, A an $I \times J$-matrix in R, B an $J \times K$-matrix in R and $x \in R_J$.*

(a) $Ax = \sum_{j\in J} A_{,j}x_j$. In particular if $A \in \mathrm{M}_I{}^J(R)$, then $Ax \in R_I$.

(b) $xB = \sum_{j\in J} x_jB_j$. In particular, if $B \in \mathrm{M}^J{}_K(R)$ then $xB \in R_K$.

(c) Suppose that $A \in M^I{}_J(R)$ or $B \in M_J{}^K(R)$. Then $AB = [AB_{,k}]_{,k\in K}$ and $AB = [A_iB]_{i\in I}$.

(d) Suppose $A \in \mathrm{M}_I{}^J(R)$ and $B \in \mathrm{M}_J{}^K(R)$. Then $AB \in \mathrm{M}_I{}^K(R)$.

(e) Suppose $A \in \mathrm{M}^I{}_J(R)$ and $B \in \mathrm{M}^J{}_K(R)$. Then $AB \in \mathrm{M}^I{}_K(R)$

Proof. Readily verified. □

Remark 3.1.10. *If $A \in \mathrm{M}_{IJ}(R)$ and $B \in \mathrm{M}^J{}_K$, then AB does not have to be in $\mathrm{M}_I{}^K$. Consider for example the case $I = J$, R has an identity, $A = [\delta_{ij}]$ is the $I \times I$ identity matrix and $B \in \mathrm{M}^J{}_K(R) \setminus \mathrm{M}^{JK}(R)$. Then $AB = B \notin \mathrm{M}_I{}^K(R)$.*

Definition 3.1.11. *Let V and W be R-modules and $f : V \to W$ be a function. Then f is called R-linear if f is an $(R, \cdot)$-equivariant homomorphism, that is*

$$f(a + b) = f(a) + f(b) \text{ and } f(ra) = rf(a).$$

for all $a, b \in V$ and $r \in R$.

Definition 3.1.12. *Let R be a ring with identity and M an R-modules.*

(a) M is a unitary *R-module provide that*

$$1_Rm = m$$

for all $m \in M$.

(b) If R is a division ring and M is unitary then M is called a vector space over R.

Definition 3.1.13. *Let R be a ring and V and W R-modules.*

(a) $\mathrm{Hom}_R(V, W)$ denotes the set of R-linear maps from V to W.

(b) $\mathrm{End}_R(V) = \mathrm{Hom}_R(V, V)$.

Lemma 3.1.14. *Let R be a ring.*

(a) Let $f : U \to V$ and $g : V \to W$ be R-linear. Then $g \circ f$ is R-linear.

(b) Let $f : V \to W$ and $g : V \to W$ be R-linear. Then $f + g$ is R-linear.

(c) Let $f : V \to W$ be R-linear. Then $-f : V \to V, v \to -(f(v))$ is R-linear.

(d) $\mathrm{Hom}_R(V, W)$ a subgroup of $\mathrm{Hom}(V, W)$.

(e) Let V be an R-module. Then $\mathrm{End}_R(V)$ is a subring of $\mathrm{End}(V)$.

Proof. (a) Composition of homomorphism are homomorphism and composition of equivariant functions are equivariant.

(b) Sums of homomorphisms are homomorphism. Also

$$(f+g)(rv) = f(rv) + g(rv) = rf(v) + r(g(v) = r(f(v) + g(v)) = r(f+g)(v)$$

(c) Negatives of homomorphisms are homomorphism. Also

$$(-f)(rv) = -(f(rv)) = -(r(f(v))) = r(-(f(v))) = r((-f)(v))$$

(d) and (e) follow from (a), (b) and (c). □

Lemma 3.1.15. *Let R be a ring with identity and I and J sets.*

(a) For $A \in \mathrm{M}^I{}_J(R)$, define

$$\alpha_A : R_I \to R_K, x \to xA$$

Then

$$\Phi : \mathrm{M}^I{}_J(R) \to \mathrm{Hom}_R(R_I, R_J), A \to \alpha_A$$

is well-defined isomorphism of abelian groups.

(b) $\Phi : \mathrm{M}^I{}_I(R) \to \mathrm{End}_R(R_I), A \to \alpha_A$ is an anti-isomorphism of rings.

(c) For $A = [A_{ij}]_{\substack{i\in I\\ j\in J}} \in \mathrm{M}^{IJ}(R)$ define $A^{\mathrm{T}} \in \mathrm{M}^{JI}(R)$ by $\left(A^{\mathrm{T}}\right)_{ji} = A_{ij}$ for all $i \in I, j \in J$. Then

$$A^{\mathrm{T}} = [A_{ij}]_{\substack{j\in J\\ i\in I}} = [A_i]_{,i\in I} = [A_{,j}]_{j\in J} \qquad \text{and} \qquad \left(A^{\mathrm{T}}\right)^{\mathrm{T}} = A$$

Moreover,

$$\begin{aligned}
\mathrm{T}^{IJ} :&\quad \mathrm{M}^{IJ}(R) \to \mathrm{M}^{JI}(R), \quad A \to A^{\mathrm{T}}\\
\mathrm{T}^I{}_J :&\quad \mathrm{M}^I{}_J(R) \to \mathrm{M}_J{}^I(R), \quad A \to A^{\mathrm{T}}\\
\mathrm{T}_I{}^J :&\quad \mathrm{M}_I{}^J(R) \to \mathrm{M}^J{}_I(R), \quad A \to A^{\mathrm{T}}
\end{aligned}$$

are well-defined isomorphisms of abelian groups.

(d) Let K be a set, $A \in \mathrm{M}^{IJ}(R)$ and $B \in \mathrm{M}^{JK}(R)$. If $A \in \mathrm{M}^I{}_J$ or $B \in \mathrm{M}_J{}^K$, then

$$(AB)^{\mathrm{T}} = B^{\mathrm{T}} \cdot_{R^{\mathrm{op}}} A^{\mathrm{T}}$$

where $\cdot_{R^{\mathrm{op}}}$ denotes the multiplication of matrices with coefficients in R^{op}.

(e) $\mathrm{T}^I{}_J : \mathrm{M}^I{}_J(R) \to \mathrm{M}_J{}^I(R^{\mathrm{op}}),\ A \to A^{\mathrm{T}}$ *is an anti-isomorphism of rings.*

Proof. It is readily verified that α_A is R-linear and Φ is a homomorphism of abelian group. To show that Φ is a bijection we find an inverse. For $k \in I$ define $e_k = (\delta_{ik})_{i\in I} \in R_I$. Let $\alpha \in \mathrm{End}_R(R_I, R_J)$ and define

$$A_\alpha := [\alpha(e_i)]_{i\in I}$$

Since $\alpha(e_i) \in R_J$, $A_\alpha \in \mathrm{M}^I{}_J$. Also for $x \in R_I$

$$xA_\alpha = x[\alpha(e_i)]_{i\in I} = \sum_{i\in I} x_i\alpha(e_i) = \alpha\Big(\sum_{i\in I} x_i e_i\Big) = \alpha(x)$$

and so $\Phi(A_\alpha) = \alpha$.

Conversely if $A \in \mathrm{M}^I{}_J(R)$, then

$$[\alpha_A(e_i)]_{i\in I} = [e_i A]_{i\in I} = [\sum_{k\in K} \delta_{ik} A_k]_{i\in I} = [A_i]_{i\in I} = A$$

So the function

$$\Psi : \mathrm{Hom}(R_I, R_J) \to \mathrm{M}^I{}_J(R), \alpha \to A_\alpha$$

is inverse to Φ.

(b) Let $A, B \in \mathrm{M}^I{}_I(R)$ and $x \in R_I$. Then

$$(\alpha_A \circ \alpha_B)(x) = \alpha_A(\alpha_B(x)) = (xB)A = x(BA) = \alpha_{BA}(x)$$

(b) now follows from (a).

(c) Note that $(A^{\mathrm{T}})^{\mathrm{T}} = A$. So all of the functions are bijections. They are clearly additive homomorphism. Note that Column i of A^{T} is row i of A. So if A has almost trivial rows, A^{T} has almost trivial columns. Thus the functions are well-defined.

(d)

$$(AB)^{\mathrm{T}} = \Big([A_i \bullet B_{,k}]_{\substack{i\in I\\ k\in K}}\Big)^{\mathrm{T}} = [A_i \bullet B_{,k}]_{\substack{k\in K\\ i\in I}} = [B_{,k} \bullet_{R^{\mathrm{op}}} A_i]_{\substack{k\in K\\ i\in I}} = \Big[\big(B^{\mathrm{T}}\big)_k \bullet_{R^{\mathrm{op}}} \big(A^{\mathrm{T}}\big)_{,i}\Big]_{\substack{k\in K\\ i\in I}} = B^{\mathrm{T}} \cdot_{R^{\mathrm{op}}} A^{\mathrm{T}}$$

(e) Follows from (c) and (d)

□

Lemma 3.1.16. *Let R be a ring and V an R-module. Let G be a semigroup acting R-linearly on V, that is for all $r \in R, g, h \in G, a, b \in V$:*

$$(gh)v = g(hv), \quad g(v + w) = gv + gw, \quad \textit{and} \quad g(rv) = r(gm)$$

Then V is an $R \times G$-sesquimodule via

$$R \times G \times V \to V, (r, g, v) \to r(gv)$$

Proof. Let $*_R$ and $*_G$ be the homomorphism from R and G to $\mathrm{End}(V)$ obtained from the action of R and G on V. Note that $r(gv) = g(rv)$ means

$$*_R(r) \circ *_G(g) = *_G(g) \circ *_R(r)$$

So by 2.2.8 shows that map

$$R \times G \to \mathrm{End}(V), (r, g) \to *_R(r) \circ *_G(g)$$

is a sesquihomomorphism. So the lemma follows from 3.1.5 □

Definition 3.1.17. *Let R be a ring and $(V, +, *)$ an R-module. An R-submodule of $(V, +, *)$ is a R-module $(W, \triangle, \square)$ such that*

(i) $W \subseteq V$.

(ii) $a \triangle b = a + b$ *for all* $a, b \in W$.

(iii) $r \square a = r * a$ *for all* $r \in R$, $a \in W$.

Note that if $(W, \triangle, \square)$ is a submodule of V, then $(W, \triangle, \square) \equiv (W, +, *)$.

Lemma 3.1.18. *Let R be a ring, V an R-module and W an R-submodule of W. Then*

$$*_{V/W} : R \times V/W \to V/W, (r, v + W) \to rv + W$$

is a well-defined ring action of R on $(V/W, +_{V/W})$. Moreover the map

$$\pi : V \to V/W, v \to v + W$$

is an onto R-homomorphism with $\ker \pi = W$.

Proof. Let $v, v' \in V$ with $v + W = v' + W$. Then $v - v' \in W$ and so also

$$rv - rv' = r(v - v') \in W$$

Thus $rv + W = rv' + W$. So $*_{V/W}$ is well-defined. Straight forward calculations show that $*_{V/W}$ is a ring action.

By 1.6.10(f), π is a well-defined onto homomorphism of abelian groups with $\ker \pi = W$. We have

$$\pi(rv) = rv + W = r(v + W) = r\pi(v)$$

and so π is R-linear. □

Lemma 3.1.19. *Let R be a ring and $f : V \to W$ be R-linear,*

(a) Let X be an R-submodule of V. Then $f(X)$ is an R-submodule of W.

(b) Let Y be an R-submodule of W. Then $f^{-1}(Y)$ is an R-submodule of V.

(c) $\operatorname{Im} f$ *is R-submodule of W.*

(d) $\ker f$ *is an R-submodule of V.*

Proof. (a) Since f an homomorphism of abelian groups, $f(X)$ is a subgroup of W. Also if $r \in R$ and $x \in X$, then $rx \in X$ and so $rf(x) = f(rx) \in f(X)$

(b) $f^{-1}(Y)$ is an additive subgroup of V. If $x \in f^{-1}(Y)$, then $f(rx) = r(f(x)) \in rY \subseteq Y$. So $rx \in f^{-1}(Y)$.

(c) and (d) follow from (a) and (b) applies to $X = V$ and $Y = \{0\}$. □

Theorem 3.1.20 (Isomorphism Theorem for Modules)**.** *Let R be a ring and $f : V \to W$ an R-linear map. Then*

$$\overline{f} : V/\ker f \to f(W), v + \ker f \to f(v)$$

is a well-defined R-linear isomorphism.

Proof. By the isomorphism theorem for groups 1.6.11, this is a well defined isomorphism of abelian groups. We just need to check that it is R-linear. So let r and $v \in V$. Then

$$\overline{f}(r(v + \ker f)) = \overline{f}(rv + W) = f(rv) = rf(v) = r\overline{f}(v + \ker f).$$

□

Definition 3.1.21. *Let R be a ring, M an R-module, $S \subseteq R$ and $X \subset M$.*

(a) $\langle X \rangle$ is the subgroup of $(M, +)$ generated X.

(b) $SX = \{sx \mid s \in S, x \in X\}$

(c) $\operatorname{Ann}_S(X) = \{s \in S \mid sx = 0_M$ *for all* $x \in X\}$. $\operatorname{Ann}_S(X)$ *is called the* annihilator *of X in S*

(d) $\operatorname{Ann}_X(S) = \{x \in X \mid sx = 0_M$ *for alls* $\in S\}$. $\operatorname{Ann}_X(S)$ *is called the* annihilator *of X in S.*

(e) $\langle X \rangle_R := \bigcap\{W \mid W$ *is an R submodule of* $M, X \subseteq M\}$. $\langle X \rangle_R$ *is called R-submodule of M* generated *by X.*

(f) M is called finitely generated *if $M = \langle I \rangle_R$ for some finite subset I of R.*

Lemma 3.1.22. *Let R be a ring, M an R-module, $S, T \subseteq R$, $X, Y \subseteq M$, $r \in R$ and $m \in M$.*

(a) $S(TX) = (ST)X)$ and we will just write STX for $S(TX)$.

(b) $r\langle X \rangle = \langle rX \rangle$ and $\langle S \rangle x = \langle Sx \rangle$.

(c) $\langle SX \rangle = \big\langle S \langle X \rangle \big\rangle = \big\langle \langle S \rangle \langle X \rangle \big\rangle = \big\langle \langle S \rangle X \big\rangle$.

(d) If S is a left ideal in R, then $\langle SX \rangle$ is a R-submodule.

(e) Let $(X_i)_{i\in I}$ be a family of R-submodules of M. Then $\langle X_i, i \in I\rangle$ is an R-submodule of M.

(f) Let $(X_i)_{i\in I}$ be a family of R-submodules of M. Then $\bigcap_{i\in I} X_i$ is a R-submodule of M.

(g) $\langle X\rangle_R$ is R-submodule of M, $\langle X\rangle_R = \langle RX, X\rangle$ and if M is unitary, $\langle X\rangle_R = \langle RX\rangle$.

(h) If S is an additive subgroup of R and $X = \langle x_i \mid i \in I\rangle$ for family $(x_i)_{i\in I}$ in X then

$$\langle SX\rangle = \Big\{ \sum_{i\in I} s_i x_i \Bigm| s \in S_I \Big\}$$

(i) If $(X_i)_{i\in I}$ is a family of subsets of M, then $\langle X_i, i \in I\rangle_R = \langle \bigcup_{i\in I} X_i\rangle_R$.

Proof. (a)

$$S(TX) = \{s(tx) \mid s \in S, t \in T, x \in X\} = \{(st)x \mid s \in S, t \in T, x \in X\} = (ST)X.$$

(b) Since left multiplication by r and right multiplication by x are additive homomorphism, (b) follows from 1.8.5(c).

(c) Let $s \in S$ and $x \in X$ By (b) $s\langle X\rangle = \langle sX\rangle \le \langle SX\rangle$ and so

$$(*) \qquad \big\langle S\langle X\rangle\big\rangle = \langle SX\rangle$$

By (b) $\langle S\rangle x = \langle Sx\rangle \le \langle SX\rangle$ and so $\big\langle\langle S\rangle X\big\rangle = \langle SX\rangle$.

(*) applied to $\langle S\rangle$ in place of S yields $\big\langle\langle S\rangle\langle X\rangle\big\rangle = \langle\langle S\rangle X\rangle$ and so (c) holds.

(d) Since S is a left ideal, $RS \subseteq S$. So

$$R\langle SX\rangle \subseteq \langle R(SX)\rangle = \langle (RS)X\rangle \subseteq \langle SX\rangle$$

and so $\langle SX\rangle$ is an R-submodule.

(e) $R\langle X_i, i \in I\rangle \subseteq \langle RX_i, i \in I\rangle \subseteq \langle X_i, i \in I\rangle$.

(f) Suppose each X_i is an R-submodule. By 1.8.3 $\bigcap_{i\in I} X_i$ is subgroup of $(R, +)$. Let $x \in \bigcap_{i\in I} X_i$. Then $x \in X_i$ and so $rx \in A_i$ for all $i \in I$. Thus $rx \in \bigcap_{i\in I} X_i$ and so $\bigcap_{i\in I} X_i$ is an R-submodule.

(g) By (f), $\langle X\rangle_R$ is an R-submodule. Clearly $\langle RX, X\rangle$ is contained in any R-submodule containing X. So $\langle RX, X\rangle \le \langle X\rangle_R$. We have

$$R\langle RX, X\rangle \subseteq \langle R(RX), RX >\subseteq \langle RX\rangle \subseteq \langle RX, X\rangle$$

and so $\langle RX, X\rangle$ is an R-submodule containing X. Hence $\langle RX, X\rangle = \langle X\rangle_R$.

If M is unitary $X = 1X \subseteq RX$ and so $\langle RX, X\rangle = \langle RX\rangle$

(h) Note that

$$\langle SX\rangle = \big\langle S\langle x_i \mid i \in I\rangle\big\rangle = \langle Sx_i \mid i \in I\rangle.$$

and by (b), Sx_i is a subgroup of M. Hence (h) holds. □

Lemma 3.1.23. *Let R be a ring and A an additive subgroup of R. Put*

$$\mathrm{I}_R(A) = \langle J \subseteq A \mid J \text{ is an ideal in } R\rangle$$

Then $\mathrm{I}_R(A)$ is an ideal of R contained in A, called the largest ideal of R contained in A.

Proof. By 2.4.7(g) $\mathrm{I}_R(A)$ is an ideal in R. Since A is an additive subgroup of R, $\mathrm{I}_R(A) \subseteq A$. □

Lemma 3.1.24. *Let R be ring, M an R-module, $S \subseteq R$ and $X \subseteq M$. Then*

(a) $S \subseteq \mathrm{Ann}_R(X)$ if and only if $X \subseteq \mathrm{Ann}_M(X)$.

(b) Let $m \in M$. Then the map

$$R \to M, r \to rm$$

is R-linear and the map

$$R/\mathrm{Ann}_R(m) \to Rm,\ r + \mathrm{Ann}_R(m) \to rm$$

is a well-defined isomorphism of R-modules.

(c) $\mathrm{Ann}_R(X)$ is a left ideal in R.

(d) Let I be a right ideal in R. Then $\mathrm{Ann}_M(I)$ is R-submodule in M.

(e) If X is a R-submodule of M, then $\mathrm{Ann}_R(X)$ is an ideal in R

(f) $\mathrm{Ann}_R(\langle X\rangle_R) = \mathrm{I}_R(\mathrm{Ann}_R(X))$.

(g) Suppose that one of the following holds:

1. *R is commutative.*
2. *All left ideals in R are also right ideals.*
3. *$\mathrm{Ann}_R(X)$ is a right ideal.*

Then $\mathrm{Ann}_R(X) = \mathrm{Ann}_R(\langle X\rangle_R)$.

Proof. (a) Both statements are equivalent to $SX = \{0\}$.

(b) and (c) Consider the map

$$f : R \to M, \quad r \to rm.$$

Let $r, s \in R$. Then $f(r+s) = (r+s)m = rm + sm = f(r) + f(s)$. Also for $r, s \in R$

$$f(rs) = (rs)m = r(sm) = rf(s)$$

So f is R-linear. Since $\mathrm{Ann}_R(m) = \ker f$, (d) follows from the Isomorphism Theorem 3.1.20.

In particular, $\mathrm{Ann}_R(m)$ is a left R-submodule of R and so a left in R. Hence also $\mathrm{Ann}_R(X) = \bigcap_{x\in X} \mathrm{Ann}_R(x)$ is a left ideal in R and (c) holds.

(d) Since left multiplication by $r \in R$ is additive homomorphism, $\mathrm{Ann}_M(r)$ is an additive subgroup of R. Hence also $\mathrm{Ann}_M(I) = \bigcup_{i\in I} \mathrm{Ann}_M(i)$ is an additive subgroup. Since

$$I\big(R\mathrm{Ann}_M(I)\big) = (IR)\mathrm{Ann}_M(I) = I\mathrm{Ann}_M(I) = 0.$$

$R\mathrm{Ann}_M(I) \subseteq \mathrm{Ann}_M(I)$ and so $\mathrm{Ann}_M(I)$ is R-submodule of M.

(e) By (b) $\mathrm{Ann}_R(X)$ is left ideal. We have

$$\big(\mathrm{Ann}_R(X)R\big)X = \mathrm{Ann}_R(X)(RX) \subseteq \mathrm{Ann}_R(X)X = 0$$

and so $\mathrm{Ann}_R(X)R \subseteq \mathrm{Ann}_R(X)$.

(f) Put $I = \mathrm{I}_R(\mathrm{Ann}_R(X))$. Then I is an ideal of R and $I \subseteq \mathrm{Ann}_R(X)$ and so $X \subseteq \mathrm{Ann}_M(I)$. By (d), $\mathrm{Ann}_M(I)$ is a submodule of M and so $\langle X\rangle_R \leq \mathrm{Ann}_R(I)$. Thus $I \subseteq \mathrm{Ann}_R(\langle X\rangle_R)$.

Since $\langle X\rangle_R$ is an R-submodule of M, (e) show that $\mathrm{Ann}_R(\langle X\rangle_R)$ is an ideal in R. Since $X \subseteq \langle X\rangle_R$, $\mathrm{Ann}_R(\langle X\rangle) \subseteq \mathrm{Ann}_R(X)$ and so the definition of I implies $\mathrm{Ann}_R(\langle X\rangle_R) \subseteq I$.

(g) Recall that by (b) $\mathrm{Ann}_R(X)$ is an left ideal in R.

Note that (g:1) implies (g:2), and (g:2) implies (g:3) So in any case $\mathrm{Ann}_R(X)$ is a right ideal and thus also ideal in $\mathrm{Ann}_R(X)$. Thus $\mathrm{Ann}_R(X) = \mathrm{I}_R(\mathrm{Ann}_R(X))$ and (g) follows from (f). □

Example 3.1.25. Let I be non-empty set, K a ring with identity, $R = M_I{}^I(K)$ and $M = K_I$. Then M is an R-module by left multiplication. Let $e_j = (\delta_{ij})_{i\in I} \in K_I$ and $A \in R$. Then $Ae_j = A_{,j}$, the j'th column of A. So $\mathrm{Ann}_R(e_j)$ consists of all matrices in R whose j'th column is 0. Let $k \in K_I$ and pick $A \in R$ with $A_{,j} = k$. Then $k = Ae_j \in \langle e_j\rangle_R$ and we conclude that $Re_j = \langle e_j\rangle_R = K_I$. Hence $\mathrm{Ann}_R\big(\langle e_j\rangle_R\big) = \mathrm{Ann}_R(K_I) = 0$. So if $|I| \geq 2$ and $K \neq 0$,

$$\mathrm{Ann}_R\big(\langle e_j\rangle)_R\big) \neq \mathrm{Ann}_R(e_j)$$

Note also that by 3.1.24(d),

$$R/\mathrm{Ann}_R(e_j) \cong Re_j = K_I$$

as an R-module.

Lemma 3.1.26. *Let R be a ring and J a left ideal in R. View R/J is an R-module by left multiplication.*

(a) $\mathrm{Ann}_R(R/J) = \{a \in R \mid aR \subseteq J\}$.

(b) Suppose that R has an identity. Then

$$\mathrm{Ann}_R(1 + J) = J \qquad \textit{and } \mathrm{Ann}_R(R/J) = \mathrm{I}_R(J)$$

Proof. Let $a, b \in R$. Then $a \in \mathrm{Ann}_R(b + J)$ if and only if $ab + J = J$ and so if and only if $ab \in J$. This gives (a) and the first statement in (b). Since $R/J = \langle 1 + J\rangle_R$, the last assertion in (b) follows from the first and 3.1.24(f). □

3.2 Free modules and torsion modules

Definition 3.2.1. *Let V be an R-module and $v = (v_i)_{i\in I}$ a family of elements in V*

(a) V is called free R-module with respect to v if V is unitary and for all unitary R-modules W and all family of elements $(w_i)_{i\in I}$ in W there exists a unique R-linear map $f : V \to W$ with $f(v_i) = w_i$ for all $i \in I$.

(b) v is called R-linearly independent, if for all $r \in R_I$,

$$\sum_{i\in I} r_i v_i = 0 \qquad \Longrightarrow \qquad r = 0$$

(c) v is called a R-spanning family for all $u \in V$ there exists $r \in R_I$ with $u = \sum_{i\in I} r_i v_i$.

(d) v is called an R-basis for V if v is an R-linearly independent R-spanning family.

(e) Let c be a cardinality. Then we say that V is free of rank c if V is a free R-module with respect to w for some set J and some $w \in V^J$ with $|J| = c$.

Lemma 3.2.2. *Let R be a ring, V an R-module and $v = (v_i)_{i\in I}$ a family of elements in V. Define*

$$f_v : R_I \to V, r \to \sum_{i\in I} r_i v_i$$

(a) f_v is R-linear.

(b) f_v is 1-1 if and only if v is R-linearly independent.

(c) f_v is onto if and only if v spans V.

Proof. (a) Let $i \in I$. Observe that the functions $R_I \to R, r \to r_i$ and $R \to V$, $r \to rv_i$ are R-linear. Hence also the composition $f_i : R_I \to V, r \to r_i v_i$ and the sum $f = \sum_{i\in I} f_i$ are R-linear.

(b) v is linearly independent if and only if $\ker f_v = 0$ and so if and only if f_v is 1-1.

(c) Follows directly from the definition of a spanning. □

Lemma 3.2.3. *Let V be a unitary R-module and $v = (v_i)_{i\in I}$ a family of elements in V. Then the following statements are equivalent.*

(a) v is a basis for V.

(b) The map $f_v : R_I \to V, r \to \sum_{i\in I} r_i v_i$ is an R-isomorphism.

(c) For each $u \in V$ there exists a uniquely determined $r \in R_I$ with $u = \sum_{i\in I} r_i v_i$.

(d) V is free R-module with respect to v

Proof. (a) $\Longleftrightarrow$ (b) : Follows from 3.2.2.

(b) $\Longleftrightarrow$ (c) : Since f_v is F-linear, f is an R-isomorphism if and only if f is a bijection. So (c) and (b) are equivalent.

(b) $\Longrightarrow$ (d): Suppose f_v is isomorphism and let W be an unitary R-module and $w = (w_i)_{i\in I}$ a family in W. Define $f_w : R_I \to W,\ r \to \sum_{i\in I} r_i w_i$. Then by 3.2.2 f_w and so also $g := \circ f_v^{-1}$ is R-linear. Let $e_i = (\delta_{ij})_{j\in J}$. Since V and W are unitary, $f_v(e_i) = 1v_i = v_i$ and $f_w(e_i) = w_i$. Hence and $g(v_i) = w_i$. If $\tilde{g} : V \to W$ is linear with $\tilde{g}(v_i) = w_i$ for all $i \in I$, then $v_i \in \ker(g - \tilde{g})$. Since $\ker(g - \tilde{g})$ is an R-submodule of V and v spans V, $\ker(g - \tilde{g}) = V$ and so $g = \tilde{g}$.

(d) $\Longrightarrow$ (a): Let $r \in R_I$ with $\sum_{i\in I} r_i v_i = 0_V$. Fix $j \in I$. Then $(\delta_{ij})_{i\in I}$ is a family of elements in R and since V is free with respect to v there exists an R-linear map $f_j : V \to R$ with $f_j(v_i) = \delta_{ij}$ for all $i \in I$. Then

$$0_R = f_j(0_V) = f_j\Big(\sum_{i\in I} r_i v_i\Big) = \sum_{i\in I} r_i f_j(v_i) = \sum_{i\in I} r_i \delta_{ij} = r_j$$

So v is linearly independent. Let $W = \langle v_i \mid i \in I\rangle_R$. Then v is a family of elements in W and since V is free with respect to v, there exists an R-linear $h : V \to W$ with $h(v_i) = v_i$ for all $i \in I$. Thus h and id_V are R-linear functions from V to V with $h(v_i) = v_i = \mathrm{id}_V(v_i)$ for all $i \in I$. Thus by the uniqueness statement in the definition of free module, $h = \mathrm{id}_V$. Thus $V = \operatorname{Im} \mathrm{id}_V = \operatorname{Im} h \leq W$ and $W = V$. So v spans V and v is a basis. □

We will now investigate when all submodules of free R-modules are free. First an example.

Example 3.2.4. Let $R = \mathbb{Z}_n$ with $n \in \mathbb{Z}^+$, n not a prime. Let $V = \mathbb{Z}_n$, viewed as an $\mathbb{Z}_n$-module by left multiplication. Let $n = pq$ with $1 < q < n$. Then $q\mathbb{Z}_n$ is a proper submodule of $\mathbb{Z}_n$, but since $p(q\mathbb{Z}_n) = 0$ and $p \not\equiv 0 \pmod{n}$, $q\mathbb{Z}_n$ is not a free R-module.

An obvious necessary condition for all submodules of all free modules for a ring R to be free is that all submodules of R itself are free. The next theorem shows that this condition is also sufficient.

Theorem 3.2.5. *Let R be a ring with identity.*

(a) Suppose that all left ideals in R are free as R-modules. Then all R-submodule of all free R-modules are free.

(b) Suppose R is a PID and V is a free R-module of rank r. Then every R-submodule of V is free of rank less or equal to r.

Proof. Let $B \subseteq V$. We say that B is an R-basis for V if $(b)_{b\in B}$ is basis for V.

(a) Let M be a free R- module with basis $B \subseteq M$ and A an R-submodule in M. According to the well ordering principal (A.3.11) we can choose a well ordering $\leq$ on B. For $b \in B$ define

$$M_b^* = \langle e \in B \mid e < b\rangle_R \qquad \text{and} \qquad M_b = \langle e \in B \mid e \leq b\rangle_R$$

Note that $M_b = M_b^* \oplus Rb$. Put $A_b = M_b \cap A$ and $A_b^* = M_b^* \cap A$. Then

$$A_b/A_b^* = A_b/A_b \cap M_b^* \cong A_b + M_b^*/M_b^* \leq M_b/M_b^* \cong Rb \cong R.$$

By assumption every submodule of R is free and so A_b/A_b^* is free. Let $E_b \subseteq A_b$ such that $(e+A_b^*)_{e\in E_b}$ is a basis for A_b/A_b^*. Let $E = \bigcup_{b\in B} E_b$. We claim that E is a basis for A.

Let $0 \neq m \in M$. Then $m = \sum_{b\in B} r_b b$ for some $0 \neq r \in R_B$. Choose $b_m \in B$ maximal with respect $r_{b_m} \neq 0$. Then $m \in M_{b_m}$ and $m \notin M_{b_m}^*$. So b_m is minimal in B with $m \in M_{b_m}$. If $b \in B$ and $e \in E_b$, then $b_e = b$.

Now suppose that $\sum_{e\in E} s_e e = 0$ for some $0 \neq s \in R_E$. Define

$$b = \max\left\{b_e \;\middle|\; e \in E, s_e \neq 0\right\}$$

Let $e \in E$ with $s_e \neq 0$. If $b_e = b$, then $e \in E_b$. If $b_e \neq b$, then $b_e < b$ and so $e \in A_b^*$ Thus

$$0 + A_b^* = \Big(\sum_{e\in E} s_e e\Big) + A_b^* = \sum_{e\in E_b} s_e\big(e + A_b^*\big).$$

Since $s_e \neq 0$ for at least one $e \in E_b$, this contradicts the linear independence of the $(e + A_b^*)_{e\in E_b}$.

Hence E is linear independent. Let $b \in B$ we will show by induction on b, that $A_b \leq \langle E\rangle_R$. Suppose inductively that $A_c \leq \langle E\rangle_R$ for all $c < b$. If $v \in A_b^*$, then $b_v < b$ and so $c \in \langle E\rangle_R$ be the induction assumption. Hence $A_b^* \leq \langle E\rangle_R$. Let $w \in A_b$. Since $(e + A_b^*)_{e\in E_b}$ spans A_b/A_b^*, there exists $t \in R_{E_b}$ with

$$w + A_b^* = \sum_{e\in E_b} t_e e + A_b^*.$$

Put $u = \sum_{e\in E_b} t_e e$. Then $u \in \langle E\rangle_R$ and $w - u \in A_b^* \subseteq \langle E\rangle_R$. Hence also $w = (w - u) + u \in \langle E\rangle_R$. Thus $A_b \subseteq \langle E\rangle_R$.

If $0 \neq a \in A$, then $a \in A_{b_a} \subseteq \langle E\rangle_R$. So E spans A and E is a basis for A.

(b) Let I be a left ideal in R. Then $I = Ri$ for some $i \in R$. Since R is an integral domain, $\mathrm{Ann}_R(i) = \{0_R\}$ and so by 3.1.24(b), $R \cong R/\mathrm{Ann}_R(i) \cong Ri$. Then I is free of rank at most 1. Hence $|E_b| \leq 1$ for all $b \in \mathcal{B}$. Thus $|E| \leq |B|$ and (b) holds. □

The proof of the previous theorem is abstract in the sense that it shows the existence of basis, but does not provide a method to compute the basis. Using the proof to find a basis for a submodule A of the free module M with basis B one has to be able to:

(i) Find a well-ordering on B; and

(ii) For each $b \in B$ find basis $(e + A_b^*)_{e\in E_b}$ for A_b/A_b^*.

If B happens to be finite, (i) is no problem and if R is Euclidean domain, one can use the Euclidean Algorithm to carry out (ii).

Example 3.2.6. Find a $\mathbb{Z}$-basis for the $\mathbb{Z}$-submodule A of $\mathbb{Z}^3$ spanned by

$$a = \big((6,15,4),(9,10,3),(15,10,1)\big)$$

We choose the basis (e_1,e_2,e_3) for $\mathbb{Z}^3$ and the ordering $e_3 < e_2 < e_1$. Then $M_3^* = 0$, $M_3 = M_2^* = 0 \times 0 \times \mathbb{Z}$, $M_2 = M_1^* = 0 \times \mathbb{Z} \times \mathbb{Z}$ and $M_1 = \mathbb{Z}^3$. Then $A_1/A_3^1 = A/A_1^*$ is isomorphic the (left) ideal $\llbracket 6,10,15 \rrbracket = \llbracket \gcd(6,10,15) \rrbracket = \llbracket 3 \rrbracket$ of $\mathbb{Z}$. Note that $(9,10,3)-(6,15,4)=(3,-5,-1)$ maps to 3 under this isomorphism So we can choose $E_3 = \{d_3\}$ where $d_1 = (3,-5,-1)$. Note also that (a_1, d_1, a_3) spans A.

By construction 3 divides first coordinate of each elements of the spanning family of A . So we can subtract multiple of d_1 from a_1 and a_3 to obtain the following spanning family for A_2

$$b = \big((0,25,6),(0,35,6)\big)$$

Thus A_2/A_2^* is isomorphic to the ideal $\llbracket 25,40 \rrbracket = \llbracket \gcd(25,35) \rrbracket = \llbracket 5 \rrbracket$ of $\mathbb{Z}$. To obtain a spanning set for A_2 with a element whose second coordinate is 5 we imitate the Euclidean algorithm. Subtract the first element from the second to obtain the spanning set

$$\big((0,25,6),(0,10,0)\big)$$

Then subtract to twice the second element from the first

$$\big((0,5,0),(0,10,6)\big)$$

So we can choose $d_2 = (0,5,6)$ and then $d_3 = (0,10,0) - 2(0,5,6) = (0,0,-12)$. So the basis for A is

$$\big((0,0,-12),(0,5,6),(3,-5,-1)\big)$$

It should now be apparent that for a Euclidean domain R we obtain a Gaussian elimination process to compute a basis for any submodule of R^n giving by a spanning family. View your spanning family as rows of matrix. Starting at the first column use the Euclidean algorithm and row operation to obtain a leading entry in a column which divides all of entries of the column. Move the row of with the leading entry to the first row. Use further row operation to make all other entries in that column zero. Ignore the first row from now on and proceed with the column to the left.

Row operations one can use: Interchange any two columns, add a multiply of a row to another row, and multiply a row by a *unit*.

In matrix form the above example looks like this

$$\begin{bmatrix}6&15&4\\9&10&3\\15&10&1\end{bmatrix} \;{\scriptstyle -R1+R2\to R2}\; \begin{bmatrix}6&15&4\\3&-5&-1\\15&10&1\end{bmatrix} \;{\scriptstyle R1\leftrightarrow R2}\; \begin{bmatrix}3&-5&-1\\6&15&4\\15&10&1\end{bmatrix} \;\substack{-2R1+R2\to R2\\ -5R1+R3\to R3}\; \begin{bmatrix}3&-5&-1\\0&25&6\\0&35&6\end{bmatrix}$$

$$\;{\scriptstyle -R2+R3\to R3}\; \begin{bmatrix}3&-5&-1\\0&25&6\\0&10&0\end{bmatrix} \;{\scriptstyle -2R3+R2\to R2}\; \begin{bmatrix}3&-5&-1\\0&5&6\\0&10&0\end{bmatrix} \;{\scriptstyle -2R2+R3\to R3}\; \begin{bmatrix}3&-5&-1\\0&5&6\\0&0&-12\end{bmatrix}$$

Remark 3.2.7. *Let R be a commutative ring with identity and suppose that every (left) ideal in R is a free R-module. Then R is a PID.*

Proof. Let $a, b \in R^{\#}$. Then $ba - ab = 0$ and so (a, b) is linearly dependent. Hence every non-zero ideal in R is free of rank 1 and so a principal ideal. Let $a, b \in R^{\sharp}$ and (v) a basis for Rb. Then $0 \neq av \in aRb = Rab$ and so $ab \neq 0$. Thus R is also an integral domain and so a PID. □

Corollary 3.2.8. *Let R be a PID and M a unitary R-module and W an R-submodule of M. If $M = \langle I \rangle_R$ for some $I \subseteq M$, then $W = \langle J \rangle$ for some $J \subseteq W$ with $|J| \leq |I|$. In particular, if M is finitely generated as an R-module, so is M.*

Proof. Let $m = (i)_{i \in I}$. Then m spans M and $f_m : R_I \to M, r \to \sum_{i \in I} r_i i$ is onto. Let $A = f_m^{-1}(W)$. By 3.2.5 A has a basis $(a_k)_{k \in K}$ with $|K| \leq |I|$. Since f_m is onto, $f_m(A) = M$. Thus

$$M = f_m(A) = f_m(\langle a_k \mid k \in K \rangle_R) = \langle f_m(a_k) \mid k \in K \rangle_R$$

and the corollary holds with $J = f_m(K)$. □

Definition 3.2.9. *Let M be an R-module and $m \in M$.*

(a) $m \in M$ is called a torsion element *if $Rm = 0$ or $\mathrm{Ann}_R(m) \neq 0$, that is $rm = 0$ for some $r \in R^{\sharp}$*

(b) M is called a torsion module *if all elements are torsion elements.*

(c) M is called torsion free *if 0_M is the only torsion element.*

(d) M is called a faithful R-module if $\mathrm{Ann}_R(M) = 0$, that is if the canonical homomorphism from R to $\mathrm{End}(M)$ is 1-1.

(e) M is a bounded R-module if R is not-faithful, that is $rM = 0$ for some $r \in R^{\sharp}$.

Note that m is not a torsion element if and only if $Rm \neq 0$ and (m) is linearly independent.

Example 3.2.10. Let $R = \mathbb{Z}$.

1. Consider $M = \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Since $2(1, 0) = (2, 0) = (0, 0)$, $(1, 0)$ is a torsion element. Also $3(0, 1) = (0, 3) = (0, 0)$ and so $(0, 1)$ is a torsion element. In fact $6(a, b) = (2(3a), 3(2b)) = (0, 0)$ for all $(a, b) \in M$ and so M is bounded.

2. Consider $\mathbb{Z}^I$. If $rz = 0$ for some $0 \neq r \in \mathbb{Z}$ and $z \in \mathbb{Z}^I$, then $rz_i = 0$ for all $i \in I$ and so $z_i = 0$ and $z = 0$. Hence $\mathbb{Z}^I$ is torsion-free.

3. Consider $M = \bigoplus_{i \in \mathbb{Z}^+} \mathbb{Z}_i$. Let $m = (m_i)_{i \in \mathbb{Z}^+} \in M$. By definition of the direct sum there exists $k \in \mathbb{Z}^+$ with $m_i = 0$ for all $i > k$. We claim that $k!m = 0_M$. Indeed of $i \leq k$, then $i \mid k!$ and so $k!m_i = 0$ in $\mathbb{Z}_i$. And if $i > k$, then $m_i = 0$ and again $k!m_i = 0$. Thus M is a torsion module.

   But M is not bounded, indeed suppose that $r \in \mathbb{Z}^+$ with $rm = 0_M$ for all $m \in M$. Let $i \in \mathbb{Z}^+$ and pick $m \in M$ with $m_i = 1$. From $rm = 0$ we get $0 = rm_i = r1 = r$ in $\mathbb{Z}_i$ and so $i \mid r$. Hence $|r| \geq i$ for all $i \in \mathbb{Z}^+$, a contradiction.

Lemma 3.2.11. *Let R be an integral domain and $\mathcal{F}$ a finite set of non-zero ideals in R. Then $\bigcap \mathcal{F} \neq 0$.*

Proof. Since R is an integral domain, $\prod_{F\in\mathcal{F}} F \neq 0$. Since $\prod_{F\in c\alpha} F \subseteq \bigcap \mathcal{F}$ the lemma holds. □

Lemma 3.2.12. *Let M be a module for the integral domain R.*

(a) Let I be a finite set of torsion elements in M. Then $\langle I\rangle_R$ is a bounded R-submodule of M.

(b) Let $\mathrm{T}(M)$ be the set of torsion elements in M. Then $\mathrm{T}(M)$ is R-submodule of M.

(c) $M/\mathrm{T}(M)$ is torsion free.

Proof. (a) Since each $i \in i$ is a torsion element, $\mathrm{Ann}_R(i) \neq 0$ for all $i \in I$. Thus by 3.2.11

$$\mathrm{Ann}_R(I) = \bigcap_{i\in I} \mathrm{Ann}_R(i) \neq 0$$

By 3.1.24(g) $\mathrm{Ann}_R(\langle I\rangle_R) = \mathrm{Ann}_R(I)$. and so $\mathrm{Ann}_R(\langle I\rangle_R) \neq 0$.

(b) Since $R0_M = 0_M$, $0_M \in \mathrm{T}(M)$. If $x, y \in \mathrm{T}(M)$ and $r \in R$, then by (a), $x+y \in \mathrm{T}(M)$, $-x \in \mathrm{T}(M)$ and $rx \in \mathrm{T}(M)$. Thus $\mathrm{T}(M)$.

(c) Let $x \in M/\mathrm{T}(M)$ be a torsion element. Pick $m \in M$ with $x = m + \mathrm{T}(M)$ and $r \in R^\sharp$ with $rx = 0_{M/\mathrm{T}(M)}$. Then $rm \in \mathrm{T}(M)$ and so $s(rm) = 0_M$ for some $s \in R^\sharp$. Hence $(sr)m = 0_M$ and as R is an integral domain, $sr \neq 0_R$. So $m \in T(M)$, $x = m + \mathrm{T}(M) = 0_{M/\mathrm{T}(M)}$ and $M/\mathrm{T}(M)$ is torsion free. □

Theorem 3.2.13. *Let R be a ring and M an R-module.*

(a) Any linearly independent subset of M lies in a maximal linear independent subset.

(b) Let L be a maximal linear independent subset of M. Then $M/\langle RL\rangle$ is a torsion module, and if M is unitary, $\langle RL\rangle$ is free R-module with basis L.

Proof. (a) Let E be a linearly independent subset of M. Let $\mathcal{L}$ be the set of linearly independent subsets of M containing E. Since $E \in \mathcal{L}$, $\mathcal{L} \neq \varnothing$. Order $\mathcal{L}$ by inclusion. Let $\mathcal{C}$ be a non-empty chain in $\mathcal{L}$ and put $D = \bigcup \mathcal{C}$.

We will show that D is linearly independent. For this let $r \in R_D$ with $\sum_{d\in D} r_d d = 0_V$. Let $F = \{d \in D \mid r_d \neq 0\}$ and note that F is finite. Let $f \in F$. Since $f \in D = \bigcup \mathcal{C}$, there exists $C_f \in \mathcal{C}$ with $f \in C_i$. Since $\{C_f \mid f \in F\}$ is a finite it has maximal element C. Then $f \in C_f \subseteq C$ for all $f \in F$. Then

$$0 = \sum_{d\in D} r_d d = \sum_{d\in F} r_d d = \sum_{d\in C} r_d d$$

and since C is linearly independent, $r_d = 0$ for all $d \in D$. Hence also $r_f = 0$ for all $f \in F$. So $F = \varnothing$ and $r = 0$. Thus D is linearly independent, $D \in \mathcal{L}$ and D is an upper bound for $\mathcal{C}$.

Thus the assumptions of Zorn's Lemma A.3.8 are fulfilled and we conclude that $\mathcal{L}$ contains a maximal element L. Then L is a maximal linearly independent subset of M containing E.

(b) Put $W = \langle RL\rangle$. Let $v \in V$. We need to show that $v + W$ is a torsion element. If $v \in L$, then $Rv \subseteq W$ and so $R(v + W) = 0_{v/W}$ and $v + W$ is a torsion element. So suppose $v \notin L$. By maximality of L $\{v\} \cup L$ is linearly dependent. Hence there exist $s \in R$ and $r \in R_L$ such that

$$sv + \sum_{l \in L} r_l l = 0$$

and at least one of s and r is not zero.

If $s = 0$, then since L is linearly independent, $r = 0$, a contradiction. Thus $s \neq 0$ and $sv = -\sum_{l \in L} r_l l \in \langle RL \rangle$. Hence $s(v + W) = 0_{V/W}$ and V/W is a torsion module.

If V is unitary, then $W = \langle L \rangle_R$ and so L is basis for W. □

We remark that if L is a maximal linear independent subset of the unitary R-module M, then $\langle L \rangle$ does not have to be a maximal free submodule. Indeed the following example shows that M does not even have to have a maximal free submodule. (Zorn's lemma does not apply as the union of a chain of free submodules might not be free)

Example 3.2.14. Let $R = \mathbb{Z}$ and $M = \mathbb{Q}$ with $\mathbb{Z}$ acting on $\mathbb{Q}$ by left multiplication. As $\mathbb{Q}$ has no zero divisors, $\mathbb{Q}$ is torsion free. In particular, every non-zero element a is linearly independent. We claim $\{a\}$ is a maximal linearly independent subset. Indeed, let $a, b \in \mathbb{Q}^\sharp$. Then $a = \frac{n}{m}$ and $b = \frac{p}{q}$ with $n, p \in \mathbb{Z}$ and $m, q \in \mathbb{Z}^\sharp$. Then

$$(mp)a + (-nq)b = mp\frac{n}{m} - nq\frac{p}{q} = pn - np = 0$$

and (a, b) is linearly dependent.

We conclude that every non-zero free submodule of $\mathbb{Q}$ is of the form $\mathbb{Z}a, a \in \mathbb{Q}^\sharp$. Since $\mathbb{Z}a \not\leq \mathbb{Z}\frac{a}{2}$ we see that $\mathbb{Q}$ has no maximal free $\mathbb{Z}$-submodule. In particular, $\mathbb{Q}$ is not free $\mathbb{Z}$-module.

$\mathbb{Q}$ as a $\mathbb{Z}$ module has another interesting property: every finitely generated submodules is cyclic Indeed, if A is generated by $\frac{n_i}{m_i}, 1 \leq i \leq k$, put $m = \mathrm{lcm}_{1 \leq i \leq k} m_i$. Then $mA \cong A$ and $mA \leq \mathbb{Z}$. So mA and A are cyclic.

Corollary 3.2.15. *Let D be a division ring and V a unitary D-module.*

(a) V is torsion free.

(b) If V is a torsion module, then $V = 0$.

(c) Every linear independent subset of V is contained in a basis of V.

(d) V has a basis and so is a free D-module.

Proof. (a) Let $d \in D^\sharp$ and $v \in V$ with $dv = 0_V$. Since D is a division ring $ed = 1_D$ for some $e \in D$. Thus $v = 1_D v = edv = e0_V = 0_V$ and so V is torsion free.

(b) This follows from (a).

(c) Let L be linearly dependent subset of V. By 3.2.13 L is contained in a maximal linearly dependent subset B. Also by 3.2.13, $V/\langle RB \rangle$ is a torsion module. So (b) applied to $V/\langle RB \rangle$ is a zero-module and so $V = \langle RB \rangle$ and B is a basis for V.

(d) By (c) applied to $L = \emptyset$, V has a basis and so by 3.2.3 V is free. □

Lemma 3.2.16. *Let $f : A \to B$ be group homomorphism and $D \leq B$. Put $F = \ker f$. Then* *(a)* $f\,|_D\colon D \to B$ *is onto if and only if* f *is onto and* $A = FD$.

(b) $f\,|_D$ *is 1-1 if and only if* $F \cap D = 1$.

(c) $f|_D : D \to B$ *is bijection if and only if* f *is onto,* $A = FD$ *and* $F \cap D = 1$.

Proof. (a) Suppose first that $f\,|_D$ is onto. Then also f is onto. Let $a \in A$. Then $f(a) = f(d)$ for some $d \in D$. Thus $ad^{-1} \in \ker f = F$ and $a = ad^{-1}d \in FD$.

Suppose next that f is onto and $A = FD$. Let $b \in B$. Since f is onto, $b = f(a)$ for some $a \in A$. Since $A = FD$, $a = cd$ for some $c \in F$ and $d \in D$. Thus $b = f(a) = f(cd) = f(c)f(d) = 1f(d) = f(d)$ and so $f\,|_D$ is onto.

(b) is obvious and (c) follows from (a) and (b). □

Lemma 3.2.17. *Let R be a ring, V a unitary R-module and W an R-submodule of V. If* V/W *is a free R-module, then there exists an R-submodule F of V with* $V = F \oplus W$. *Moreover,* $F \cong V/W$ *and so F is a free R-module.*

Proof. Let V/W be free with respect to the family $(x_i)_{i\in I}$ in V/W. By the axiom of choice there exists a family $(v_i)_{i\in I}$ with $v_i \in x_i$ for all $i \in I$. Then $x_i = v_i + W$ for all $i \in I$. The definition of a free module implies that there exists an R-linear map$f : V/W \to V$ with $f(x)i) = v_i$ for all $i \in I$. Define $g : V/W \to V/W, x \to f(x) + W$. Then $g(x_i) = v_i + W = x_i$ for all $i \in I$ and so by the uniqueness assertion in the definition of a free module, $g = \mathrm{id}_{V/W}$. Define $h : V \to V, v \to f(v + W)$. Then for $v \in V$,

$$h(v) + W = f(v + W) + W = g(v + W) = v + W$$

Finally define $k = \mathrm{id}_W - h$. Then $k(v) = v - h(v) \in W$ for all $v \in V$ and so k is function from V to W. If $w \in W$, then $h(w) = f(w + W) = f(0_{V/W} = 0$ and so

$$k|_W = \mathrm{id}_W - h|_W = \mathrm{id}_W$$

3.2.16 now shows that $V = F \oplus W$ for the R-submodule $F = \ker k$ of V. The second isomorphism theorem gives $V/W = (F \oplus W)/W \cong F/F \cap W = F/0 \cong F$ and the lemma is proved. □

Lemma 3.2.18. *Let D be a division ring, V a D-module and W a D-submodule. Then there exists a D-submodule K of V with* $V = K \oplus W$.

Proof. By 3.2.15(b), V/W is a free D-module and so the lemma follows from 3.2.17. □

Lemma 3.2.19. *Let M be a torsion free R-module for the integral domain R. Suppose that one of the following holds:*

1. M is finitely generated.

2. If N is a submodule of M such that M/N *is a torsion module, then* M/N *is bounded.*

Then there exists a free R-submodule W such that M is isomorphic to a submodule W. In particular, M is isomorphic to a submodule of free R-module.

Proof. Suppose (1) holds and let N be an R-submodule of M such that M/N is a torsion module. Then M/N is a finitely generated torsion module and 3.2.12 implies that M/N is bounded. Hence condition (1) implies condition (2).

So we may assume that (2) holds. By 3.2.13 there exists a free submodule W of V such that M/W is torsion. By (2) there exists $r \in R^\sharp$ with $rx = 0_{M/W}$. Hence $rM \leq W$.

Consider the map

$$\alpha : M \to W, m \to rm.$$

Since R is commutative, α is a R-linear. As M is torsion free, α is 1-1. Thus $M \cong \alpha(M) = rM \leq W$. □

3.3 Modules over PIDs

Definition 3.3.1. *Let R be a PID, M an R-module, $X \subseteq\in M$ and $r \in R$. Then we say that X has R-exponent r and write $r \sim \exp_R(X)$ if $\mathrm{Ann}_R(X) = \llbracket r \rrbracket$.*

Example 3.3.2. *Let A be abelian group. Then A is a $\mathbb{Z}$-module and $\exp_{\mathbb{Z}}(X) \sim \exp(X)$ for all $X \leq A$. Moreover, $\exp_{\mathbb{Z}}(a) \sim |a|$ for all $a \in A$.*

Lemma 3.3.3. *Let R be PID, M an R-module and $X \subseteq M$. Then*

$$\exp_R(\langle X \rangle_R) = \exp_R(X) = \operatorname*{lcm}_{x \in X} \exp_R(x)$$

Proof.

$$\mathrm{Ann}_R(\langle X \rangle_R) = \mathrm{Ann}_R(X) = \bigcap_{x \in X} \mathrm{Ann}_R(x) = \bigcap_{x \in X} \llbracket (\exp_R(x) \rrbracket = \llbracket \operatorname*{lcm}_{x \in X} \exp_R(x) \rrbracket$$

□

Lemma 3.3.4. *Let R be PID, M an R-module, $m \in M$ and $e \in R$ with $e \sim \exp_R(m)$. Then*

(a) $Rm \cong R/\llbracket e \rrbracket$ as an R-module.

(b) Let $r \in R$. Then $e \mid r$ if and only if $rm = 0$.

(c) Suppose M is unitary, $m \neq 0$ and $e = p^l$ for some prime p and some $l \in \mathbb{N}$. Then $p \mid r$ for all $r \in \mathrm{Ann}_R(M)$.

Proof. (a) By 3.1.24(b), $Rm \cong R/\mathrm{Ann}_R(m)$. Since $\mathrm{Ann}_R(m) = \llbracket e \rrbracket$, (a) holds.

(b) Follows from $\mathrm{Ann}_R(m) = \llbracket e \rrbracket$.

(c) Since M is unitary, $1m \neq 0$ and so $\mathrm{Ann}_R(m) \neq R$ and $l \geq 1$. Thus $p \mid e$ and(c) follows from (b). □

Theorem 3.3.5. *Let R be a PID and $p \in R$ a prime. Suppose that M is a unitary R-module with $p^k M = \{0_M\}$ for some $k \in \mathbb{N}$. Then M is a direct sum of non-zero cyclic submodules of M.*

Proof. The proof is by induction on k. If $k = 0$, then, since M is unitary, $M = \{0\}$ and the theorem holds.

So suppose $k > 0$. Since $p^{k-1}(pM) = p^kM = \{0_M\}$ we conclude by induction on k that there exist non-zero cyclic submodules $A_i, i \in I$ of pM with $M = \bigoplus_{i\in I} A_i$. Since A_i is cyclic $A_i = \langle a_i\rangle_R = Ra_i$ for some $a_i \in A_i$. Thus

1°. $pM = \bigoplus_{i\in I} Ra_i$

Since A_i is non-zero, $a_i \neq 0$. Since $a_i \in pM$ there exists $b_i \in B$ with $a_i = pb_i$. Put

$$B = \langle b_i \mid i \in I\rangle_R = \sum_{i\in I} Rb_i.$$

We will show

2°. $B = \bigoplus_{i\in I} Rb_i$

For this let $r \in R_I$ with

$$(*) \qquad \sum_{i\in I} r_i b_i = 0_M.$$

We need to show that $r_ib_i = 0_M$ for all $i \in I$. From (*) we have

$$\sum_{i\in I} r_i a_i = \sum_{i\in I} r_i p b_i = p\sum_{i\in I} r_i b_i = p0_M = 0_M.$$

Thus (1°) implies that $r_ia_i = 0_M$ for all $i \in I$. By 3.3.4(c), $p \mid r_i$ and so $r_i = t_ip$ for some $t_i \in R$. Then $r_ib_i = t_ipb_i = t_ia_i$ and

$$(**) \qquad r_ib_i = t_ia_i.$$

Substitution into (*) gives:

$$\sum_{i\in I} t_ia_i = 0_M.$$

Thus by (1°), $t_ia_i = 0_M$ and by (**) $r_ib_i = 0_M$. Hence (2°) holds.

3°. $M = \mathrm{Ann}_M(p) + B.$

We have $pB = p\sum_{i\in I} Rb_i = \sum_{i\in I} Rpb_i = \sum_{i\in I} Ra_i = pM$. Define $\alpha : M \to pM, m \to pm$. Then α is R-linear and $\alpha(B) = pM$. Thus by 3.2.16(a) $M = \ker\alpha + B = \mathrm{Ann}_M(p) + B$.

4°. *R/Rp is a field and $\mathrm{Ann}_M(p)$ is module for R/Rp.*

Since p is a prime, R/Rp is a field by 2.5.17. Since $Rp \leq \mathrm{Ann}_R(\mathrm{Ann}_M(p))$, $\mathrm{Ann}_M(p)$ is an R/Rp module via $(r + Rp)m = rm$.

5°. *There exists an R-submodule D of $\mathrm{Ann}_M(p)$ with $\mathrm{Ann}_M(p) = D \oplus \mathrm{Ann}_B(p)$ and $M = D \oplus B$.*

Since R/Rp is a field we conclude from 3.2.18 that $\mathrm{Ann}_M(p) = D \oplus \mathrm{Ann}_B(p)$ for some R/Rp submodule D of $\mathrm{Ann}_M(p)$. Then D is also an R-submodule of $\mathrm{Ann}_M(p)$. We have

$$M = \mathrm{Ann}_M(p) + B = D + \mathrm{Ann}_B(p) + B = D + B$$

and

$$D \cap B = D \cap \mathrm{Ann}_M(p) \cap B = D \cap \mathrm{Ann}_B(p) = \{0_M\}.$$

So $M = D \oplus B$.

We now can complete the proof of the theorem. By 3.2.15(b), the R/Rp-module D has a basis $(d_j)_{j\in J}$. Then

$$D = \bigoplus_{j\in J} R/pR \cdot d_j = \bigoplus_{j\in J} Rd_j.$$

Together with (2°) and (5°) we get

$$M = D \oplus B = \bigoplus_{j\in J} Rd_j \ \oplus \ \bigoplus_{i\in I} Rb_i$$

□

Theorem 3.3.6. *Let M be a finitely generated module for the PID R. Then there exists a free submodule $F \leq M$ with $M = F \oplus \mathrm{T}(M)$.*

Proof. By 3.2.12, $M/\mathrm{T}(M)$ is torsion free, so by 3.2.19 $M/\mathrm{T}(M)$ is isomorphic to a submodule of a free module. Hence by 3.2.5 $M/\mathrm{T}(M)$ is free. Thus by 3.2.17 $M = F \oplus \mathrm{T}(M)$ for a free R-submodule F of M. □

Definition 3.3.7. *Let R be a PID, P a set of representatives for the associate classes of primes in R and $Q \subseteq P$.*

(a) Let $0 \neq r \in R$. Then r is called a Q-elements if $r \sim \prod_{q\in Q} q^{n_q}$ for some $n \in \mathbb{N}_Q$. (Here we interpret the empty product as 1, so a $\varnothing$-element is a unit.)

(b) Let M be an R-module. Then $m \in M$ is called an Q-element if $\exp_R(m)$ is a Q-elements. M_Q is the set of Q-elements in M.

Theorem 3.3.8. *Let R be a PID, M a unitary torsion R module R, P a set of representatives for the associated classes of primes in R and $Q, T \subseteq P$. Put $Q' = P \setminus Q$. Then*

(a) Let $m \in M$. Then m is a Q-elements if and only if $rm = 0$ for some Q-elements $r \in R$.

(b) M_Q is an R-submodule of M.

(c) M/M_Q has no-nonzero Q-elements and all elements of M/M_Q are Q'-elements.

(d) $M_Q \cap M_R = M_{Q\cap R}$.

(e) $M_\varnothing = 0$ and so $M_Q \cap M_{Q'} = 0$.

(f) $M_Q = \bigoplus_{q\in Q} M_q$.

(g) $M = \bigoplus_{p\in P} M_p$.

Proof. (a) This holds since $\exp_R(m)|r$ for all $r \in R$ with $rm = 0$.

(b) Let x, y be Q-elements. Then $\exp_R(\langle x, y\rangle_R) = \operatorname{lcm}\big(\exp_R(x), \exp_R(y)\big)$ is a Q-element in R. Hence (a) shows that all elements in $\langle x, y\rangle_R$ are Q-elements. Hence $\langle x, y\rangle_R \subseteq M_Q$ and M_Q is an R-submodule of M.

(c) Let $m + M_Q$ be a Q-elements. Then $em \in M_Q$ for some Q-elements $e \in R$. So em is a Q-element and $f(em) = 0$ for some Q-elements f in R. Then fe is a Q-element in R and $(fe)m = 0$. So $m \in M_Q$ and $m + M_Q = 0_{M/M_Q}$.

Now let w be any elements of M/M_Q and $d \sim \exp_R(w)$. Then $d \sim ef$ for some Q-element e and Q'-element f. Then $e(fw) = 0$, fw is a Q-element and $fw = 0$ and w is a Q'-element.

(d) By the uniqueness of prime factorization $r \in R$ is a $Q \cap T$ element if and only if r is a Q and a T-elements. So (d) holds.

(e) If m is $\varnothing$-element in M, then $um = 0$ for some unit u. Then also $1m = u^{-1}um = 0$ and since M is unitary, $m = 0$.

(f) Let $W = \sum_{q\in Q} M_Q$. Let $q \in Q$. By (c) all elements in M/M_q are q'-elements. Thus also all elements in M/W are q' elements and so Q'-elements. Thus all elements of M_Q/W are Q and Q'-elements. Hence (e) applied to M/W shows that $M_Q/W = 0$ and so $W = M_Q$. Thus $M_Q = \sum_{q\in Q} M_Q$. Now

$$M_q \cap \sum_{\substack{t\in Q \\ t\neq q}} M_t \subseteq M_q \cap M_{q'} = 0$$

and so $M_Q = \sum_{q \in Q} M_q$.

(g) Since M is a torsion-module, $M = M_P$. So (g) follows from (f) applied with $P = Q$. □

Lemma 3.3.9. *Let R be a ring, and $(M_i)_{i \in I}$ a family of non-zero R-modules. If $\bigoplus_{i \in I} M_i$ is finitely generated, then I is finite.*

Proof. Let A be a finite subset of $M := \bigoplus_{i \in I} M_i$ with $M = \langle A \rangle_R$. By definition of "direct sum" each m is a tuple $(m_i)_{i \in I}$ with almost all m_i zero. So for $a \in A$ we can choose a finite subset J_a of I with $a_k = 0$ for all $k \in I \setminus J_a$. Put $J = \bigcup_{a \in A} J_a$. Then J is finite. We will show that $J = I$. For this let $i \in I$ and put $W = \{m \in M \mid m_i = 0\}$. Then W is a R-submodule of M and since $M_i \neq 0$, $W \neq M$. Since $M = \langle A \rangle_R$ we get $A \nsubseteq W$ and so $a_i \neq 0$ for some $a \in A$. Thus $i \in J_a \subseteq J$, $I = J$ and I is finite. □

Theorem 3.3.10. *Let M be a finitely generated module for the PID R. Then M is direct sum of finitely many cyclic R-modules. Moreover, each of the summand can be chosen be isomorphic to R or R/p^kR for some prime ideal $p \in R$ and some $k \in \mathbb{Z}^+$. In other words,*

$$M \cong \underbrace{R \oplus R \oplus \ldots \oplus R}_{k\text{-times}} \oplus R/p_1^{k_1}R \oplus R/p_2^{k_2}R \oplus \ldots \oplus R/p_n^{k_n}R$$

for some $k, n \in \mathbb{N}$, $k_1, k_2 \ldots, k_n \in \mathbb{Z}^+$ and primes $p_1, p_2, \ldots, p_n \in R$.

Proof. By 3.3.6, $M = F \oplus T(M)$, where F is a free R-module. So F is a direct sum of copies of R. Also by 3.3.8 $T(M) = \bigoplus_{p \in P} M_p$, where P is set of representatives for the associate classes of primes in R. Let $p \in P$. Since M is finitely generated and M_P is a homomorphic image of M, M_p is finite generated. Thus $M_p = \langle I \rangle_R$ for some finite subset I of M_P. For $i \in I$ pick $l_i \in \mathbb{N}$ with $p^{l_i} i = \{0_M\}$ and put $l = \max_{i \in I} l_i$. Then $p^l M_p = \{0_M\}$. Thus by 3.3.5 M_p is the direct sum of non-zero cyclic submodules. By 3.3.4 each of these cyclic submodules is isomorphic to R/p^kR for some $k \in \mathbb{Z}^+$.

It follows that M is a direct sum modules of the form R or R/p^kR, $p \in P$, $k \in \mathbb{Z}^+$. Since M is finitely generated, 3.3.9 this direct sum is a finite direct sum. □

Corollary 3.3.11. *(a) Let A be a finitely generated abelian group. Then A is the direct sum of cyclic groups.*

(b) Let A be an elementary abelian *p-group for some prime p. (That is A is abelian and $pA = 0$). Then A is the direct sum of copies of $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Note that an abelian group is nothing else as a module over $\mathbb{Z}$. So (a) follows from 3.3.10 and (b) follows from 3.3.5 and 3.3.4

(b) can also by proved by observing that A is also a module over the field $\mathbb{Z}/p\mathbb{Z}$ and so has a basis. □

3.4 Jordan Canonical Form

Definition 3.4.1. *Let R be a ring, V and W R-modules, $A \in \mathrm{End}_R(V)$ and $B \in \mathrm{End}_R(W)$. We say that A and B are* similar *over R if there exists a R-linear isomorphism $\Phi : V \to W$ with $\Phi \circ A = B \circ \Phi$.*

We leave it as an exercise to show that ”similar” is an equivalence relation. Also the condition $\Phi \circ A = B \circ \Phi$ is equivalent to $B = \Phi \circ A \circ \Phi^{-1}$.

Remark 3.4.2. *Let R be a ring and V a module over R. Let $A \in \mathrm{End}_R(V)$. $*^*_R : \alpha : R \to \mathrm{End}_{\mathbb{Z}}(V), r \to r^*$ be the ring homomorphism associated to the action of R on M. we will usually right $r\mathrm{id}_V$ for $\alpha(r)$. Since A is R-linear, A commutes with each r^*, $r \in R$ and so by 2.2.19(b) there exists a unique ring homomorphism $\alpha_A : R[x] \to \mathrm{End}_{\mathbb{Z}}(V)$ with $r \to r^*$ and $x \to A$. Let $f = \sum_{i=0}^n f_i x^i \in R[x]$. We will write $f(A)$ for $\alpha_A(f)$. Then $f(A) = \sum_{i=0}^n f_i^* A^i$. It follows that V is a $R[x]$-module with*

$$fv = f(A)(v) = \sum_{i=0}^{n} f_i(A^i(v)).$$

To indicate the dependence on A we will sometimes write V_A for the $R[x]$ module V obtain in this way.

Lemma 3.4.3. *Let R be a ring and V and W R-modules. Let $A \in \mathrm{End}_R(V)$. and $B \in \mathrm{End}_R(V)$. Then the $R[x]$-modules V_A and W_B are isomorphic if and only if A and B are similar over R.*

Proof. Suppose first that V_A and V_B are isomorphic. Then there exists an $R[x]$-linear isomorphism $\Phi : V \to W$. In particular Φ is R-linear and $\Phi(xv) = x\Phi(v)$ for all $v \in V$. By definition of V_A and W_B thus means $\Phi(A(v)) = B(\Phi(v)$ and so A and B and are similar.

Conversely, if A and B are similar there exists an R-linear isomorphism $\Phi : V \to W$ with $\Phi \circ A = B \circ \Phi$. Hence $\Phi(rv) = r\Phi(v)$ and $\Phi(xv) = x\Phi(v)$ for all $r \in R$ and $v \in V$. Since Φ is $\mathbb{Z}$-linear this implies $\Phi(fv) = f\Phi(v)$ for all $f \in R[x]$. Hence Φ is an $R[x]$-linear isomorphism. □

Definition 3.4.4. *Let R be a ring with identity, V and W free R-modules with basis $v = (v_i)_{i \in I}$ and $w = (w_j)_{j \in J}$, respectively. Let $A \in \mathrm{End}_R(V)$. Then the matrix $M = M_{vw}(A)$ of A with respect to v and w is matrix in $M^I_J(R)$ defined by by*

$$A(v_i) = \sum_{j \in J} M_{ij} w_j$$

for all $i \in I$.

Lemma 3.4.5. *Let R be a ring, V and W R-modules, $A \in \mathrm{End}_R(V)$ and $B \in \mathrm{End}_R(W)$. Suppose that V is free with basis $v = (v_i)_{i \in I}$. Then A and B are similar if and only if there exists a basis $w = (w_i)_{i \in I}$ for W with*

$$M_{vv}(A) = M_{ww}(B)$$

Proof. Let $M = M_{vv}(A)$. Let $\Phi : V \to W$ be R-linear and $w_i \in W$ with $w_i = \Phi(v_i)$ for all $i \in I$. We compute

$$(*) \qquad \Phi\big(A(v_i)\big) = \Phi\big(\sum_{j \in J} M_{ij} v_j\big) = \sum_{j \in J} M_{ij} \Phi(v_j) = \sum_{j \in J} M_{ij} w_j$$

$\Longrightarrow$: Suppose first that A and B are similar. Then there exists an R-linear isomorphism $\Phi : V \to W$ with $\Phi \circ A = B \circ \Phi$. Define $w_i = \Phi(v_i)$ and $w = (w_i)_{i\in I}$. As I is a basis for V and Φ is an R-isomorphism, w is a basis for W. We compute

$$B(w_i) = B\big(\Phi(v_i)\big) = \Phi\big(A(v_i)\big) \overset{(*)}{=} \sum_{j\in J} M_{ij} w_j$$

Hence $M_{ww}(B) = M = M_{vv}(A)$.

$\Longleftarrow$: Suppose conversely that there exists a basis $w = (w_i)_{i\in I}$ with $M_{vv}(A) = M_{ww}(B)$.

Let $\Phi : V \to W$ be the unique R-linear map from V to W with $\Phi(v_i) = w_i$ for all $i \in I$. As v and w are R-bases, Φ is an R- isomorphism. Moreover,

$$(\Phi \circ A)(v_i) = \Phi(A(v_i)) \overset{(*)}{=} \sum_{j\in J} M_{ij} w_j = Bw_i = B(\Phi(v_i)) = (B \circ \Phi)(v_i)$$

Since V is free with respect to $(v_i)_{i\in I}$ this implies $\Phi \circ A = B \circ \Phi$ and so A and B are similar. □

Lemma 3.4.6. *Let R be a ring and $f = \sum_{i=0}^n a_i x^i$ a monic polynomial of degree $n > 0$. Let $I = R[x]f$ be the left ideal in $R[x]$ generated by f. Let $A \in \mathrm{End}_R(R[x]/I)$ be defined by $A(h+I) = hx + I$.*

(a) $(x^i)_{i\in\mathbb{N}}$ is a basis for $R[x]$ as a left R-module.

(b) For $0 \le i < n$ let h_i be a monic polynomial of degree i in $R[x]$. Then $(h_i + I)_{i=1}^{n-1}$ is basis for $R[x]/I$.

(c) The matrix of A with respect the basis $(x^i + I)_{i=0}^{n-1}$ of $R[x]/I$ is

$$M(f) := \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ -f_0 & -f_1 & -f_2 & \dots & -f_{n-2} & -f_{n-1} \end{bmatrix}$$

(d) Suppose that $f = g^m$ for some monic polynomial g of degree s and some $m \in \mathbb{Z}^+$. Let E^{s1} be the $s \times s$-matrix in $\mathbb{K}$ with $E^{s1}_{ij} = 0$ if $(i,j) \neq (s,1)$ and $E^{s1}_{s1} = 1$. Then the matrix of A with respect to the basis

$$\big(1 + I, x + I, \dots x^{s-1}, g + I, xg + I, \dots, x^{s-1}g + I, \dots, g^{m-1} + I, xg^{m-1} + I, x^{s-1}g^{m-1} + I\big)$$

of $R[x]/I$ is

$$M(g,m) := \begin{bmatrix} M(g) & E^{s1} & 0 & \dots & 0 & 0 & 0 \\ 0 & M(g) & E^{s1} & \ddots & 0 & 0 & 0 \\ 0 & 0 & M(g) & \ddots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & M(g) & E^{s1} & 0 \\ 0 & 0 & 0 & \ddots & 0 & M(g) & E^{s1} \\ 0 & 0 & 0 & \dots & 0 & 0 & M(g) \end{bmatrix}$$

Proof. (a) is obvious as any polynomial can be uniquely written as R-linear combination of the x^i.

(b): We will first show by induction on $\deg h$ that every $h+I, h \in R[x]$ is a R linear combination of the $h_i, 0 \leq i < n$. Since f is monic, long division of polynomials shows that $h = qf + r$ for some $q, r \in R[x]$ with $\deg r < \deg f = n$. Since $h + I = r + I$ we may assume that $h = r$ and so $i := \deg h < n$. Let a be the leading coefficient of h. Then $\deg h - ah_i < \deg h$ and so by induction is a linear combination of the h_i's.

Suppose now that $\sum_{i=0}^{n-1} \lambda_i (h_i + I) = 0 + I$ for some $\lambda_i \in \mathbb{K}$, not all 0. Then $h := \sum_{i=0}^{n-1} \lambda_i h_i \in I$. Let j be maximal with $\lambda_j \neq 0$. Then clearly $j = \deg h$ and the leading coefficient of h is λ_j. In particular $h \neq 0$.

Note that all non-zero polynomials in I have degree larger or equal to n. But this contradicts $0 \neq h \in I$ and $\deg h = j < n$. Thus (b) holds.

(c) is the special case $g = f$ and $m = 1$ of (d). So it remains to prove (d). Note that $\deg x^i g^j = i + js$. Hence by (b) $(x^i g^j + I)_{0 \leq i < s, 0 \leq j < m}$ is a basis for $R[x]/I$.

Let $y_{i,j} := x^i g^j + I$. Then

$$A(y_{i,j}) = x^{i+1} g^j + I.$$

Thus

$$A(y_{i,j}) = y_{i+1,j} \text{ for all } 0 \leq i < s-1, 0 \leq j < m.$$

As g is monic $g_s = 1$ and so $x^s = g + \sum_{i=0}^{s-1} (-g_i) x^i$.

Hence

$$A(y_{s-1,j}) = x^s g^j + I = (g^{j+1} + \sum_{i=0}^{s-1} (-g_i) x^i g^j) + I = (g^{j+1} + I) + \sum_{i=0}^{s-1} (-g_i) y_{i,j}.$$

If $j < m-1$, $g^{j+1} + I = y_{0,j+1}$ and so

$$A(y_{s-1,j}) = y_{0,j+1} - \sum_{i=0}^{s-1} (-g_i) y_{i,j}.$$

If $j = m-1$ then $g^{j+1} = g^m = f \in I$ and so

$$A(y_{s-1,m-1}) = \sum_{i=0}^{s-1}(-g_i)y_{i,m-1}$$

Thus (d) holds. □

Theorem 3.4.7 (Jordan Canonical Form)**.** *Let $\mathbb{K}$ be a field, V a non-zero finite dimensional vector space over $\mathbb{K}$ and $A \in \operatorname{End}_{\mathbb{K}}(V)$. Then there exist irreducible monic polynomials $f_1, \dots, f_t \in \mathbb{K}[x]$, positive integers $m_1, \dots m_t$ and a basis*

$$(y_{ijk})_{0\leq i<\deg f_k, 0\leq j<m_k, 1\leq k\leq t}$$

of V such that the matrix of A with respect to this basis is

$$M(f_1,m_1 \mid \dots \mid f_t,m_t) := \begin{bmatrix} M(f_1,m_1) & 0 & \dots & 0 & 0 \\ 0 & M(f_2,m_2) & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & M(f_{t-1},m_{t-1}) & 0 \\ 0 & 0 & \dots & 0 & M(f_t,m_t) \end{bmatrix}$$

Proof. View V as a $\mathbb{K}[x]$-module by $fv = f(A)(v)$ for all $f \in \mathbb{K}[x]$ and $v \in V$ (see before 3.4.3). Since $\mathbb{K}[x]$ is a PID (see 2.6.6) we can use Theorem 3.3.10. Thus V_A is the direct sum of modules V_k, $1 \leq k \leq t$ with $V_k \cong K[x]/(f_k^{m_k})$, where $f_k \in \mathbb{K}[x]$ is either 0 or prime, and $m_k \in \mathbb{Z}^+$. By 3.4.6(a) $\mathbb{K}[x]$ is infinite dimensional over $\mathbb{K}$. As V is finite dimensional, $f_k \neq 0$. So we may choose f_k to be irreducible and monic. By 3.4.6(cb), V_k has a basis y_{ijk}, $0 \leq i < \deg f_k, 0 \leq j < m_k$ so that the matrix of $A\mid_{V_k}$ with respect to this basis is $M(f_k,m_k)$. Combining the basis for V_k, $1 \leq k \leq t$, to a basis for V we see that the theorem is true. □

The matrix $M(f_1,m_1 \mid f_2,m_2 \mid \dots \mid f_t,m_t)$ from the previous theorem is called the *Jordan canonical form* of A. We should remark that our notion of the Jordan canonical form differs slightly from the notion found in most linear algebra books. It differs as we do not assume that all the roots of the minimal polynomial (see below) of A are in $\mathbb{K}$. Note that if $\mathbb{K}$ contains all the roots then $f_k = x - \lambda_k$ and $M(f_k)$ is the 1×1 matrix (λ_k) and E^{1s} is the 1×1 identity matrix. So the obtain the usual Jordan canonical form.

We remark that the pairs $(f_k,m_k), 1 \leq k \leq t$ are unique up to ordering. Indeed let f be an irreducible monic polynomial of degree s and m a positive integer. Then the number of k's with $(f_k,m_k) = (f,m)$ is $\frac{d}{s}$ where d is the dimension of the $\mathbb{K}$-space

$$\ker f^m(A)/\ker f^m(A) \cap \operatorname{Im} f(A)$$

We leave the details of this computation to the dedicated reader.

The following two polynomials are useful to compute the Jordan canonical form of A. The *minimal polynomial* m_A and the *characteristic polynomial* χ_A.

m_A is defined has the monic polynomial of minimal degree with $m_A(A) = 0$. i.e m_A is monic and (m_A) is the kernel of the homomorphism $\alpha_A : \mathbb{K}[x] \to \mathrm{End}_{\mathbb{K}}(V)$. m_A can be computed from the Jordan canonical form. For each monic irreducible polynomial let e_f be maximal so that (f, e_f) is one of the (f_k, m_k) (with $e_f = 0$ if f is not one of the f_k.)Then

$$m_A = \prod f^{e_f}$$

The characteristic polynomial is defined as

$$\chi_A = (-1)^n f_1^{m_1} f_2^{m_2} \dots f_k^{m_k}$$

where n is the dimension of V. The importance of the characteristic polynomials comes from the fact that χ_A can be computed without knowledge of f_k's. Indeed

$$\chi_A = \det(A - x\mathrm{id}_V).$$

To see this we use the Jordan canonical form of f. Note that

$$\det(A - x\mathrm{id}_V) = \prod_{k=1}^{t} \det(M(f_k, m_k) - xI)$$

and

$$\det(M(f,m) - xI) = (\det(M(f) - xI))^m.$$

Finally its is easy to verify that

$$\det(M(f) - xI) = (-1)^{\deg f} f.$$

3.5 Exact Sequences

Definition 3.5.1. *Let $(A, \leq)$ be partially ordered set and $B \subset A$.*

(a) B is called a segment of A if $c \in A$ for all $a, b \in B$ and all c with $a \leq c \leq b$.

(b) $B^- = \{a \in B \mid a < b$ for some $b \in B\}$.

Definition 3.5.2. *Let I be a segment of integers and R be a ring. An I-* sequence *of R-linear maps is a pair $\left((A_i)_{i\in I}, (f_i)_{i\in I^-}\right)$ such such that for $i \in I$, $A_i, i \in I$ is an R-module and for $i \in I^-$, $f_i : A_i \to A_{i+1}$ is an R-linear function. We denote such a sequence by*

$$\dots \xrightarrow{f_{i-2}} A_{i-2} \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots$$

Such a sequence is called exact *if*

$$\mathrm{Im}\, f_i = \ker f_{i+1}$$

for all $i \in I^{--}$.

Example 3.5.3. *(a) The sequence*

$$0 \to A \xrightarrow{f} B$$

is exact if and only if f is 1-1

(b)

$$A \xrightarrow{f} B \to 0$$

is exact if and only if f is onto.

(c) The sequence

$$0 \to A \xrightarrow{f} B \to 0$$

is exact if and only if f is an isomorphism.

(d) A sequence of the form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is called a short sequence. It is exact if and only if then f is 1-1, $\ker g = \operatorname{Im} f$ and g is onto. In this case $A \cong \operatorname{Im} f$, $C = \operatorname{Im} g$ and by the isomorphism Theorem, $B/\ker g \cong C$.. So B has a submodule which isomorphic to A and whose quotient is isomorphic to C.

Definition 3.5.4. *Given two I-sequences of R-linear maps*

$$\mathcal{A} : \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} \text{ and } \mathcal{B} : \xrightarrow{g_{i-1}} B_{i-1} \xrightarrow{g_i} B_i \xrightarrow{g_{i+1}}$$

(a) A homomorphism *$h : \mathcal{A} \to \mathcal{B}$ from $\mathcal{A}$ to $\mathcal{B}$ is a family $(h_i)_{i\in I}$ of functions such that for $i \in I$, $h_i : A_i \to B_i$ is R-linear and for all $i \in I^+$*

$$g_i \circ h_{i-1} = h_i \circ f_i$$

In other words, the diagram

$$\begin{tikzcd}
{} \arrow[r, "f_{i-1}"] & A_{i-1} \arrow[r, "f_i"] \arrow[d, "h_{i-1}"] & A_i \arrow[r, "f_{i+1}"] \arrow[d, "h_i"] & A_{i+1} \arrow[r, "f_{i+2}"] \arrow[d, "h_{i+1}"] & {} \\
{} \arrow[r, "g_{i-1}"] & B_{i-1} \arrow[r, "g_i"] & B_i \arrow[r, "f_{i+1}"] & B_{i+1} \arrow[r, "g_{i+2}"] & {}
\end{tikzcd} .$$

commutes.

(b) The homomorphism $(\mathrm{id}_{A_i})_{i\in A}$ from $\mathcal{A}$ to $\mathcal{A}$ is denoted by $\mathrm{id}_{\mathcal{A}}$.

(c) If $\alpha = (\alpha_i)_{i\in I}$ and $(\beta_i)_{i\in I}$ are family of functions, then $\beta \circ \alpha = (\beta_i \circ \alpha_i)_{i\in I}$.

Example 3.5.5. *Let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact sequence of R-modules. Then g is onto and so by the First Isomorphism Theorem $\overline{g} : B/\ker g \to C, b+\ker g \to g(b)$ is an isomorphism. Put $D := \operatorname{Im} g = \ker g$. It follows that*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "f"] & B \arrow[r, "g"] \arrow[d, equal] & C \arrow[r] \arrow[d, "\overline{g}^{-1}"] & 0 \\
0 \arrow[r] & D \arrow[r, "\mathrm{id}_D"'] & B \arrow[r, "\pi_{B,D}"'] & B/D \arrow[r] & 0
\end{tikzcd}$$

is an isomorphism of short exact sequences.

Lemma 3.5.6. *Let R be a ring and I a segment of integers. Let $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$ be I-sequences of R-linear maps.*

(a) Let $\alpha : \mathcal{A} \to \mathcal{B}$ and $\beta : \mathcal{B} \to \mathcal{C}$ be homomorphism. Then $\beta \circ \alpha : \mathcal{A} \to \mathcal{C}$ is a homomorphism.

(b) Let $\alpha = (\alpha_i)_{i\in I} : \mathcal{A} \to \mathcal{B}$ be a homomorphism. Then α is an isomorphism if and only if each $\alpha_i, i \in I$ is a R-isomorphism and if and only if each $\alpha_i, i \in I$ is a 1-1 and onto.

Proof. Readily verified. □

Theorem 3.5.7 (Short Five Lemma)**.** *Given a homomorphism of short exact sequences:*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0
\end{tikzcd}.$$

Then

(a) If α and γ are 1-1, so is β.

(b) If α and γ are onto, so is β.

(c) If α and γ are isomorphisms, so is β.

Proof. (a) Let $b \in B$ with $\beta(b) = 0$. Then also $g'(\beta(b)) = 0$ and as the diagram commutes $\gamma(g(b)) = 0$. As γ is 1-1 $g(b) = 0$. As $\ker g = \operatorname{Im} f$, $b = f(a)$ for some $a \in A$. Thus $\beta(f(a)) = 0$ and so $f'(\alpha(a)) = 0$. As f' is one 1-1, $\alpha(a) = 0$. As α is 1-1, $a = 0$. So $b = f(a) = 0$ and β is 1-1.

(c) Let $b' \in B'$. As γ and g are onto, so is $\gamma \circ g$. So there exists $b \in B$ with $g'(b') = \gamma(g(b))$. As the diagram commutes $\gamma(g(b)) = g'(\beta(b))$. Thus

$$d' := b' - \beta(b) \in \ker g'$$

As $\ker g' = \operatorname{Im} f'$, $d' = f'(a')$ for some $a' \in A'$. Since α is onto So $a' = \alpha(a))$ for some $a \in A$.

$$b' - \beta(b) = d' = f'(a') = f'(a'(\alpha(a)) = \beta(f(a)$$

and so $b' = \beta(b) + \beta(f(a)) = \beta(b + f(a))$. Thus β is onto.

(c) follows from (a) and (b). □

Definition 3.5.8. *Let V be an R-module, Then a direct summand of V is an R-submodule U of V such that $V = U \oplus W$ for some R-submodule W of V.*

Theorem 3.5.9. *Given a short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$. Then the following three statements are equivalent:*

(a) There exists a R-linear map $\gamma : C \to B$ with $g \circ \gamma = \mathrm{id}_C$.

(b) There exists a R-linear map $\eta : B \to A$ with $\eta \circ f = \mathrm{id}_A$.

(c) There exists a R-linear map $\tau : B \to A \oplus C$ such that

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, equal] & B \arrow[r, "g"] \arrow[d, "\tau"] & C \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & A \arrow[r, "\rho_1"] & A \bigoplus C \arrow[r, "\pi_2"] & C \arrow[r] & 0
\end{tikzcd}$$

is an isomorphism of short exact sequences.

(d) Im f *is a direct summand of B.*

Proof. (a) $\Longrightarrow$ (c): Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\rho_1"] \arrow[d, equal] & A \bigoplus C \arrow[r, "\pi_2"] \arrow[d, "(f,\gamma)"] & C \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$

where $(f, \gamma) : A \oplus C \to B, (a, c) \to f(a) + \gamma(c)$. We have

$$(f, \gamma)(\rho_1(a)) = (f, \gamma)(a, 0) = f(a) + \gamma(0) = f(a) = f(\mathrm{id}_A(a))$$

By exactness, $g(f(a) = 0$ and since $g \circ \gamma = \mathrm{id}_C$, $g(\gamma(c)) = c$. Thus

$$g((f, \gamma)(a, c)) = g(f(a) + \gamma(c)) = g(f(a)) + g(\gamma(c)) = 0 + c = c = \mathrm{id}_C(c) = \mathrm{id}_C(\pi_2(a, c))$$

So the diagram commutes. Since id_A and id_C are isomorphism, the Short Five Lemma 3.5.7 implies that the diagram is an isomorphism.

(c) $\Longrightarrow$ (b): Define $\eta = \pi_1 \circ \tau$. Then

$$\eta \circ f = (\pi_1 \circ \tau) \circ f = \pi_1 \circ (\tau \circ f) = \pi_1 \circ \rho_1 = \mathrm{id}_A$$

(b) $\Longrightarrow$ (d): Since $\eta \circ f = \mathrm{id}_A$, $\eta \circ f$ is a bijection. Thus $\eta\mid_{\mathrm{Im} f}$ is a bijection and 3.2.16(c) shows that $B = \mathrm{Im} f \oplus \ker \eta$.

(d) $\Longrightarrow$ (a): Suppose that $B = \mathrm{Im} f \oplus D$ for some R-submodule D of B. Then also $B = \ker g \oplus D$ and 3.2.16(c) shows that $g\mid_D \colon D \to C$ is a bijection. Put $\gamma = (g\mid_D)^{-1}$. Then $g \circ \gamma = \mathrm{id}_C$ and (a) holds. □

Definition 3.5.10. *A short exact sequence which fulfills the four equivalent conditions in 3.5.9 is called* split.

Lemma 3.5.11. *Let R be ring.*

(a) Let V be an R-module. Then there exists an R-module W with $W \cong V \oplus W$.

(b) Let $(V_i)_{i\in I}$ be a family of R-modules. Then there exists an R-module W with $W \cong V_i \oplus W$. for all $i \in I$.

(c) Let V be an R-module and U an R-submodule of V. Then there exists an R-module W such that $U \leq V \leq W$, V is a direct summand of W and $W \cong U \oplus W/U$. Moreover, if U is not a direct summand of V, U is also not a direct summand of W.

Proof. (a) Put $W = V^{\mathbb{Z}^+}$. Then $V \oplus W = V \oplus V^{\mathbb{Z}^+} \cong V^{\mathbb{N}} \cong V^{\mathbb{Z}^+} = W$.

(b) Let $i \in I$. By (a) there exists an R-module W_i with $W_i \cong V_i \oplus W_i$. Put $W = \bigoplus_{j\in I} W_j$. Then

$$V_i \oplus W = V_i \oplus \bigoplus_{j\in I} W_j \cong V_i \oplus W_i \oplus \bigoplus_{\substack{j\in J\\ j\neq i}} W_j \cong W_i \oplus \bigoplus_{\substack{j\in J\\ j\neq i}} W_j \cong \bigoplus_{j\in I} W_j = W$$

(c) According to (b) there exists a R-module W with $W \cong V \oplus W$ and $W \cong (U \oplus V/U) \oplus W$. Replacing W be an isomorphic R-module we may assume that $W = V \oplus Z$ for some submodule Z of W with $Z \cong W$. Then

$$W/U = (V \oplus D)/U \cong (V/U) \oplus D \cong V/U \oplus W$$

and so

$$U \oplus W/U \cong U \oplus V/U \oplus W \cong W$$

Suppose U is a direct summand of W and say $W = U \oplus E$. Since $U \leq V \leq W$, this gives $V = U \oplus (V \cap E)$ and so U is also a direct summand of V. □

To make the last two theorems a little more transparent we will restate them in an alternative way. First note that any short exact sequence can be viewed as pair of R modules $D \leq M$. Indeed, given $D \leq M$ we obtain a short exact sequence

$$0 \longrightarrow D \longrightarrow M \longrightarrow M/D \longrightarrow 0$$

Here $D \to M$ is the inclusion map and $M \to M/D$ is the canonical epimorphism. Conversely, every short exact sequence is isomorphic to one of this kind:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "f"] & B \arrow[r, "g"] \arrow[d, equal] & C \arrow[r] \arrow[d, "\bar{g}^{-1}"] & 0 \\
0 \arrow[r] & \operatorname{Im} f \arrow[r] & B \arrow[r] & B/\operatorname{Im} f \arrow[r] & 0
\end{tikzcd}$$

Secondly define a homomorphism $\Phi : (A \leq B) \to (A' \leq B')$ to be a homomorphism $\Phi : B \to B'$ with $\Phi(A) \leq A'$

Such a Φ corresponds to the following homomorphism of short exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\Phi_A"] & B \arrow[r] \arrow[d, "\Phi"] & B/A \arrow[r] \arrow[d, "\Phi_{B/A}"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & B'/A' \arrow[r] & 0
\end{tikzcd}$$

Here $\Phi_A : A \to A' : a \to \Phi(a)$ and $\Phi_{B/A} : B/A \to B'/A' : b + A \to \Phi(b) + A'$. Since $\Phi(A) \leq A'$ both of these maps are well defined.

Lets translate the Five Lemma into this language:

Lemma 3.5.12. *Let $\Phi : (A \leq B) \to (A' \leq B')$ be a homomorphism.*

(a) If Φ_A and $\Phi_{B/A}$ are one to one, so is Φ.

(b) If Φ_A and $\Phi_{B/A}$ are onto so is Φ.

(c) If Φ_A and $\Phi_{B/A}$ are isomorphism, so is Φ.

Proof. This follows from the five lemma, but we provide a second proof.

(a) As $\ker \Phi_{B/A} = 0$, $\ker \Phi \leq A$. So $\ker \Phi = \ker \Phi_A = 0$.

(b) As $\Phi_{B/A}$ is onto, $B' = \Phi(B) + A'$. As $\Phi(A) = A'$ we conclude $B' = \Phi(B)$.

(c) Follows from (a) and (b). □

The three conditions on split exact sequences translate into:

Lemma 3.5.13. *Given a pair of R-modules $A \leq B$. The following three conditions are equivalent.*

(a) There exists a homomorphism $\gamma : B/A \to B$ with $\bar{b} = \gamma(\bar{b}) + A$ for all $\bar{b} \in B$.

(b) There exists a homomorphism $\eta : B \to A$ with $\eta(a) = a$ for all $a \in A$.

(c) There exists a R-submodule K of B with $B = A \oplus K$.

Proof. Again this follows from 3.5.9 but we give a second proof:

(a)$\Rightarrow$ (c): Put $K = \gamma(B/A)$. Then clearly $K + A = B$. Also if $\gamma(b+A) \in A$ we get $b + A = A = 0_{B/A}$. Thus $\gamma(b + A) = 0$ and $K \cap A = 0$.

(b)⇒ (c) Put $K = \ker \eta$. The clearly $K \cap A = 0$. Also if $b \in B$. Then $\eta(b) \in A$ and $\eta(b - \eta(b)) = \eta(b) - \eta(b) = 0$. Thus $b = \eta(b) + (b - \eta(b)) \in A + B$. Thus $B = A + K$.

(c) ⇒ (a): Define $\gamma(k + A) = k$ for all $k \in K$.

(c) ⇒ (b): Define $\eta(a + k) = a$ for all $a \in A, k \in K$ □

Finally if A is a R-submodule of B we say that B splits over A if the equivalent conditions in the previous lemma hold.

3.6 Homomorphisms and Tensor Products

Definition 3.6.1. *Let R and S be rings. Then an (R, S)-bimodule is a triple $(M, *, \diamond)$ such that $(M, *)$ is an R-module, $(M, \diamond)$ is an right S-module and*

$$(r * m) \diamond s = r * (m \diamond s)$$

for all $r \in R, m \in M, s \in S$.

Example 3.6.2. *1. Let R be a ring. Then R is an (R, R)-bimodule by left and right multiplication.*

2. *Let R be a ring and M an R-module. Then M is an $(R, \mathbb{Z})$-bimodule.*

3. *Let R be a ring and M a right R-module. Then M is an $(\mathbb{Z}, R)$-bimodule.*

4. *Let R be a commutative ring and M an R-module. Note that M is a right R-module via $mr = rm$ for all $m \in M, r \in R$ and M is an (R, R)-bimodule.*

5. *Let R be a ring and M a right R-module. Then $\phi(mr) = \phi(m)r$ for all $\phi \in \mathrm{End}_R(M)$, $m \in M, r \in R$ and so M is an $(\mathrm{End}_R(M), R)$-bimodule.*

6. *Let R be a ring and M an R-module. Note that M is right R^{op}-module via $mr = rm$. Then M is an $(\mathrm{End}_R(M), R^{\mathrm{op}})$-bimodule.*

Lemma 3.6.3. *Let R and S be rings, M an abelian group, $(M, \bullet)$ a left R-module and $(M, \diamond)$ a right S-module. Then the following are equivalent:*

(a) $(M, \bullet, \diamond)$ is an (R, S)-bimodule.

(b) $\bullet_R$ is a homomorphism from R to $\mathrm{End}_S(M)$, that is for each $r \in R$ the function

$$r^{\bullet} : M \to M, m \to rm$$

is S-linear.

(c) $\diamond_S$ is a anti-homomorphism from S to to $\mathrm{End}_R(M)$, that is for each $s \in S$ the function

$$s^{\diamond} : M \to M, m \to ms$$

is R-linear.

Proof. (a) $\Longleftrightarrow$ (b) : Just observe that

$$\begin{aligned} & r^\bullet(ms) = (r^\bullet m)s \\ \Longleftrightarrow \quad & r(ms) = (rm)s \end{aligned}$$

for all $r \in R, m \in m$ and $s \in S$.

(a) $\Longrightarrow$ (c): Apply the fact that (a) and (b) are equivalent to the opposite rings. □

Lemma 3.6.4. *Let R be a ring and A, B and T be R-modules. Let $\phi : A \to B$ be R-linear.*

(a) The function

$$\phi^* : \mathrm{Hom}_R(B,T) \to \mathrm{Hom}_R(A,T),\ f \to f \circ \phi.$$

is $\mathbb{Z}$-linear.

(b) The function

$$\check{\phi} : \mathrm{Hom}_R(A,T) \to \mathrm{Hom}_R(B,T),\ f \to \phi \circ f.$$

is $\mathbb{Z}$ linear.

(c) Suppose $\psi : B \to C$ is R-linear function. Then

$$(\psi \circ \phi)\check{} = \check{\phi} \circ \check{\psi} \quad \textit{and} \quad (\phi \circ \psi)^* = \psi^* \circ \phi^*.$$

Proof. (a) Since compositions of R-linear functions are R-linear, ϕ^* is well-defined. By A.2.3(b), ϕ^* is $\mathbb{Z}$-linear.

(b) Since compositions of R-linear functions are R-linear, $\check{\phi}$ is well-defined. By A.2.3(a), $\check{\phi}$ is $\mathbb{Z}$-linear.

(c) follows from A.1.8. □

Lemma 3.6.5. *(a) Let T and S be rings, A an (T,S)-bimodule and B a right S-module Then* $\mathrm{Hom}_S(A,B)$ *is an right T-module via $(\phi t)a = \phi(ta)$ for all $\phi \in$* $\mathrm{Hom}_S(A,B)$*, $a \in A$ and $t \in T$.*

(b) Let R and S be rings, A a right S-module and B an (R,S)-bimodule. Then $\mathrm{Hom}_S(A,B)$ *is an left-R-module $(r\phi)m = r\phi(m)$ for all $\phi \in$* $\mathrm{Hom}_S(A,B)$*, $m \in M$ and $r \in R$.*

(c) Let R, S and T be rings, A an (T,S)-bimodule and B an (R,T)-module. Then $\mathrm{Hom}_S(A,B)$ *is an (R,T)-bimodule via the actions in (a)nd (b).*

Proof. Put $\tilde{A} = \mathrm{Hom}_S(A,B)$

(a) We claim that

$$\sigma : \mathrm{End}_S(A) \to \mathrm{End}_{\mathbb{Z}}(\tilde{A}), \alpha \to \alpha^* = (\phi \to \phi \circ \alpha)$$

is well defined ring anti-homomorphism. Indeed 3.6.4(a) shows that σ is well-defined. 3.6.4(b) implies that σ is an additive homomorphism and 3.6.4(c) shows that σ is a multiplicative antihomomoprhism.

Let $\bullet : T \times A \to A$ be the ring action of T on A. By 3.6.3, $\bullet_T$ is a ring homomorphism from T to $\mathrm{End}_S(A)$. Thus we obtain an anti ring-homomorphism

$$\sigma \circ \bullet_T : T \to \mathrm{End}_{\mathbb{Z}}(\tilde{A}), t \to (t^{\bullet})^*$$

Let $t \in T$ and $\phi \in \tilde{A}$ and $a \in A$. Note that $(\phi t)a = \phi(tm) = \phi(t^{\bullet}a)$ and so

$$\phi t = \phi \circ t^{\bullet} = (t^{\bullet})^* \phi = \big((\sigma \circ \bullet_T)t\big)\phi$$

So action of T on $\tilde{A}$ given in (a) is exactly the right ring action associated to the anti homomorphism $\sigma \circ \diamond_T$.

(b) We claim that

$$\rho : \mathrm{End}_S(A) \to \mathrm{End}_{\mathbb{Z}}(\tilde{A}), \alpha \to \check{\alpha} = (\phi \to \alpha \circ \phi)$$

is well defined ring homomorphism. Indeed 3.6.4(b) shows that ρ is well-defined. 3.6.4(a) implies that ρ is an additive homomorphism and 3.6.4(c) shows that ρ is a multiplicative homomorphism.

Let $\square : R \times A \to A$ be the ring action of R on A. By 3.6.3, $\square_R$ is a ring homomorphism from R to $\mathrm{End}_S(A)$.

Thus we obtain a ring-homomorphism

$$\rho \circ \square_R : R \to \mathrm{End}_{\mathbb{Z}}(\tilde{A}), r \to (r^{\square})\check{}$$

Let $r \in R$ and $\phi \in \tilde{A}$ and $a \in A$. Note that $(r\phi)a = r(\phi a) = r^{\square}(\phi a)$ and so

$$r\phi = r^{\square} \circ \phi = (r^{\square})\check{}\,\phi = \big((\rho \circ \square_T)r\big)\phi$$

So action of R on $\tilde{A}$ given in (b) is exactly the ring action associated to the ring-homomorphism $\rho \circ \square_T$.

(c) Let $r \in R, \phi \in \tilde{A}$ and $t \in T$. Then

$$(r\phi)t = (r^{\square} \circ \phi) \circ t^{\bullet} = r^{\square} \circ (\phi \circ t^{\bullet}) = r(\phi t)$$

$\square$

Corollary 3.6.6. *Let R be a ring and B an abelian group.*

(a) Let A a right R-module. Then $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ *is an left R-module via* $(r\phi)a = \phi(ar)$ *for all* $r \in R, a \in A$, *and* $\phi \in \mathrm{Hom}_{\mathbb{Z}}(A, B)$.

(b) Suppose B is left R-module. Then $\mathrm{Hom}_R(R, B)$ *is an R-module via* $(r\phi)a = \phi(ar)$ *for all* $a, r \in R$ *and* $\phi \in \mathrm{Hom}_R(R, B)$.

(c) $\mathrm{Hom}_{\mathbb{Z}}(R, B)$ *is an R-module via* $(r\phi)a = \phi(ar)$ *for all* $a, r \in R$ *and* $\phi \in \mathrm{Hom}_R(R, B)$.

Proof. (a) Note that A is a $(\mathbb{Z}, R)$-bimodule and B is a left $\mathbb{Z}$-module. So (a) follows from 3.6.5(a) with left and right modules interchanged.

(b) Note that R is an (R,R)-bimodule. So (a) follows from 3.6.5(a) with left and right modules interchanged.

(c) Since R is a right R-module, this is the special case $A = R$ in (a). □

Definition 3.6.7. *Let $f : A \times B \to D$ be a function.*

(a) Suppose R is a ring and A and D are left R-module. Then f is called R-linear in the first coordinate if for all $b \in B$, $f_b : A \to D, a \to f(a,b)$ is R-linear.

(b) Suppose T is a ring and B and D are right R-module. Then f is called T-linear in the second coordinate if for all $a \in A$, $f_a : B \to A, b \to f(a,b)$ is R-linear.

(c) Suppose R and S are ring, A is left R-module, B is right T-module and D is a (R,T)-bimodule. Then f is called (R,S)-bilinear if f is R-linear in the first coordinate and S-linear in the second coordinate. In the special case $R = S$ we will use the term R-bilinear for (R,R)-bilinear.

(d) Suppose R, S,T are ring A is (R,S)-bimodule, B is a (S,T)-bimodule and D is an (R,T)-bimodule. Then f is called (R,S,T)-linear if f is (R,S)-bilinear and

$$f(as,b) = f(a,sb)$$

for all $a \in A, s \in S$ and $b \in B$.

(e) Suppose S is a ring, A is left S=module, B is a right S-module and D is an abelian group. Then f is called S-balanced if f is $(\mathbb{Z}, S, \mathbb{Z})$-linear.

Definition 3.6.8. *Let $f : A \times B \to C$ be an (R,S,T)-linear function. Then (C,f) is called an (R,S)-tensor product of A and B over R if for all all (R,S,T)-linear function $g : A \times B \to D$ there exists a unique (R,T)-linear function*

$$\overline{g} : C \to D \text{ with } g = \overline{g} \circ f.$$

$$\begin{tikzcd}
A \times B \arrow[rr, "f"] \arrow[dr, "g"'] & & C \arrow[dl, "\exists!\,\overline{g}"] \\
& D &
\end{tikzcd}$$

If $R = T = \mathbb{Z}$ we just say tensor product for $(\mathbb{Z},\mathbb{Z})$-tensor product.

Notation 3.6.9. *Let R be a ring, A a right R-module and B an R-module. Let (C,f) be tensor product of A and B over $\mathbb{R}$. Then we write $A \otimes_R B$ for C and $\otimes$ for f. Abusing notation, each of $(A \otimes_R B, \otimes)$, $A \otimes_R B$ and $\otimes$ are called the tensor product of A and B over R.*

Example 3.6.10. 1. Let R be a ring. Compute $R \otimes_R R$.

We claim the multiplication that the multiplication

$$\cdot : \; R \times R \to R, \; (a,b) \to ab$$

is a tensor product for R and R over R. Since $\cdot$ is distributive, $\cdot$ is $\mathbb{Z}$-linear. Since $\cdot$ is associative, $\cdot$ is R-balanced.

Let D be an abelian group, $g : R \times R \to D$ an R-balanced function and $h : R \to D$ a $\mathbb{Z}$-linear function. Then $g = h \circ \cdot$ if and only if

$$h(ab) = g(a,b)$$

for all $a, b \in R$. Choosing $a = 1$ we see that $h(b) = g(1,b)$ and so h is unique. Define $h(b) = g(1,b)$. Using that g is R-balanced we compute

$$h(ab) = g(1,ab) = g(1a,b) = g(a,b)$$

and so $\cdot$ is indeed an tensor product of R and R over R. Hence $R \otimes RR = R$.

2. Let R be a ring and M an R-module. Compute $R \otimes_R M$.

We claim the ring action of R on M

$$* : R \times M \to M, (a,m) \to am$$

is a tensor product for R and M over R. It follows immediately from the definition of an ring action that $*$ is R-balanced. So $R \otimes_R M = R$.

Let D be an abelian group, $g : R \times M \to D$ an R-balanced function and $h : M \to D$ a $\mathbb{Z}$-linear function. Then $g = h \circ *$ if and only if

$$h(am) = g(a,m)$$

for all $a \in R$ and $m \in M$. Choosing $a = 1$ we see that $h(m) = h(1m) = g(1,m)$ and so h is unique. Define $h(m) = g(1,m)$ and using that g is R-balanced we compute

$$h(am) = g(1,am) = g(1a,m) = g(a,m)$$

and so $*$ is indeed an tensor product of R and M over R.

3. Let R be a ring and M an right R-module. Compute $M \otimes_R R$.

Again the ring action $* : M \times R \to M, (m,a) \to am$ is tensor product. So $M \otimes_R R = M$.

Theorem 3.6.11. *Let R be a ring, A be a right and B a left R-module. Then there exits a tensor product of A and B over R.*

Proof. Let $\mathcal{R}$ be the set consisting of the following relations on $A \times B$

$$\begin{aligned}(a,b)+(a',b) &\equiv (a+a',b) \quad a,a' \in A, b \in B\\ (a,b)+(a,b') &\equiv (a,b+b') \quad a \in A, b,b' \in B\end{aligned}$$

and

$$(ar,b) \equiv (a,rb) \qquad a \in A, b \in B, r \in R$$

Let D be an abelian group and $g : A \times B \to D$ a function. Note that g is R-balanced if and only if $\big(g(a,b)\big)_{(a,b)\in A\times B}$ fulfills the relations $\mathcal{R}$.

Let $\Big(X, \big(x(a,b)\big)_{(a,b)\in A\times B}\Big)$ be an abelian group with generators $A \times B$ and relations $\mathcal{R}$. We claim that

$$\otimes : A \times B \to X, \ (a,b) \to x(a,b)$$

is a tensor product of A and B over R.

Since $\big(x(a,b)\big)_{(a,b)\in A\times B}$ fulfills the relation, $\otimes$ is R-balanced. Let D be an abelian group and $g : A \times B \to D$ be an R-balanced map. Then $\big(g(a,b))_{(a,b)\in A\times B}\big)$ fulfills the relations $\mathcal{R}$ and so by the definition of a group with generators and relations, there exists a unique homomorphism (of abelian groups) $\overline{g} : X \to D$ with $\overline{g}(x(a,b)) = g(a,b)$ for all $(a,b) \in A \times B$. So $(X, \otimes)$ is indeed a tensor product of A and B over R. □

Lemma 3.6.12. *Let R, S, T be rings.*

(a) Suppose A is (R,S)-bimodule and B an S-module. Then there exists a unique ring action of R on $A \otimes_S B$ with

$$r(a \otimes b) = ra \otimes b$$

for all $a, A, b \in B$.

(b) Suppose A is a right S-module and B is (S,T)-bimodule. Then there exists a unique right ring action of T on $A \otimes_S B$ with

$$(a \otimes b)t = a \otimes bt$$

for all $a, A, b \in B$ and $t \in T$.

(c) Suppose A is (R,S)-bimodule and B is (S,T)-bimodule. Then $A \otimes_S B$ is an (R,T)-bimodule via the actions in (a) and (b). Moreover $\otimes$ is a (R,T)-tensor product for A and B over S.

Proof. (a) For $r \in R$ define

$$\phi_r : A \times B \to A \otimes B, (a,b) \to ra \otimes b$$

We claim that ϕ_r is R-balanced. Indeed since $a \to ra$-$\mathbb{Z}$-linear and $\otimes$ is $\mathbb{Z}$-linear in the first coordinate, ϕ_r is $\mathbb{Z}$-linear in the first coordinate. Since $\otimes$ is $\mathbb{Z}$-linear in second coordinate, so is ϕ_r. Also since A is (R, S)-bimodule and $\otimes$ is S-balanced:

$$\phi_r(as, b) = r(as) \otimes b = (ra)s \otimes b = ra \otimes sb = \phi_r(a, sb)$$

for all $a \in A, s \in S, b \in B$. So ϕ_r is S-balanced and so by the definition of a tensor product there exists a unique $\mathbb{Z}$-linear function:

$$r^* : A \otimes_S B \to A \otimes B$$

with $\phi_r = \Phi_r \circ \otimes$, that is $\Phi_r(a \otimes b) = ra \otimes b$.

Define

$$* : R \times \big(A \otimes B\big) \;\to\; A \otimes B, (r, u) \to r^*(u)$$

Since r^* is $\mathbb{Z}$-linear, $*$ is $\mathbb{Z}$-linear in the second coordinate.

$$(u^* + v^*)(a \otimes b) = ua \otimes b + va \otimes b = (ua + va) \otimes b = (u + v) \otimes b$$

and since $u^* + v^*$ is $\mathbb{Z}$-linear the definition of $(u+v)^*$ implies $u^* + v^* = (u+v)^*$.

Also

$$(u^* \circ v^*)(a \otimes b) = u^*(va \otimes b) = u(va) \otimes b = (uv)a \otimes b$$

and since $u^* \circ v^*$ is $\mathbb{Z}$-linear the definition of $(uv)^*$ implies $u^* \circ v^* = (uv)^*$. Thus $*$ is a ring action of R on $A \otimes_S B$.

(b) Apply (a) to the opposite rings.

(c) Let $r \in R, t \in T$. Then

$$\big(r(a \otimes b)\big)t = (ra \otimes b)t = ra \otimes bt = r(a \otimes bt) = r\big(a \otimes b\big)t$$

for all $a \in A$ and $b \in B$. So the definition of the tensor products show $(rm)t = r(mt)$ for all $m \in A \otimes_R B$. Thus $A \otimes_R B$ is an (R, T)-bimodule. By definition of a tensor product, $\otimes$ is S-balance and in particular, $\mathbb{Z}$-bilinear. The definition of the action of R and T on $A \times_R B$ shows that $\otimes$ is R-linear in the first coordinate and T-linear in the second coordinate. Thus $\otimes$ is (R, S, T)-linear.

To show that $\otimes$ is an (R, T)-tensor product of A and B over S, let D be an (R, T)-bimodule and $g : A \times B \to D$ be an (R, S, T)-linear function. By definition of tensor product there exist a unique $\mathbb{Z}$-linear function $\overline{g} : A \otimes B \to D$ with $g = \overline{g} \circ \otimes$ and it remains to verify that $\overline{g}$ is (R, T)-linear.

Let $r \in R$ and $r^\square : D \to D, d \to rd$. Then both $\overline{g} \circ r^*$ and $r^\square$ are $\mathbb{Z}$-linear. Also

$$(\overline{g} \circ r^*)(a \otimes b) = g(ra, b) = r\big(g(a, b)\big) = (r^\square \circ \overline{g})(a \otimes b)$$

Thus the definition of the tensor product shows that $\overline{g} \circ r^* = r^\square \circ \overline{g}$. Thus $\overline{g}$ is R-linear. By symmetry $\overline{g}$ is T-linear and so $\overline{g}$ is indeed (R, T)-linear. □

Lemma 3.6.13. *Let R, S ,T be rings, A an (R, S)-bimodule, B an (S, T)-bimodule and D an (R, T)-bimodule. Let $f : A \times B \to D$ be a function. Let f_A and f_B be the corresponding functions on A and B (see 1.7.5, so for $a \in A$, $f_a = f_A(a)$ is the function $B \to C, b \to f(a, b)$.) Then the following statements are equivalent.*

(a) f is (R, S, T)-linear.

(b) f_A is a (R, S)-linear functions from A to $\mathrm{Hom}_T(B, D)$

(c) f_B is a (S, T)-linear function from B to $\mathrm{Hom}_R(A, D)$.

Proof. f is T-linear in the second coordinate if and only if f_a is T-linear for each $a \in A$ and so if and only if f_A is a function from A to $\mathrm{Hom}_T(B, D)$.

We have

$$\begin{array}{llll} & f(ra, b) = r\big(f(a, b)\big) & & \text{for all } a \in A, b \in B, r \in R \\ \Longleftrightarrow & f_{ra}\, b & = r(f_a b) & \text{for all } a \in A, b \in B, r \in R \\ \Longleftrightarrow & f_{ra} b & = (r f_a) b & \text{for all } a \in A, b \in B, r \in R \\ \Longleftrightarrow & f_{ra} & = r f_a & \text{for all } a \in Ar \in T \\ \Longleftrightarrow & f_A(ra) & = r(f_A a) & \text{for all } a \in A, r \in R \end{array}$$

So f is R-linear in the first coordinate if and only if f_A is R-linear.

$$\begin{array}{llll} & f(as, b) & = f(a, sb) & \text{for all } a \in A, b \in B, s \in S \\ \Longleftrightarrow & \big(f_A(as)\big)b & = (f_A a)(sb) & \text{for all } a \in A, b \in B, s \in S \\ \Longleftrightarrow & \big(f_A(as)\big)b & = \big((f_A a)s\big)b & \text{for all } a \in A, b \in B, s \in S \\ \Longleftrightarrow & f_A(ar) & = (f_A a)r & \text{for all } a \in A, s \in S \end{array}$$

So f is S-balanced if and only if f_A is S-linear. Hence (a) and (b) are equivalent. By symmetry (a) and (c) are equivalent. □

Theorem 3.6.14. *Let R, S ,T be rings. A an (R, S)-bimodule, B an (S, T)-bimodule and D an (R, T)-bimodule. Let $\otimes : A \times B \to A \otimes_S B$ be the tensor product of A and B over R. Then of the following maps are $\mathbb{Z}$-isomorphisms:*

(a) $\otimes^* : \mathrm{Hom}_{R,T}(A \otimes_S B, D) \to \mathrm{Hom}_{R,S,T}(A \times B, D), f \to f \circ \otimes$.

(b) $\mathrm{Hom}_{R,S,T}(A \times B, D) \to \mathrm{Hom}_{R,S}\big(A, \mathrm{Hom}_T(B, C)\big),\ f \to f_A$.

(c) $\mathrm{Hom}_{R,S,T}(A \times B, D) \to \mathrm{Hom}_{S,T}\big(B, \mathrm{Hom}_R(A, C)\big),\ f \to f_B$.

Proof. Note first that by 3.6.12 $\otimes$ is an (R,T)-tensor product for A and B over S.(a) Let $f \in \mathrm{Hom}_{R,T}(A \otimes_S B, D)$. Since $\otimes$ is (R,S,T)-linear and f is (R,T)-linear. $f \circ \otimes$ is $(R,S,T($ Hence $\otimes^*$ is well defined.

By definition of (R,T)- tensor product $\otimes^*$ is 1-1 and onto. By A.2.3(b), $\otimes^*$ is $\mathbb{Z}$-linear. So (a) holds.

(b) By 3.6.13 the function is a bijection and by A.2.5 its $\mathbb{Z}$-linear. Thus (b) holds. By symmetry also (c) holds. □

Lemma 3.6.15. *Let R be a ring and M an R-module. Then the function*

$$\mathrm{Ev}_1 : \mathrm{Hom}_R(R,M) \to M,\ \phi \to \phi 1.$$

is a R-isomorphism with inverse

$$\Gamma :\ M \to \mathrm{Hom}_R(R,M), m \to (r \to rm)$$

Proof. By A.2.8 Ev_1 is $\mathbb{Z}$-linear. Let $\phi \in \mathrm{Hom}_R(R,M))$ and $r \in R$. Then

$$\mathrm{Ev}_1(r\phi) = (r\phi)1 = \phi(1r) = \phi(r1) = r(\phi 1) = r(\mathrm{Ev}_1\phi)$$

and so Ev_1 is R-linear.

By 3.1.24(b), $r \to rm$ is R-linear. Hence Γ is well-defined.

To show that Ev_1 and Γ are inverse to each other we compute:

$$\mathrm{Ev}_1(\Gamma m) = (\Gamma m)1 = 1m = m$$

and

$$\big(\Gamma(\mathrm{Ev}_1\phi)\big)r = r(\mathrm{Ev}_1\phi) = r(\phi 1) = \phi(r1) = \phi r$$

□

Definition 3.6.16. *Let R and S be rings and A and B (R,S)-bimodule. A function $f : A \to B$ is called (R,S)-linear if it is R-linear and S-linear.*

Lemma 3.6.17. *Let R, S and T be rings. $\alpha : A \to A'$ an (R,S)-linear function and $\beta : B \to B'$ and (S,T)-linear map. Then there exists a unique (R,T)-linear function*

$$\alpha \otimes \beta : A \otimes_S B \to A' \otimes_S B',\ \textit{with}\ a \otimes b \to \alpha a \otimes \beta b$$

for all $a \in A, b \in B$.

Proof. Consider the function $\Phi : A \times B \to A' \times B'$, $(a,b) \to \alpha a \otimes \beta b$. Since α is R linear and $\otimes$ is R-linear in the first coordinate, Φ is R-linear in the first coordinate. By symmetry, Φ is T-linear in the second coordinate. Let $a \in A, b \in B$ and $s \in S$. Then

$$\Phi(as,b) = \alpha(as) \otimes \beta b = (\alpha a)s \otimes \beta b = \alpha a \otimes s\beta b = \alpha a \otimes \beta(sb) = \Phi(a, sb)$$

and so Φ is also S-balanced. Since $A \otimes_S B$ is an (R,T)-tensor product over S, the lemma follows from the definition of an (R,T)-tensor product. □

Lemma 3.6.18. *Let (R,S,T) be rings and suppose that S is an (R,S)-bimodule with S acting by right multiplication. Let $\alpha : B \to B'$ be an (S,T)-linear function.*

(a) B is an (R,T) module via $rb = (r1_S)b$ for all $r \in R$, $b \in B$.

(b) α is (R,T)-bilinear.

Proof. (a) By 3.6.10(2)

$$\otimes : S \times B \to B, (s,b) \to sb$$

is the tensor product of S and B over S. Thus by 3.6.12 B is an (R,T)-bimodule via

$$rb = r(1_S \otimes b) = (r1_S) \otimes b = (r1_S)b.$$

(b) Note that id_S is (R,S)-linear. So by 3.6.17 $\mathrm{id}_S \otimes \alpha$ is (R,T)-linear. We have

$$(\mathrm{id}_S \otimes \alpha)a = (\mathrm{id}_S \otimes \alpha)(1 \otimes a) = 1 \otimes \alpha a = \alpha a$$

So $\alpha = \mathrm{id}_S \otimes \alpha$ and (b) holds. □

Lemma 3.6.19. *Let R, S and T be rings. Suppose S is an (R,S)-bimodule with S acting by right multiplication. Let B be an (S,T)-bimodule and D an (R,T)-bimodule. For an (R,T)-bimodule E define*

$$\hat{E} = \mathrm{Hom}_S(S,E) \quad \textit{and} \quad \mathrm{Ev}_1 : \hat{E} \to E,\ \delta \to \delta 1$$

(a) $\hat{D}$ is an (S,T)-bimodule.

(b) The map

$$\check{\mathrm{Ev}}_1 : \mathrm{Hom}_{S,T}(B,\hat{D}) \to \mathrm{Hom}_{R,T}(B,D), \quad \phi \to \mathrm{Ev}_1 \circ \phi$$

is well-defined $\mathbb{Z}$-isomorphism.

(c) Let $\beta : D \to E$ be (R,T)-linear. Then the following diagram is commutative:

$$\begin{tikzcd}
\mathrm{Hom}_{S,T}(B,\hat{D}) \arrow[r, "\check{\mathrm{Ev}}_1"] \arrow[d, "\check{\check{\beta}}"] & \mathrm{Hom}_{R,T}(B,D) \arrow[d, "\check{\beta}"] \\
\mathrm{Hom}_{S,T}(B,\hat{E}) \arrow[r, "\check{\mathrm{Ev}}_1"] & \mathrm{Hom}_{R,T}(B,E))
\end{tikzcd}$$

(d) Let $\eta : B \to C$ be (S,T)-linear. Then the following diagram is commutative:

$$\begin{tikzcd}
\mathrm{Hom}_{S,T}(B,\hat{D}) \arrow[r, "\check{\mathrm{Ev}}_1"] & \mathrm{Hom}_{R,T}(B,D) \\
\mathrm{Hom}_{S,T}(C,\hat{D}) \arrow[r, "\check{\mathrm{Ev}}_1"] \arrow[u, "\eta^*"] & \mathrm{Hom}_{R,T}(C,D) \arrow[u, "\eta^*"]
\end{tikzcd}$$

Proof. (a) follows from 3.6.12(c).

(b) By 3.6.14 applies with $A = S$ and using that $S \otimes_S B = B$ we have $\mathbb{Z}$-isomorphism

$$\begin{tikzcd}
\mathrm{Hom}_{R,T}(B,D) = \mathrm{Hom}_{R,T}(S \otimes_S B, D) \arrow[r] & \mathrm{Hom}_{R,S,T}(S \times B, D) \arrow[r] & \mathrm{Hom}_{S,T}(B,\hat{D}) \\
f \arrow[r] & f \circ \otimes \arrow[r] & (f \circ \otimes)_B
\end{tikzcd}$$

Let $f \in \mathrm{Hom}_{R,T}(B,D)$ and $b \in B$. Then

$$\Big(\mathrm{E\check{v}}_1\big((f \circ \otimes)_B\big)\Big)b = \big(\mathrm{Ev}_1 \circ (f \circ \otimes)_B\big)b = \mathrm{Ev}_1\big(f \circ \otimes)_B b\big) = (f \circ \otimes)(b,1) = f(b \otimes 1) = f(b)$$

So $\mathrm{E\check{v}}_1$ is inverse of isomorphism $f \to (f \circ \otimes)_B$.

(c) Using A.1.8 and A.1.9

$$\mathrm{E\check{v}}_1 \circ \check{\check{\beta}} = (\mathrm{Ev}_1 \circ \check{\beta})\check{} = (\beta \circ \mathrm{Ev}_1)\check{} = \check{\beta} \circ \mathrm{E\check{v}}_1$$

(d) By A.1.8 $\beta^* \circ \mathrm{E\check{v}}_1 = \mathrm{E\check{v}}_1 \circ \beta^*$. □

Proposition 3.6.20. *Let R be ring and D a fixed left R-module. For a left R-module E define $E^\dagger = \mathrm{Hom}_R(E,D)$.*

Let S be a ring, A be an (R,S)-bimodule, and B a left S-module. Then

$$\Xi : (A \otimes_S B)^\dagger \to \mathrm{Hom}_S(A, B^\dagger), f \to (f \circ \otimes)_A$$

is a $\mathbb{Z}$-isomorphism with inverse

$$\Theta : \mathrm{Hom}_S(A, B^\dagger) \to (A \otimes_S B)^\dagger, \alpha \to \big(a \otimes b \to (\alpha a)b\big)$$

Proof. 3.6.14 applied with $T = \mathbb{Z}$, Ξ is a $\mathbb{Z}$-isomorphism. Let $\alpha \in \mathrm{Hom}_S(A, B^\dagger)$. Then $\alpha = \Xi f = (f \circ \otimes)_A$ for some $f \in (A \otimes_S B)^\dagger$. Then

$$f(a \otimes b) = (f \circ \otimes)(a,b) = \big((f \circ \otimes)_A\, a\big)b = (\alpha a)b = (\Theta\alpha)(a \otimes b)$$

Hence $\Theta(\alpha) = f$ and Θ is the inverse of Ξ. □

3.7 Projective and injective modules

In this section all rings are assumed to have an identity and all R-modules are assumed to be unitary.

Notation 3.7.1. *(a) $\phi : A \twoheadrightarrow B$ means that ϕ is an onto function from A to B.*

(b) $\phi : A \rightarrowtail B$ means that ϕ is an 1-1 function from A to B.

Definition 3.7.2. *Let P be a module over the ring R. We say that P is projective provided for all R-linear function $\beta : P \to B$ and all onto R-linear functions $\alpha : A \twoheadrightarrow B$ there exists a R-linear function $\gamma : P \to B$ with $\beta = \alpha \circ \gamma$.*

$$\begin{tikzcd}
P \arrow[dr, tail, "\beta"'] & & A \arrow[dl, two heads, "\alpha"] & \Longrightarrow & P \arrow[rr, "\gamma"] \arrow[dr, "\beta"'] & & A \arrow[dl, two heads, "\alpha"] \\
& B & & & & B &
\end{tikzcd}$$

Lemma 3.7.3. *Any free module is projective.*

Proof. Let V be a free module with basis $(v_i)_{i\in I}$. Given $\alpha : A \twoheadrightarrow B$ and $\beta : V \to B$. Let $i \in I$. Since α is onto, $\beta(v_i) = \alpha(a_i)$ for some $a_i \in A$. By the definition of a free module there exists $\gamma : V \to A$ with $\gamma(v_i) = a_i$. Then

$$\alpha(\gamma(v_i) = \alpha(a_i) = \beta(v_i).$$

So by the uniqueness assertion in the definition of a free module $\alpha \circ \gamma = \beta$. □

Lemma 3.7.4. *(a) Every module is isomorphic to a quotient of a free module.*

(b) Every module is isomorphic to a quotient of projective module.

Proof. (a) Let R be a ring and M be an R-module. Let V be a free R-module with basis $(v_m)_{m\in M}$. Then there exists an R-linear map $g : V \to M$ with $g(v_m) = m$ for all $m \in M$. Then g is clearly onto. (b) Since free modules are projective, this follows from (a). □

Lemma 3.7.5. *Any direct summand of a projective module is projective.*

Proof. Let P be projective and $P = P_1 \bigoplus P_2$ for some submodules P_i of P. We need to show that P_1 is projective. Given aR-linear maps $\alpha : A \twoheadrightarrow B$ and $\beta : P_1 \to B$. Since P is projective there exists an R-linear map $\tilde{\gamma} : P \to A$ with

$$\alpha \circ \tilde{\gamma} = \beta \circ \pi_1$$

Put $\gamma = \tilde{\gamma} \circ \rho_1$. Then

$$\alpha \circ \gamma = \alpha \circ \tilde{\gamma} \circ \rho_1 = \beta \circ \pi_1 \circ \rho_1 = \beta$$

$$\begin{tikzcd}
& P \arrow[dl, two heads, shift right, "\pi_1"'] \arrow[dr, "\tilde{\gamma}"] \arrow[dd, "\beta \circ \pi_1"] & \\
P_1 \arrow[ur, tail, shift right, "\rho_1"'] \arrow[rr, "\tilde{\gamma} \circ \rho_1"] \arrow[dr, "\beta"'] & & A \arrow[dl, two heads, "\alpha"] \\
& B &
\end{tikzcd}$$

□

Theorem 3.7.6. *Let P be a module over the ring R. Then the following are equivalent:*

(a) P is projective.

(b) Every short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ splits.

(c) P is (isomorphic to) a direct summand of a free module.

Proof. (a) $\Longrightarrow$ (b): Since P is projective we have

$$\begin{tikzcd} P \arrow[dr, "\mathrm{id}_P"'] & & B \arrow[dl, two heads, "g"] \\ & P & \end{tikzcd} \quad \Longrightarrow \quad \begin{tikzcd} P \arrow[rr, "\gamma"] \arrow[dr, "\mathrm{id}_P"'] & & A \arrow[dl, two heads, "g"] \\ & B & \end{tikzcd}$$

So $g \circ \gamma = \mathrm{id}_P$ and the exact sequence is split by 3.5.9.

(b) $\Longrightarrow$ (c): By 3.7.4 the exists a free module F and onto R-linear map $g : F \to P$. This yields the a short exact sequence:

$$0 \to \ker g \to F \overset{g}{\to} P \to 0$$

By assumption the sequence split and so by 3.5.9 $F \cong \ker g \oplus P$. Thus P is isomorphic to a direct summand of a free module. Any module isomorphic to free module is free and so P is also a direct summand of a free module.

(c) $\Longrightarrow$ (a): Suppose P is a direct summand of a free module F. By 3.7.3 F is projective. So P is the direct summand of and projective module and so by 3.7.5 also F is projective. □

Lemma 3.7.7. *Let R be ring such that every left ideal in R is a free R-module. Let M be an R-module. Then M is a projective if and only if M is free.*

Proof. Suppose first that M is projective. Then by 3.7.6 M is a direct summand of a free R-module F. By 3.2.5, since all left ideal in R are free, all submodules of the free module F are free. Thus M is free.

Conversely, if M is a free R-module, then by 3.7.3 M is free. □

Corollary 3.7.8. *Direct sums of projective modules are projective.*

Proof. Let $(P_i)_{i\in I}$ be a family of projective R-modules. By 3.7.6 for each $i \in I$ there exists a free R-module F_i and an R-submodule Q_i of F_i with $F_i = P_i \oplus Q_i$. Then

$$\bigoplus_{i\in I} F_i \cong \bigoplus_{i\in I} M_i \oplus \bigoplus_{i\in I} Q_i$$

Note that $\bigoplus_{i\in I} F_i$ is a free R-module. So $\bigoplus_{i\in I} M_i$ is a direct summand of a free module and so projective. □

Next we will dualize the concept of projective modules.

Definition 3.7.9. *Let J be a module over the ring R. We say that J is injective provided for all R-linear function $\beta : B \to J$ and all 1-1 R-linear functions $\alpha : B \rightarrowtail A$ there exists a R-linear function $\gamma : A \to J$ with $\beta = \gamma \circ \alpha$.*

$$\begin{tikzcd}
J & & A & & J & & A \arrow[ll, "\gamma"'] \\
& B \arrow[ul, "\beta"] \arrow[ur, tail, "\alpha"'] & & \Longrightarrow & & B \arrow[ul, "\beta"] \arrow[ur, tail, "\alpha"'] &
\end{tikzcd}$$

Above we showed that free modules are projective and so every module is isomorphic to a quotient of a projective module. To dualize this our first goal is to find a class of injective R-modules that every R-module is isomorphic to submodule of member of that class the class. We do this into step steps: First we find injective modules for $R = \mathbb{Z}$. Then we use those find injective modules for an arbitrary ring (with identity).

To get started we prove the following lemma, which makes it easier to verify that a given module is injective.

Lemma 3.7.10. *Let J be a module over the ring R. Then J is injective if and only if for left ideal I of R and all R-linear functions $\beta : I \to J$ there exists an R-linear function $\gamma : R \to J$ with $\gamma\mid_I = \beta$.*

$$\begin{tikzcd}
J & & R & & J & & R \arrow[ll, "\gamma"'] \\
& I \arrow[ul, "\beta"] \arrow[ur, tail, "\mathrm{id}_I"'] & & \Longrightarrow & & I \arrow[ul, "\beta"] \arrow[ur, tail, "\mathrm{id}_I"'] &
\end{tikzcd}$$

Proof. Given R-linear maps $\alpha : B \rightarrowtail A$ and $\beta : B \to J$, we need to find an R-linear map $\gamma : B \to J$ with $\beta = \gamma \circ \alpha$. Without loss, $B \leq A$ and $\alpha = \mathrm{id}_B$. Then $\beta = \gamma \circ \alpha$ just means $\gamma\mid_B = \beta$.

So we are trying to extend β to A to a linear map $\gamma : B \to J$. We will use Zorn's lemma find a maximal extension of β. For this let $\mathcal{M}$ be the set of all R-linear maps $D \to J$, where D an R-submodule of A with $B \leq D$ and $\delta\mid_B = \beta$. Order $\mathcal{M}$ by $(\delta_1 : D_1 \to J) \leq (\delta_2 : D_2 \to J)$ if

$$D_1 \subseteq D_2 \quad \text{and} \quad \delta_2\mid_{D_1} = \delta_1$$

We claim that every chain $\{\delta_k : D_k \to J \mid k \in K\}$ in $\mathcal{M}$ has an upper bound. Let $D = \bigcup_{k \in K} D_k$ and define $\delta : D \to J$ by $\delta(d) = \delta_k(d)$ if $d \in D_i$ for some $k \in K$. It is easy to verify that δ is well defined, $\delta \in \mathcal{M}$ and δ is an upper bound for $\{\delta_k : D_k \to J \mid k \in K\}$.

Hence by Zorn's lemma, $\mathcal{M}$ has a maximal element $\delta : D \to J$. [1]

[1] We did note not use our assumptions on J yet. Maximal extensions always exists.

Let $a \in A$. We will show that $a \in D$. For this consider the R-linear map:

$$\mu : D \oplus R \to A, \quad (d, r) \to d + ra.$$

Let $I = \pi_2(\ker mu)$ be the projection of $\ker \mu$ onto R. Since $\ker \mu$ is am R-submodule of $D \oplus R$, I is a R-submodule of R, that is I is left ideal in R. We claim that

$$\ker \mu = \{(-ia, i) \mid i \in I\}.$$

Indeed, let $(d, r) \in \ker \mu$. Then $d + ra = 0$ and so $d = -ra$ and $(d, r) = (-ra, r)$. Moreover, $r = \pi_2(d, r) \in I$. Conversely, let $i \in I$. Then $i = \pi_2(d, r)$ for some $(d, r) \in \ker \mu$. Then $i = r$, $d = -ra = -ia$ and so $(-ia, i) = (d, r) \in \ker \mu$. This proves the claim.

Consider the R-linear map

$$I \to J, \quad i \to \delta(ia).$$

By assumption this map can be extended to an R-linear map

$$\epsilon : R \to J \quad \text{with } \epsilon(i) = \delta(ia) \quad \text{for all } i \in I$$

Define

$$\eta : D \oplus R \to J, (d, r) \to \delta(d) + \epsilon(r).$$

Then η is R-linear. Also for $i \in I$,

$$\eta(-ia, i) = -\delta(ia) + \xi(i) = -\delta(ia) + \delta(ia) = 0.$$

Hence $\ker \mu \leq \ker \eta$ and we obtain a R-linear map

$$\overline{\eta} : (D \bigoplus R)/\ker \mu \to J, (d, r) + \ker \mu \to \delta(d) + \epsilon(r).$$

By the Isomorphism Theorem $\overline{\mu} : (D \bigoplus R)/\ker \to D + ra, (d, r) \to d + ra$ is an isomorphism and we obtain an R-linear map

$$\tau = \overline{\eta} \circ \overline{\mu} : D + Ra \to J \quad \text{with } \tau(d + ra) = \delta(d) + \xi(r) \text{ for all } d \in D, r \in R$$

Then $\tau(d) = \delta(d)$ and so $\tau \in \mathcal{M}$, The maximal choice of δ implies that $D + Ra = D$. Thus $a \in D$. Since this holds for all $a \in A$, $D = A$

Thus $D = A$ and J is injective. The other direction of the lemma is obvious. □

Definition 3.7.11. *Let R be a ring and M an R-module. M is called R-divisible if $rM = M$ for all non-zero r in R.*

Remark 3.7.12. *Let R be a ring and suppose R has a non-zero divisible module. Then R has no zero-divisors.*

Proof. Let R be a ring and M a divisible R-module. Suppose that $ab = 0$ for some non-zero $a, b \in R$.

$$M = bM = a(bM) = (ab)M = 0M = 0$$

□

Lemma 3.7.13. *Let R be a ring and M a divisible R-module,*

(a) Let S be subring of R. Then M is a divisible S-module.

(b) Any R-quotient of M is a divisible R-module.

Proof. Follows directly from the definition of a divisible module. □

Example 3.7.14. *(a) Let R be a ring. Then R is divisible as a left R-module if and only if R is a division ring.*

(b) Let R be an integral domain. Then field of fraction, $\mathbb{F}_R$ is divisible as an R-module.

Lemma 3.7.15. *Let R be a ring and M an R-module.*

(a) If R has no zero-divisors and M is injective, then M is divisible.

(b) If R is a PID, then M is injective if and only of M is divisible.

Proof. (a) Let $0 \neq t \in R$ and $m \in M$ Consider the map

$$Rt \to M, rt \to rm$$

Since R has non-zero divisors this is a well defined R-linear map. As M is injective this map can be extended to an R-linear map $\gamma : R \to M$. Then

$$t\gamma(1) = \gamma(t1) = \gamma(1t) = 1m$$

So Thus $m \in tM$ and $M = tM$. Hence M is divisible.

(b) Suppose that M is divisible. Let I be a ideal in R and $\beta : I \to M$ an R-linear map. As R is a PID, $I = Rr$ for some $t \in R$. As M is divisible, $\beta(t) = tm$ for some $m \in M$. Define

$$\gamma : R \to M, r \to rm.$$

Then γ is R-linear and $\gamma(rt) = rtm = \beta(rt)$. We showed that the condition of 3.7.10 are fulfilled. So M is injective. □

Proposition 3.7.16. *Let R be a integral domain.*

(a) Every R module can be embedded into an divisible R-module.

(b) If R is a PID, then every R-module can be embedded into a injective module.

Proof. (a) Let M an R- module. By 3.7.4(b), M is isomorphic to a quotient of a free R-module. So

$$M \cong A/B,$$

where $A = \bigoplus_{i \in I} R$ for some set I and B is a submodule of A. Let $D = \bigoplus_{i \in I} \mathbb{F}_R$. Then $B \leq A \leq D$ and A/B is a submodule of D/B isomorphic to M. Since $\mathbb{F}_R$ is divisible, 3.7.13 shows that D and D/B are divisible. Thus (a) holds.

(b) By 3.7.15 divisible R-modules for PID's are injective. So (b) follows from 3.7.15. □

Remark 3.7.17. *(a) Let R be a ring and A be an abelian group. Define*

$$\hat{A} = \mathrm{Hom}_{\mathbb{Z}}(R, A) \qquad \textit{and} \qquad \mathrm{Ev}_1 : \tilde{A} \to A,\ \delta \to \delta 1.$$

Let M be an R-module. The fact that

$$\check{\mathrm{Ev}}_1 : \mathrm{Hom}_R(M, \hat{A}) \to \mathrm{Hom}_{\mathbb{Z}}(M, A), \phi \to \mathrm{Ev}_1 \circ \phi$$

is a bijection just means that for all $\mathbb{Z}$-linear maps $\alpha : M \to A$ there exist a unique R-linear map $\phi : M \to \hat{A}$ with $\alpha = \mathrm{Ev}_1 \circ \phi$:

$$\begin{tikzcd}
M \arrow[rr, "\alpha"] \arrow[dr, "\exists!\ \phi"'] & & A \\
& \hat{A} \arrow[ur, "\mathrm{Ev}_1"'] &
\end{tikzcd}$$

Let R be a ring and I a set. Let V be an R-module and $v = (v_i)_{i \in I}$ a family in V. Let A be a projective $\mathbb{Z}$-module. Then by 3.7.7 A is a free module with basis say $(a_i)_{i \in I}$. Obbserve that there exists a unique $\mathbb{Z}$-linear map $\tau : A \to V$ with $\tau(a_i) = v_i$ for all $i \in I$. Moreover, V is free R-module with basis $(v_i)_{i \in I}$ if and only if for all $\mathbb{Z}$-linear functions $\alpha : A \to M$ there exists a unique R-linear map $\phi : V \to M$ with $\alpha = \tilde{\alpha} \circ \tau$:

$$\begin{tikzcd}
M & & A \arrow[ll, "\alpha"'] \arrow[dl, "\tau"] \\
& V \arrow[ul, "\exists!\ \phi"] &
\end{tikzcd}$$

The remarks shows that the class of free R-modules is "dual" to the class of R-modules

$$\{\mathrm{Hom}_R(R, A) \mid A \text{an injective } \mathbb{Z}\textit{-module}\}.$$

We proved above that every free module is projective and every module is the quotient of a free module. We will now proceed to prove the dual versions of these two statements: $\mathrm{Hom}_R(R,A)$ is an injective R-module for any injective $\mathbb{Z}$-module A and any injective R-module is isomorphic to a submodule of $\mathrm{Hom}_R(R,A)$ for some injective $\mathbb{Z}$-module A.

Lemma 3.7.18. *Let R and S be rings and D an injective R-module. Suppose that S is an (R,S)-bimodule with S acting by right multiplication and put $\hat{D} = \mathrm{Hom}_S(S,D)$. Then $\hat{D}$ is an injective S-module.*

Proof. Let $\hat{\beta} : B \to \hat{D}$ and $\alpha : B \to A$ be S-linear functions with α 1-1. Put $\beta = \mathrm{Ev}_1 \circ \hat{\beta}$. By 5.3.9 α is R-linear and since D is injective there exists an R-linear function $\gamma : A \to D$ with $\beta = \gamma \circ \alpha$. By 3.6.19 $\check{\mathrm{Ev}}_1$ is onto and so $\gamma = \mathrm{Ev}_1 \circ \hat{\gamma}$ for some S-linear function $\hat{\gamma} : A \to \check{D}$. Then

$$\mathrm{Ev}_1 \circ (\hat{\gamma} \circ \alpha) = (\mathrm{Ev}_1 \circ \hat{\gamma}) \circ \alpha = \gamma \circ \alpha = \beta = \mathrm{Ev}_1 \circ \hat{\beta}$$

Since $\check{\mathrm{Ev}}_1$ is 1-1 this gives $\hat{\gamma} \circ \alpha = \beta$ and so $\hat{D}$ is projective. □

Theorem 3.7.19. *Let R be a ring and M an R-module.*

(a) There exists a divisible $\mathbb{Z}$-module A such that M is isomorphic to submodule of $\mathrm{Hom}_{\mathbb{Z}}(R,A)$.

(b) Every M is the submodule of an injective R-module.

Proof. (a) Let M be a R-module. By 3.7.16 the $\mathbb{Z}$-module M is a $\mathbb{Z}$-submodule of some divisible $\mathbb{Z}$-module A. Note that $\mathrm{Hom}_R(R,M)$ is an R-submodule of $\mathrm{Hom}_{\mathbb{Z}}(R,A)$. By 3.6.15 $M \cong \mathrm{Hom}_R(R,M)$ as an R-module and so M is isomorphic to an R-submodule of $\mathrm{Hom}_{\mathbb{Z}}(R,A)$.

(b) If A is a divisible $\mathbb{Z}$-module, 3.7.15 shows that A is an injective $\mathbb{Z}$-module. By 3.6.19 (applied to $(\mathbb{Z},R)$ in place of (R,S)) $\mathrm{Hom}_{\mathbb{Z}}(R,A)$ is an injective R-module and so (b) follows from (a). □

Lemma 3.7.20. *(a) Direct summands of injective modules are injective.*

(b) Direct products of injective modules are injective.

Proof. Let R be a ring.

(a) Let $J = J_1 \oplus J_2$ with J injective. Given $\alpha : B \rightarrowtail A$ and $\beta : B \to J_1$. As J is injective there exists $\tilde{\gamma} : A \to J$ with

$$\tilde{\gamma} \circ \alpha = \rho_1 \circ \beta.$$

Put $\gamma = \pi_1 \circ \tilde{\gamma}$. Then

$$\tilde{\gamma} \circ \alpha = \pi_1 \circ \tilde{\gamma} \circ \alpha = \pi_1 \circ \rho_1 \circ \alpha = \alpha.$$

$$\begin{tikzcd}
 & J_1 \oplus J_2 \arrow[dl, two heads, shift right, "\pi_1"'] & \\
J_1 \arrow[ur, tail, shift right, "\rho_1"'] & & A \arrow[ul, "\tilde{\gamma}"'] \arrow[ll, "\pi_1 \circ \tilde{\gamma}"'] \\
 & B \arrow[uu, "\rho_1 \circ \beta"] \arrow[ul, "\beta"] \arrow[ur, tail, "\alpha"'] &
\end{tikzcd}$$

(b) Suppose that $(J_i)_{i\in I}$ is a family of injective R-modules. Given R-linear maps $\alpha : B \rightarrowtail A$ and $\beta : B \to \bigtimes_{i\in I} J_i$. Let $i \in I$. Since J_i is injective there exist an R-linear function $\gamma_i : A \to J_i$ with

$$\gamma_i \circ \alpha = \pi_i \circ \beta$$

By the universal property of $\bigtimes_{\in I} J_i$ there exists an R-linear function

$$\gamma = (\gamma_i)_{i\in I} : A \to \bigtimes_{i\in I} J_i, \ a \to \big(\gamma_i(a)\big)_{i\in I}$$

with

$$\pi_i \circ \gamma = \gamma_i$$

for all $i \in I$. Hence

$$\pi_i \circ \gamma \circ \alpha = \gamma_i \circ \alpha = \pi_i \circ \beta$$

and so $\gamma \circ \alpha = \beta$. Hence $\prod_{i\in I} J_i$ is injective.

$$\begin{tikzcd}
 & J_i & \\
\bigtimes_{i\in I} J_i \arrow[ur, two heads, "\pi_i"] & & A \arrow[ul, "\gamma_i"'] \arrow[ll, "(\gamma_i)_{i\in I}"'] \\
 & B \arrow[uu, "\pi_i \circ \beta"] \arrow[ul, "\beta"] \arrow[ur, tail, "\alpha"'] &
\end{tikzcd}$$

□

Theorem 3.7.21. *Let J be a module over the ring R. Then the following are equivalent:*

(a) J is injective .

(b) Every short exact sequence $0 \to J \xrightarrow{f} B \xrightarrow{g} C \to 0$ splits.

(c) There exists a divisible abelian group A such that J is isomorphic to a direct summand of $\mathrm{Hom}_{\mathbb{Z}}(R,A)$.

Proof. (a) $\Longrightarrow$ (b): Since J is injective we have

$$\begin{tikzcd}
J & & B & & J & & A \arrow[ll, "\eta"'] \\
& J \arrow[ul, "\mathrm{id}_J"] \arrow[ur, tail, "f"'] & & \Longrightarrow & & J \arrow[ul, "\mathrm{id}_J"] \arrow[ur, tail, "f"'] &
\end{tikzcd}$$

So $\eta \circ f = \mathrm{id}_J$ and the exact sequence is split by 3.5.9.

(b) $\Longrightarrow$ (c): By 3.7.19 there exists a divisible abelian group A such that J is isomorphic to a submodule of $\tilde{A} = \mathrm{Hom}_{\mathbb{Z}}(R,A)$. So the exists a 1-1 R-linear function $f : J \to \tilde{A}$ and we obtain a short exact sequence:

$$0 \to J \overset{f}{\to} \tilde{A} \overset{\pi_{\mathrm{Im}\, f}}{\to} \tilde{A}/\operatorname{Im} f \to 0$$

By assumption the sequence split and so by 3.5.9 $\tilde{A} \cong J \oplus \tilde{A}/\operatorname{Im} f$. So (b) holds.

(c) $\Longrightarrow$ (a): By 3.7.18 $\mathrm{Hom}_{\mathbb{Z}}(R,A)$ is injective and so by 3.7.20 any direct summand of $\mathrm{Hom}_{\mathbb{Z}}(R,A)$ is injective. □

3.8 The Functor Hom

Lemma 3.8.1. *Let R be a ring. Given a sequence $A \xrightarrow{f} B \xrightarrow{g} C$ of R-modules. Then the following two statements are equivalent:*

(a)

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is exact and A splits over $\ker f$ *(thats is,* $\ker f$ *is a direct summand of A).*

(b) For all R-modules D,

$$\mathrm{Hom}_R(D,A) \xrightarrow{\check{f}} \mathrm{Hom}_R(D,B) \xrightarrow{\check{g}} \mathrm{Hom}_R(D,C)$$

is exact.

Proof. We first compute $\ker \check{g}$ and $\operatorname{Im} \check{f}$. Let $\beta \in \mathrm{Hom}_R(D,B)$. Then $g \circ \beta = 0$ if and only if $\operatorname{Im}\beta \leq \ker g$. Thus

$$\ker \check{g} = \mathrm{Hom}_R(D, \ker g).$$

Also

$$\operatorname{Im}\check{f} = \{f \circ \alpha \mid \alpha \in \operatorname{Hom}_R(D,A)\} \leq \operatorname{Hom}_R(D, \operatorname{Im} f).$$

(a) $\Longrightarrow$ (b): Suppose first that (a) holds. Then $\ker g = \operatorname{Im} f$ and $A = \ker f \oplus K$ for some R-submodule K of A. It follows that $f\,|_K\colon K \to \operatorname{Im} f$ is an isomorphisms. Let $\phi \in \operatorname{Hom}_R(D, \operatorname{Im} f)$. Put

$$\alpha = (f\,|_K)^{-1} \circ \phi.$$

Then $\alpha \in \operatorname{Hom}_R(D,A)$ and $f \circ \alpha = \phi$. Thus $\phi \in \operatorname{Im}\check{f}$. Since this holds for all $\phi \in \operatorname{Hom}_R(F, \operatorname{Im} f)$ we conclude

$$\operatorname{Im}\check{f} = \operatorname{Hom}_R(D, \operatorname{Im} f) = \operatorname{Hom}_R(D, \ker g) = \ker \breve{g}.$$

(b)a Suppose next that (b) holds. Choose $D = A$. Since the sequence in (b) is exact, $\operatorname{Im}\check{f} = \ker \breve{g}$. Hence

$$f = f \circ \mathrm{id}_A \in \operatorname{Im}\breve{g} = \ker \breve{g} = \operatorname{Hom}_R(D, \ker g)$$

and so $\operatorname{Im} f \leq \ker g$.

Bext choose $D = \ker g$. Then $\operatorname{Im} \mathrm{id}_D = \ker \breve{g}$ and so so

$$\mathrm{id}_D \in \ker \breve{g} = \operatorname{Im}\breve{g} \leq \operatorname{Hom}_R(D, \operatorname{Im} f)$$

and so $\ker g = \operatorname{Im} \mathrm{id}_D \leq \operatorname{Im} f$.

Hence $\ker g = \operatorname{Im} f$ and the sequence in (a) is exact. Also $\mathrm{id}_D \in \operatorname{Im}\check{f}$ and so

$$\mathrm{id}_{\operatorname{Im} f} = \mathrm{id}_D = f \circ \gamma$$

for some $\gamma \in \operatorname{Hom}(\operatorname{Im} f, A)$. Thus 3.5.9 shows that the exact sequence

$$0 \ker f \overset{\mathrm{id}_{\ker f}}{\to} A \overset{f}{\to} \operatorname{Im} f \to 0$$

is split. Thus $\ker f$ is a direct summand of A. □

Here is the dual version of the previous lemma:

Lemma 3.8.2. *Let R be a ring. Given a sequence $A \xrightarrow{f} B \xrightarrow{g} C$. Then following two statements are equivalent:*

(a)

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is exact and C splits over $\operatorname{Im} g$.

(b) For all R-modules D,

$$\mathrm{Hom}_R(A,D) \xleftarrow{f^*} \mathrm{Hom}_R(B,D) \xleftarrow{g^*} \mathrm{Hom}_R(C,D)$$

is exact.

Proof. Dual to the proof of3.8.1. See Homework 2. □

The following three theorem are immediate consequences of the previous two:

Theorem 3.8.3. *Let R be ring. Given a sequence of R-linear maps $A \xrightarrow{f} B \xrightarrow{g} C$. the following are equivalent*

(a)

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C$$

is exact.

(b) For every R module D,

$$0 \to \mathrm{Hom}(D,A) \xrightarrow{\check{f}} \mathrm{Hom}(D,B) \xrightarrow{\check{g}} \mathrm{Hom}(D,C)$$

is exact.

Proof. □

Theorem 3.8.4. *Let R be ring. Then the following are equivalent*

(a)

$$A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is exact.

(b) For every R module D,

$$\mathrm{Hom}_R(A,D) \xleftarrow{f^*} \mathrm{Hom}_R(B,A) \xleftarrow{g^*} \mathrm{Hom}_R(C,A) \leftarrow 0$$

is exact.

Proof. See Homework 2 □

Theorem 3.8.5. *Let R be a ring. Given a sequence of R-linear maps $A \xrightarrow{f} B \xrightarrow{g} C$. Given a sequence of R-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to$. Then the following three statements are equivalent:*

(a)

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is exact and splits.

(b) For all R-modules D,

$$0 \longrightarrow \mathrm{Hom}_R(D,A) \xrightarrow{\check{f}} \mathrm{Hom}_R(D,B) \xrightarrow{\check{g}} \mathrm{Hom}_R(D,C) \longrightarrow o$$

is exact.

(c) For all R-modules D,

$$0 \longleftarrow \mathrm{Hom}_R(A,D) \xleftarrow{f^*} \mathrm{Hom}_R(B,D) \xleftarrow{g^*} \mathrm{Hom}_R(C,D) \longleftarrow 0$$

is exact.

Proof. See Homework 2. □

Theorem 3.8.6. *Let R be a ring, A and R-module and $(B_i)_{i\in I}$ be family of R-modules. Then as abelian groups:*

(a) $\mathrm{Hom}_R(\bigoplus_{i\in I} B_i, A) \cong \bigtimes_{i\in I} \mathrm{Hom}_R(B_i, A)$

(b) $\mathrm{Hom}_R(A, \bigtimes_{i\in I} B_i) \cong \bigtimes_{i\in I} \mathrm{Hom}_R(A, B_i)$

(c) Suppose A is finitely generated as an R-module. Then $\mathrm{Hom}_R(A, \bigoplus_{i\in I} B_i) \cong \bigoplus_{i\in I} \mathrm{Hom}_R(A, B_i)$

Proof. See Homework 2. □

Lemma 3.8.7. *Let R and S be rings. Let $\phi : A \to A'$ be R-linear and let B a (R,S)-bimodule. Then*

(a) $\mathrm{Hom}_R(A,B)$ *is a right S-module by*

$$(fs)(a) = f(a)s.$$

(b)

$$\phi^* : \mathrm{Hom}_R(A',B) \to \mathrm{Hom}_R(A,B),\ f \to f \circ \phi$$

is S-linear.

(c) $\mathrm{Hom}_R(B,A)$ *is a left S-module with action of S given by*

$$(sf)(b) = f(bs)$$

(d)

$$\check{\phi} : \mathrm{Hom}_R(B,A) \to \mathrm{Hom}_R(B,A'), f \to \phi f$$

is S linear.

Proof. Straightforward. □

Let R be a ring and M a R-module. The *dual* of M is the module

$$M^* := \mathrm{Hom}_R(M,R)$$

As R is an (R,R)-bimodule, M^* is a right R-module. The elements of M^* are called *linear functionals* on M.

From 3.8.6 we have

$$(\bigoplus_{i\in I} M_i)^* \cong \prod_{i\in I} M_i^*$$

By 3.6.15 $R^* = \cong R$, (but the reader should be aware that here R is a right R-module that is the action is given by right multiplication.)

We conclude

$$F(I)^* \cong R^I$$

and so if I is finite then $F(I)^*$ is isomorphism to the free right-module on I.

An R-module M is called *cyclic* of $M = Rm$ for some $m \in M$.

Lemma 3.8.8. *Let R be a ring and $M = Rm$ a cyclic R modules. Let $I = \mathrm{Ann}_R(m)$ and $J = \{r \in R \mid Ir = 0\}$.*

(a) J is an right ideal in R.

(b)

$$\tau : M^* \to J, \quad f \to f(m)$$

is an isomorphism of right R-modules.

Proof. (a) Let $j \in J$, $r \in R$ and $i \in I$. Then $i(jr) = (ij)r = 0r = 0$ and so $jr \in J$. Thus (a) holds.

(b) Let $a \in \mathrm{Ann}_R(m)$. Then $af(m) = f(am) = f(0) = 0$ and so $f(m) \in J$. So τ is well defined. It is clearly $\mathbb{Z}$-linear and

$$(fr)(m) = f(m)r$$

So $\tau(fr) = \tau(f)r$ and τ is right R-linear.

Let $j \in J$. Then $Ij = 0$ and so the map

$$\xi(j) : M \to R, rm \to rj$$

is well defined and R-linear.

$$\tau(\xi(j) = \xi(j)(m) = \xi(j)(1m) = 1j = j$$

and

$$(\xi(\tau(f)))(rm) = r\tau(f) = rf(m) = f(rm)$$

and so $\xi(\tau(f)) = f$ and τ is a bijection. □

If R is commutative, left and right modules are the same. So we might have that $M \cong M^*$ as R-modules. In this case M is called *self-dual*. For example free modules of finite rang over a commutative ring are self-dual. Let R be a ring, the *double dual* of a module M is $M^{**} := (M^*)^*$. Define

$$\vartheta : M \to M^{**}, \vartheta(m)(f) = f(m).$$

It is readily verified that ϑ is R-linear. If $M = F_R(I)$ is free of finite rang we see that ϑ is an isomorphism. If $M = F_R(I)$ is free of infinite rang, then ϑ is a monomorphism but usually not an isomorphism.

In general ϑ does not need to be one to one. For example if $R = \mathbb{Z}$, $n \in \mathbb{Z}^+$ and $M = \mathbb{Z}/n\mathbb{Z}$, then it is easy to see that $M^* = 0$. Indeed let $\phi \in M^*$ and $m \in M$. Then $nm = 0$ and so $n\phi(m) = \phi(nm) = 0$. Thus $\phi(m) = 0$ Since $M^* = 0$, also $M^{**} = 0$.

Let us investigate $\ker\vartheta$ in general. Let $m \in M$ then $\vartheta(m) = 0$ if and only if $\phi(m) = 0$ for all $\phi \in M^*$.

3.9 Tensor products

Lemma 3.9.1. *Let R be a ring, A a right R-module, B a left R-module, E an right R-submodule of A and $F = \langle e \otimes b \mid e \in E, b \in B\rangle \leq A \otimes_R B$. Then*

$$\otimes_E : A/E \times B \to (A \otimes_R B)/F, (a + E, b) \to a \otimes b + F$$

is a well defined tensor product of A/E and B over R.

Proof. We will first verify that $\otimes_I$ is well defined: Let $a \in A, e \in E$ and $b \in B$. Then $e \otimes b \in F$ and so

$$(a + e) \otimes b + I = a \otimes b + e \otimes b + F = a \otimes b + F$$

Since $\otimes$ is R-balanced also $\otimes_I$ is R-balanced.

Suppose now that $f : A/E \times B \to D$ is R-balanced.

Consider the function

$$g : A \times B \to D, (a, b) \to f(a + E, b)$$

Since f is $\mathbb{Z}$-bilinear and π_E is $\mathbb{Z}$-linear, g is $\mathbb{Z}$-bilinear. Since f is R-balanced and π_R-is R-linear, g is R-balanced. So there exists a unique $\mathbb{Z}$-linear function

$$\overline{g} : A \otimes B \to D \text{ with } \overline{g}(a \otimes b) = g(a, b) = f(a + E, b)$$

Let $e \in E$ and $b \in B$. Then

$$\overline{g}(e \otimes b) = f(e + E, b) = f(0_{A/E}, b) = 0$$

and so $\epsilon \otimes b \in \ker\overline{g}$. Since $\overline{g}$ is $\mathbb{Z}$-linear this give $F \leq \ker\overline{g}$ and we obtain a well defined $\mathbb{Z}$-linear map

$$\overline{f} : (A \otimes B)/F \to D, u + F \to \overline{g}(u)$$

Then $\overline{f}(a + E \otimes_E b)) = \overline{f}(a \otimes b + F) = \overline{g}(a \otimes b) = g(a, b)$

If $h : A \otimes B/F \to D$ is a $\mathbb{Z}$-linear function with $h(a \otimes b + F) = f(a + E, b)$, then $h = f \circ \pi_F : A \otimes F \to D$ is $\mathbb{Z}$-linear function with $(h \circ \pi_F)(a \otimes b) = g(a, b)$, Thus $h \circ \pi_F = \overline{g}$ and so also $\overline{h} = \overline{f}$. □

Corollary 3.9.2. *Let R be a ring and I a right ideal in R.*

(a) Let M be a left R-module. Then

$$\otimes : R/I \times M \to M/\langle IM\rangle, (r + I, m) \to rm + \langle IM\rangle$$

is a well-defined tensor product of R/I and M over R.

(b) Let J a left ideal in R . Then

$$\otimes : R/I \times R/J \to R/(I + J), \ (r + I, s + J) \to rs + (I + J).$$

is a tensor product for $(R/I, R/J)$ over R.

Proof. (a) By 3.6.10(2) $* : R \times M \to M, (r, m) \to rm$ is a tensor product of R and M over R. Note that $F := \langle i * m \mid i \in I, m \in M\rangle = \langle IM\rangle$ and so (a) follows from 3.9.1.

(b) We apply (a) to $M = R/J$. Then $\langle IM = \langle IR\rangle + J/J = (I + J)/J$. Since $R/J\big/(I + J)/J \cong R/I + J$, we see that (b) holds.

□

Example 3.9.3. 1. Let R be a PID and $a, b \in R$. Then $Ra + Rb = R\gcd(a, b)$ and so

$$R/Ra \otimes_R R/Rb = R/\gcd(a, b)R$$

In particular, if $\gcd(a, b) = 1$, then $R/Ra \otimes_R R/Rb = 0$.

2. Let K be set and R a ring. Let $S = \mathrm{M}_{KK}(R)$. Then R_K is a left and right S-module by left and right multiplication. Fix $k \in K$. Put

$$I = \{A \in S \mid e_k A = 0\} \text{ and } \{A \in S \mid Ae_s\}$$

Since $Se_k = R_K = e_k S$ the left R-module R_K is isomorphic to S/J and the right R-module R_K is isomorphic to S/I. Thus

$$R_K \otimes_S R_K \cong S/I \otimes_S S/J \cong S/(I + J)$$

Since

$$I = \{A \in S \mid A_{kl} = 0 \text{ for all } l \in K\} \quad \text{and } J = \{A \in S \mid A_{lk} = 0 \text{ for all } l \in K\}$$

we have

$$I + J = \{A \in S \mid A_{kk} = 0\}$$

Thus $S/(I+J) \cong R$. It follows that

$$R_K \times R_K \to R,\ (a,b) \to ab = \sum_{i\in I} a_i b_i$$

is a tensor product of R_K and R_K over S.

Proposition 3.9.4. *Let D be a right R-module and*

$$A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

an exact sequence of left R-linear functions. Then

$$D \otimes_R A \overset{\mathrm{id}_D \otimes f}{\longrightarrow} D \otimes_R B \overset{\mathrm{id}_D \otimes g}{\longrightarrow} D \otimes C \to 0$$

is exact sequence of $\mathbb{Z}$-linear maps.

Proof. Put $X = \operatorname{Im} f = \ker g$ and consider the sequences

$$A/\ker f \xrightarrow{\overline{f}} \operatorname{Im} f \xrightarrow{\mathrm{id}_X} B \xrightarrow{\pi_X} B/X \xrightarrow{\overline{g}} C \tag{1}$$

and

$$D \otimes_R A/\ker f \overset{\mathrm{id}_D \otimes \overline{f}}{\longrightarrow} \operatorname{Im} f \overset{\mathrm{id}_D \otimes \mathrm{id}_X}{\longrightarrow} D \otimes_R B \overset{\mathrm{id}_D \otimes \pi_X}{\longrightarrow} D \otimes B/X \overset{\mathrm{id}_D \otimes \overline{g}}{\longrightarrow} D \otimes C \tag{2}$$

Put $E = \langle d \otimes x \mid d \in d, x \in X\rangle \leq D \otimes_R B$ and note that $E = \operatorname{Im}(\mathrm{id}_D \otimes \mathrm{id}_X)$. By 3.9.1 $D \otimes B/X = (D \otimes B)/E$ and $d \otimes (b + X) = (d \otimes b + E)$. Thus $\mathrm{id}_D \otimes \pi_X = \pi_E$ and so $\ker \mathrm{id}_D \otimes \pi_X = E$ and $\mathrm{id}_D \otimes \pi_X$ is onto.

Since the first and the the last functions in (1) are isomorphisms, also the first and last function in (2) are isomorphisms. It follows that

$$\operatorname{Im}(\mathrm{id}_D \otimes f) = \operatorname{Im}(\mathrm{id}_F \otimes \overline{f} = \operatorname{Im}(\mathrm{id}_D \otimes \mathrm{id}_X) = E = \ker(\mathrm{id}_D \otimes \pi X) = \ker(\mathrm{id}_D \otimes g)$$

and $\mathrm{id}_D \otimes g$ is onto. □

Example 3.9.5. Let $R = \mathbb{Z}$, $A = \mathbb{Z}_8$, $B = \mathbb{Z}_4$, $E = 2A$ and $F = \langle e \otimes b \mid e \in E, b \in B\rangle$. Then

$$F = \langle 2a \otimes b \mid a \in A, b \in B\rangle = 2\langle a \otimes b \mid a \in A, b \in B\rangle = 2(A \otimes_R B)$$
$$A \otimes_R B = \mathbb{Z}_8 \otimes_{\mathbb{Z}} \mathbb{Z}_4 = \mathbb{Z}_{\gcd(8,4)} = \mathbb{Z}_4$$
$$(A \otimes_R B)/F = \mathbb{Z}_8/2\mathbb{Z}_8 \cong \mathbb{Z}_2$$
$$A/E = \mathbb{Z}_8/2\mathbb{Z}_8 \cong \mathbb{Z}_2$$
$$(A/E)\otimes_R \cong \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_4 = \mathbb{Z}_{\gcd(2,4)} = \mathbb{Z}_2$$

So $(A/E) \otimes R$ and $A \otimes_R B/F$ are indeed isomorphic.
Consider

$$\sigma : E \otimes_R B \to A \otimes_R B, a \otimes b \to a \otimes b$$

Note that the image of σ is $F \cong \mathbb{Z}_2$. But $E = 2A \cong \mathbb{Z}_4$ and so $E \otimes_R B \cong \mathbb{Z}_4 \otimes \mathbb{Z}_4 = \mathbb{Z}_{\gcd(4,4)} = \mathbb{Z}_4$. Thus σ is not 1-1

Lemma 3.9.6. *Let R be a ring.*

(a) Let $(A_i)_{i\in I}$ be a family of right R-modules and $(B_j)_{j\in J}$ a family of left R-modules. Then

$$h : \bigoplus_{i\in I} A_i \times \bigoplus_{j\in J} B_j \to \bigoplus_{(i,j)\in I\times J} A_i \otimes_R B_j, \quad \big((a_i)_{i\in I}, (b_j)_{j\in J}\big) \to (a_i \otimes b_j)_{(i,j)\in I\times J}$$

is a tensor product of $\bigoplus_{i\in I} A_i$ and $\bigoplus_{j\in J} B_j$ over R.

(b) Let I and J be sets. Then

$$R_I \times_R R_J \to R_{I\times J}, \quad \big((a_i)_{i\in I}, (b_j)_{j\in J}\big) \to (a_i b_j)_{(i,j)\in I\times J}$$

is a tensor product for R_I and R_J over R.

(c) Let R and S be rings with $R \leq S$. Let I be a set and view S as an (S,R)-bimodule. Then

$$S \otimes_R F_R(I) \cong F_S(I)$$

as S-module.

Proof. Note that h is R-balanced. Let $f : \bigoplus_{i\in I} A_i \times \bigoplus_{j\in J} B_j \to D$ be a R-balanced function. For $i \in I$ and $j \in J$ define

$$f_{ij} = f \circ (\rho_i, \rho_j) : A_i \times B_j \to D, (a_i, b_j) \to f(\rho_i a_i, \rho_j b_j)$$

Since ρ_i is $\mathbb{Z}$-linear and f_{ij} is $\mathbb{Z}$-linear in the first coordinate. $\mathbb{Z}$-linear in the first coordinate. By symmetry, f is $\mathbb{Z}$-linear in the second coordinate. Since ρ_i R-linear and f is R-balanced, f_{ij} is R-balanced. Thus the exists unique $\mathbb{Z}$-linear function $\overline{f}_{ij} : A_i \otimes RB_j \to D$ with $\overline{f}_i(a_i \otimes b_j) = f_{i,j}(a_i, b_j)$ for all $a_i \in A_i$ and $b_j \in B_j$. Define

$$\overline{f}: \bigoplus_{(i,j)\in I\times J} A_i \otimes_R B_j \to D, (u_{ij})_{(i,j)\in I\times J} \to \sum_{(i,j)\in I\times J} \overline{f}_{ij}(u_{ij})$$

Then $\overline{f}$ is clearly $\mathbb{Z}$-linear and

$$\begin{aligned}(\overline{f}\circ h)\big((a_i)_{i\in I}, (b_j)_{j\in J}\big) = \overline{f}\big((a_i\otimes b_j)_{(i,j)\in I\times J}\big) &= \sum_{(i,j)\in(I,J)} \overline{f}_{ij}(a_i\otimes b_j) = \sum_{(i,j)\in(I,J)} f_{ij}(a_i,b_j)\\ &= \sum_{(i,j)\in(I,J)} f(\rho_i a_i, \rho_j b_j) = f\left(\sum_{i\in I}\rho_i a_i, \sum_{j\in J}\rho_j b_j\right) = f\big((a_i)_{i\in I}, (b_j)_{j\in J}\big)\end{aligned}$$

and so $f = \overline{f}\circ h$.

Since $\bigoplus_{(i,j)\in I\times J} A_i \otimes_R B_j$ is generated by the $a_i\otimes b_j$, $\overline{f}$ is unique with respect to $f = \overline{f}\circ h$. So (a) holds.

(b) Since $R\times R\to R, (a,b)\to ab$ is a tensor product of R and R over R, (b) follows from (a).

(c) As $S\otimes_R R \cong S$, (c) follows from (a). □

Lemma 3.9.7. *Let A be a right R-module, B a (R,S)-bimodule and C a left S-module. Then there exists $\mathbb{Z}$-linear isomorphism*

$$(A\otimes_R B)\otimes_S C \to A\otimes_R (B\otimes_S C) \text{ with } (a\otimes b)\otimes c \to a\otimes(b\otimes c)$$

for all $a\in A, b\in B, c\in C$.

Proof. Let $c\in C$. Then the function

$$A\times B\to A\otimes(B\otimes C), (a,b)\to a\otimes(b\otimes c)$$

is R-balanced and we obtain a $\mathbb{Z}$-linear function

$$f_c : A\otimes_R B\to A\otimes(B\otimes C), \text{ with } f_c(a\otimes b) = a\otimes(b\otimes c)$$

Then the function

$$f : A\otimes_R B\times C\to A\otimes(B\otimes C), (u,c)\to f_c u$$

is S-balanced and we obtain an $\mathbb{Z}$-linear function

$$F : (A\otimes_R B)\otimes_S C\to A\otimes_R(B\otimes_S C) \text{ with } F(u\otimes c) = f_c u$$

Then $F\big((a\otimes b)\otimes c\big) = f_c(a\otimes b) = a\otimes(b\otimes c)$. By symmetry there exists $\mathbb{Z}$-linear function

$$G : A\otimes_R(B\otimes_S C)\to(A\otimes_R B)\otimes_S C) \text{ with } G\big(a\otimes(b\otimes c)\big) = (a\otimes b)\otimes c$$

F and G are clearly inverse to each other the lemma is proved. □

In future we will just write $A \otimes_R B \otimes_S C$ for any of the two isomorphic tensor products in the previous lemma. A similar lemma holds for more than three factors. $A \otimes_R B \otimes_S C$ can also be characterized through (R,S)-balanced maps from $A \times B \times C \to T$, where T is an abelian group. We leave the details to the interested reader.

Lemma 3.9.8. *Let R be a ring, I and ideal in R, A be a right R-module and B a left R-module. Suppose that $AI = 0$ and UB is zero and observe that A and B are modules for R/I. Then*

$$A \otimes_{R/I} B = A \otimes_R B$$

Proof. Just observe that a function $f : A \times B \to D$ is R-balanced if and only if it is R/I-balanced. □

Lemma 3.9.9. *Let R be a commutative ring and A, B, C, D R-modules.*

(a) There exists a unique R-linear function

$$\mathrm{Hom}_R(A,C) \otimes_R \mathrm{Hom}_R(B,D) \to \mathrm{Hom}_R(A \otimes_R B, C \otimes_R D) \textit{ with } \alpha \otimes \beta \to \alpha \otimes \beta = \big(a \otimes b \to \alpha a \otimes \beta b\big)$$

(b) For an R-module E put $E^* = \mathrm{Hom}_R(E,R)$. There exists a unique R-linear function

$$\sigma : A^* \otimes_R B^* \to (A \otimes_R B)^*, \alpha \otimes \beta \to \alpha \cdot \beta = \big(a \otimes b \to (\alpha a)(\beta b)\big)$$

Proof. (a) Just observe that the function $(\alpha,\beta) \to \alpha \otimes \beta$ is R-balanced.

(b) Since $\cdot : R \times R \to R, (a,b) \to ab$ is the tensor product of R and R over R, this follows from (a) applied with $C = D = R$.

□

Example 3.9.10. *Let R be a ring, I be a left ideal in R and M an R-module. Compute* $\mathrm{Hom}_R(R/I, M)$.

Let $\pi_I : R \to R/I, r \to r + I$ be the natural epimorphism. Then by 3.8.1 the function

$$\pi_I^* : \mathrm{Hom}_R(R/I, M) \to \mathrm{Hom}_R(R, M), \phi \to \phi \circ \pi_I$$

is 1-1 and

$$\mathrm{Im}_{\pi_I^*} = \{\alpha \in \mathrm{Hom}_R(R, M) \mid I \le \ker a\}.$$

By 3.6.15

$$M \to \mathrm{Hom}_R(R, M), m \to (r \to rm)$$

is an R- isomorphism.

Note that $I \subseteq \ker(r \to rm)$ if and only $im = 0$ for all $i \in M$ and so if and only if $m \in \mathrm{Ann}_M(I)$. Thus

$$\mathrm{Ann}_M(I) \to \mathrm{Hom}_R(R/I, M), m \to (r + I \to rm)$$

is a well-defined R isomorphism.

Example 3.9.11. *Let R be a commutative ring*

(a) Let I and J sets. Compute the map $\sigma : R_I^* \otimes_R R_J^* \to (R_I \otimes_R R_J)^*$.

(b) Let I_1 and I_2 be ideal in R. Compute the map $\sigma : (R/I_1)^* \otimes (R/I_2)^* \to (R/I_1 \otimes R/I_2)^*$.

(a) We have

$$(R_I)^* = \mathrm{Hom}_R(\bigoplus_{i\in I} R, R) \cong \bigtimes_{i\in I} \mathrm{Hom}_R(R, R) \cong \bigtimes_{i\in I} R = R^I$$

and

$$(R_I \otimes R_J)^* = (R_{I\times J})^* \cong R^{I\times J}$$

Using these isomorphism σ turns into the function

$$R^I \otimes_R R^J \to R^{I\times J}, \quad (r_i)_{i\in I} \otimes (s_j)_{j\in J} \ \to \ (r_i s_j)_{(i,j)\in I\times J}$$

(b) Put $J_k = \mathrm{Ann}_R(I_k)$. By example 3.1.15,

$$(R/I_k)^* = \mathrm{Hom}_R(R/I_k, R) \cong \mathrm{Ann}_R(I_k) = J_k$$

and by 3.9.2 $R/I_1 \otimes R/I_2 = R/(I_1 \cap I_2)$ and so

$$(R/I_1 \otimes R/I_2)^* = (R/(I_1 \cap I_2))^* = \mathrm{Ann}_R(I_1 + I_2) = \mathrm{Ann}_R(I_1) \cap \mathrm{Ann}_R(I_2) = J_1 \cap J_2.$$

Thus σ turns into the function

$$\sigma : J_1 \otimes_R J_2 \to J_1 \cap J_2 \quad (j_1, j_2) \to j_1 j_2.$$

Lemma 3.9.12. *Let R and S be rings and M an (R,S)-bimodule. Let*

$$T = \left\{ \begin{bmatrix} r & m \\ 0 & s \end{bmatrix} \middle| \ r \in R, m \in M, s \in S \right\}$$

Define an addition and multiplication on T by

$$\begin{bmatrix} r_1 & m_1 \\ 0 & s_1 \end{bmatrix} + \begin{bmatrix} r_2 & m_2 \\ 0 & s_2 \end{bmatrix} = \begin{bmatrix} r_1 + r_2 & m_1 + m_2 \\ 0 & s_1 + s_2 \end{bmatrix}$$

and

$$\begin{bmatrix} r_1 & m_1 \\ 0 & s_1 \end{bmatrix} \cdot \begin{bmatrix} r_2 & m_2 \\ 0 & s_2 \end{bmatrix} = \begin{bmatrix} r_1 r_2 & r_1 m_2 + m_1 s_2 \\ 0 & s_1 s_2 \end{bmatrix}$$

(a) As an additive magma, $T \cong R \oplus M \oplus S$ and we identify R, M with there images in T.

(b) T is a ring.

(c) M is an ideal in T, $T/M \cong R \times S$, $SM = MR = MM = 0$, the action of R on M by left multiplication is the same as the action of M as left R-module, and the action of S on M by right multiplication is the same as the action of S on M as a right S-module.

(d) $\mathrm{Ann}_T^{\text{left}}(M) = \mathrm{Ann}_R(M) + M + S$ *and* $\mathrm{Ann}_T^{\text{right}}(M) = R + M + \mathrm{Ann}_S(M)$

The ring T is denoted by $R \rtimes M \ltimes S$.

Proof. (a) should be obvious.

(b) By (a) T is abelian group under addition. It is rather obvious that the distributive laws holds and so it remains to verify that the multiplication is associative:

$$\left(\begin{bmatrix} r_1 & m_1 \\ 0 & s_1 \end{bmatrix} \cdot \begin{bmatrix} r_2 & m_2 \\ 0 & s_2 \end{bmatrix}\right) \cdot \begin{bmatrix} r_3 & m_3 \\ 0 & s_3 \end{bmatrix} = \begin{bmatrix} r_1 r_2 & r_1 m_2 + m_1 s_2 \\ 0 & s_1 s_2 \end{bmatrix} \cdot \begin{bmatrix} r_3 & m_3 \\ 0 & s_3 \end{bmatrix}$$
$$= \begin{bmatrix} r_1 r_2 r_3 & r_1 r_2 m_3 + r_1 m_2 s_3 + m_1 s_2 s_3 \\ 0 & s_1 s_2 s_3 \end{bmatrix}$$

and

$$\begin{bmatrix} r_1 & m_1 \\ 0 & s_1 \end{bmatrix} \cdot \left(\begin{bmatrix} r_2 & m_2 \\ 0 & s_2 \end{bmatrix} \cdot \begin{bmatrix} r_3 & m_3 \\ 0 & s_3 \end{bmatrix}\right) = \begin{bmatrix} r_1 & m_1 \\ 0 & s_1 \end{bmatrix} \begin{bmatrix} r_2 r_3 & r_2 m_3 + m_2 s_3 \\ 0 & s_2 s_3 \end{bmatrix}$$
$$= \begin{bmatrix} r_1 r_2 r_3 & r_1 r_2 m_3 + r_1 m_2 s_3 + m_1 s_2 s_3 \\ 0 & s_1 s_2 s_3 \end{bmatrix}$$

(c) Identifying R,S and T with the images in T the formula for multiplication looks as follows:

$$(r_1 + m_1 + s_1) \cdot (r_2 + m_2 + s_2) = r_1 r_2 + (r_1 m_2 + +m_1 s_2) + s_1 s_2$$

Thus

$$\begin{array}{ccc} r_1 \cdot r_2 = r_1 r_2 & r \cdot m = rm & r \cdot s = 0 \\ m \cdot r = 0 & m_1 \cdot m_2 = 0 & m \cdot s = 0 \\ s \cdot r = 0 & s \cdot m = 0 & s_1 \cdot s_2 = s_1 s_2 \end{array}$$

This gives (c). (d) follows from (c). □

Example 3.9.13. *Let R be commutative ring and M a faithful R-module. Let*

$$U = \left\{ \begin{bmatrix} r & m \\ 0 & r \end{bmatrix} \middle| \; r \in R, m \in M \right\} \leq T = R \ltimes M \rtimes R$$

Show that U is commutative ring and M is an ideal in U. Compute the function

$$\sigma : (U/M)^* \otimes_U (U/M)^* \to (U/M \otimes U/M)^*$$

Identify $r \in R$ with $\begin{bmatrix} r & m \\ 0 & r \end{bmatrix}$ in U and $m \in M$ with $\begin{bmatrix} 0 & m \\ 0 & 0 \end{bmatrix}$. Then $U = R + M$. $r_1 \cdot r_2 = r_1 r_2$, $r \cdot m = rm = m \cdot r$ and $m_1 \cdot m_2 = m_2 \cdot m_1 = 0$. Thus U is commutative and $\mathrm{Ann}_U(M) = \mathrm{Ann}_R(M) + M = M$.

Thus by Example 3.9.11(b), σ is the function

$$M \times_R M \to M, (m_1, m_2) \to m_1 \cdot m_2 = 0$$

So σ is the zero function.

3.10 Composition series

Definition 3.10.1. *Let R be a ring, M an R-module and $\mathcal{C}$ a set of R-submodules in R. We say that $\mathcal{C}$ is a R*-series *on M provided that*

(a) $\mathcal{C}$ is a chain, that is for any $A, B \in \mathcal{C}$, $A \leq B$ or $B \leq A$.

(b) $0 \in \mathcal{C}$ and $M \in \mathcal{C}$.

(c) $\mathcal{C}$ is closed under unions and intersections, that is if $\mathcal{D} \subseteq \mathcal{C}$, then

$$\bigcup \mathcal{D} \in \mathcal{C} \textit{ and } \bigcap \mathcal{D} \in \mathcal{C}.$$

For example any finite chain

$$0 = M_0 < M_1 < M_2 < M_3 < \ldots < M_{n-1} < M_n = M$$

of R-submodules of M is an R-series.

If $R = M = \mathbb{Z}$ and p is a prime then

$$0 < \ldots < p^{k+1}\mathbb{Z} < p^k\mathbb{Z} < p^{k-1}\mathbb{Z} < \ldots < p\mathbb{Z} < \mathbb{Z}$$

is a $\mathbb{Z}$-series. More generally, if $n_1, n_2, n_3, \ldots$ is any sequence of integers larger than 1, then

$$0 < n_1 \ldots n_{k+1}\mathbb{Z} < n_1 \ldots n_k\mathbb{Z} < \ldots < n_1 n_2\mathbb{Z} < n_1\mathbb{Z} < \mathbb{Z}$$

is a $\mathbb{Z}$ series on $\mathbb{Z}$.

Definition 3.10.2. *Let R be a ring, M an R-module and $\mathcal{C}$ an R-series on M.*

(a) A jump *in $\mathcal{C}$ is a pair (A, B) with $A, B \in \mathcal{C}$, $A \not\leq B$ and so so that*

$$D \leq A \text{ or } B \leq D \text{ for all } D \in \mathcal{C}.$$

Jump$(\mathcal{C})$ *is the set of all jumps of $\mathcal{C}$.*

(b) If (A, B) is a jump of $\mathcal{C}$ then B/A is called a factor *of $\mathcal{C}$.*

*(c) $\mathcal{C}$ is a R-*composition series *on M provided that all the factors of $\mathcal{C}$ are simple R-modules.*

Let $\mathcal{C}$ be R-series on M. For $B \in \mathcal{C}$ define

$$B^- = \bigcup\{A \in \mathcal{C} \mid A \not\leq B\}.$$

Note that $B^- \in \mathcal{C}$ and $B^- \leq B$.

Suppose that $B^- \neq B$. Let $D \in \mathcal{C}$. Then $B \leq D$ or $D \not\leq B$. In the latter case, $D \leq B^-$ and so (B^-, B) is a jump of $\mathcal{C}$.

Conversely, if (A, B) is a jump it is easy to see that $A = B^-$. Thus

$$\text{Jump}(\mathcal{C}) = \{(B^-, B) \mid B \in \mathcal{C}, B^- \neq B\}.$$

Consider the series

$$0 < n_1 \ldots n_{k+1}\mathbb{Z} < n_1 \ldots n_k\mathbb{Z} < \ldots < n_1 n_2\mathbb{Z} < n_1\mathbb{Z} < \mathbb{Z}.$$

As $n_1 \ldots n_{k+1})\mathbb{Z}/n_1 \ldots n_k\mathbb{Z} \cong \mathbb{Z}/n_k\mathbb{Z}$ as R-modules, this series is a composition series if and only if each n_k is a prime. If we chose $n_k = p$ for a fixed prime p we get a composition series all of whose factors are isomorphic. On the other hand we could choose the n_k to be pairwise distinct primes and obtain a composition series so that now two factors are isomorphic.

Proposition 3.10.3. *Let R be a ring and M a R-module. Let $\mathcal{M}$ be the set of chains of R-submodules in M. Order $\mathcal{M}$ by inclusion and let $\mathcal{C} \in \mathcal{M}$. Then $\mathcal{C}$ is a composition series if and only if $\mathcal{C}$ is a maximal element in $\mathcal{M}$.*

Proof. $\Longrightarrow$ Suppose that $\mathcal{C}$ is a composition series but is not maximal in $\mathcal{M}$. Then $\mathcal{C} \subsetneq \mathcal{D}$ for some $\mathcal{D} \in \mathcal{M}$. Hence there exists $D \in \mathcal{D} \setminus \mathcal{C}$. We will show that there exists a jump of $\mathcal{C}$ so that the corresponding factor is not simple, contradicting the assumption that $\mathcal{C}$ is a composition series. Define

$$D^+ = \bigcap\{E \in \mathcal{C} \mid D \leq E\} \text{ and } D^- = \bigcup\{E \in \mathcal{C} \mid E \leq D\}.$$

As $\mathcal{C}$ is closed under unions and intersections both D^+ and D^- are members of $\mathcal{C}$. In particular, $D^- \neq D \neq D^+$. From the definition of D^+, $D \leq D^+$, also $D^- \leq D$ and so

$$D^- \not\leq D \not\leq D^+.$$

Thus D/D^+ is a proper R-submodule of D^+/D^- and it remains to verify that (D^-, D^+) is a jump. For this let $E \in \mathcal{C}$. As $\mathcal{D}$ is totally ordered, $E \leq D$ or $D \leq E$. In the first case $E \leq D^-$ and in the second $D^+ \leq E$.

$\Longleftarrow$ Let $\mathcal{C}$ be a maximal element of $\mathcal{M}$. We will first show that

(*) Let E be an R-submodule of G such that for all $C \in \mathcal{C}$, $E \leq C$ or $C \leq E$. Then $E \in \mathcal{C}$.

Indeed, under these assumptions, $\{E\} \cup \mathcal{C}$ is a chain of submodules and so the maximality of $\mathcal{C}$ implies $E \in \mathcal{C}$.

From (*) we conclude $0 \in \mathcal{C}$ and $M \in \mathcal{C}$. Let $\mathcal{D} \subseteq \mathcal{C}$ and put $E = \bigcup \mathcal{D}$. We claim that E fulfills the assumptions of (*). For this let $C \in \mathcal{C}$. If $C \leq D$ for some $D \in \mathcal{D}$ then $C \leq D \leq E$. So suppose that $C \nleq D$ for each $D \in \mathcal{D}$. As $\mathcal{C}$ is totally ordered, $D \leq C$ for each $D \in \mathcal{D}$. Thus $E \leq D$. So we can apply (*) and $E \in \mathcal{C}$. Thus $\mathcal{C}$ is closed under unions.

Similarly, $\mathcal{C}$ is closed under intersections. Thus $\mathcal{C}$ is a series and it remains to show that all its factors are simple. So suppose that (A, B) is a jump of $\mathcal{C}$ so that B/A is not simple. Then there exists a proper R-submodule $\bar{E}$ of B/A. Note that $\bar{E} = E/A$ for some R-submodule E of M with

$$A \nleq E \nleq B.$$

As (A, B) is a jump, $E \notin \mathcal{C}$. Let $C \in \mathcal{C}$. Then $C \leq A$ or $B \leq C$. So $C \leq E$ or $E \leq C$. Thus by (*), $E \in \mathcal{C}$, a contradiction □

Corollary 3.10.4. *Every R-modules has a composition series.*

Proof. Let $\mathcal{M}$ be as in 3.10.3. We leave it as an routine application of Zorn's Lemma A.3.8 to show that $\mathcal{M}$ has a maximal element. By 3.10.3 any such maximal element is a composition series. □

In the next lemma we will find series for direct sums and direct products of modules. For this we first need to introduce the concept of cuts for a totally ordered set $(I, \leq)$.

We say that $J \subseteq I$ is a *cut* of I if for all $j \in J$ and all $i \in I$ with $i \leq j$ we have $i \in J$. Let $\mathrm{Cut}(I)$ be the set of all cuts of I. Note that $\varnothing \in \mathrm{Cut}(I)$ and $I \in \mathrm{Cut}(I)$. Order $\mathrm{Cut}(I)$ by inclusion. We claim that $\mathrm{Cut}(I)$ is totally ordered. Indeed, let $J, K \in \mathrm{Cut}(I)$ with $K \nsubseteq J$. Then there exists $k \in K \setminus J$. Let $j \in J$. Since $k \notin J$ and J is a cut, $k \nleq j$. Since I is totally ordered, $j < k$ and since K is a cut, $j \in K$. So $J \subseteq K$ and $\mathrm{Cut}(I)$ is totally ordered.

Let $i \in I$ and put $i^+ = \{j \in I \mid j \leq i\}$. Note that i^+ is a cut of I. The map $I \to \mathrm{Cut}(I)$, $i \to i^+$ is an embedding of totally ordered sets. Put $i^- = \{j \in I \mid j < i\}$. Then also i^- is a cut.

We leave it as an exercise to verify that unions and intersection of arbitrary sets of cuts are cuts.

As an example consider the case $I = \mathbb{Q}$ ordered in the usual way. Let $r \in \mathbb{R}$ and define $r^- = \{q \in \mathbb{Q} \mid q < r\}$. Clearly r^- is a cut. We claim that every cut of $\mathbb{Q}$ is exactly one of the following cuts:

$$\varnothing; \quad \mathbb{Q}; \quad q^+ \,(q \in \mathbb{Q}); \quad r^- \,(r \in \mathbb{R})$$

Indeed, let be J be a non-empty cut of $\mathbb{Q}$. If J has no upper bound in $\mathbb{Q}$, then $J = \mathbb{Q}$. So suppose that J has an upper bound. By a property of the real numbers, every bounded non-empty subset of $\mathbb{R}$ has a least upper bound. Hence J has a least upper bound a. Then $J \subseteq r^+$.

If $r \in J$, then $r \in \mathbb{Q}$ and $r^+ \subseteq J \subseteq r^+$. So $J = r^+$.

If $r \notin J$ we have $J \subseteq r^-$. We claim that equality holds. Indeed let $q \in r^-$. As r is a least upper bound for J, q is not an upper bound for J and so $q < j$ for some $j \in J$. Thus $q \in J$ and $J = r^-$.

Lemma 3.10.5. *Let $(I, \leq)$ be a totally ordered set and R a ring. For $i \in I$ let M_i be a non zero R-module. Let $M \in \{\bigoplus i \in IM_i, \prod_{i\in I} M_i$. For J a cut of I define*

$$M_J^+ = \{m \in M \mid m_i = 0 \, \forall i \in I \smallsetminus J\}$$

and if $J \neq \varnothing$,

$$M_J^- = \{m \in M \mid \exists j \in J \text{ with } m_i = 0 \, \forall i \geq j\}.$$

Put $M_\varnothing^- = 0$.

(a) For all $k \in I$, $M_{k^+}^- = M_{k^-}^+$ and $M_{k^+}^+ / M_{k^-}^+ \cong M_k$.

(b) Let $M = \bigoplus_{i \in I} M_i$. Then

  (a) $\mathcal{C} := \{M_J^+ \mid J \in J \in \mathrm{Cut}(I)\}$ is an R-series on M.

  (b) $\mathrm{Jump}(\mathcal{C}) = \{(M_{k^-}^+, M_{k^+}^+) \mid k \in I\}$.

  (c) $\mathcal{C}$ an R-composition series if and only if each $M_k, k \in I$ is a simple R-module.

(c) Let $M = \prod_{i\in I} M_i$ Then

  (a) $\mathcal{C} := \{M_J^+, M_J^- \mid J \in J \in \mathrm{Cut}(I)\}$ is an R-series on M.

  (b) $\mathrm{Jump}(\mathcal{C}) := \{(M_J^-, M_J^+) \mid \varnothing \neq J \in \mathrm{Cut}(I)\}$.

  (c) $\mathcal{C}$ is an R-composition series if and only if each non-empty subset ofI has a maximal element and each $M_k, k \in I$ is a simple R-module.

Proof. (a) The first statement follows directly from the definitions. For the second note that the map $M_{k^+} \to M_k, m \to m_k$ is onto with kernel M_{k^-}.

(b) & (c) Note that $M_J^- \leq M_J^+$.

Let $\mathrm{Cut}^*(I)$ be the set of cuts without a maximal element. So

$$\mathrm{Cut}(I) = \{k^+ \mid k \in K\} \cup \mathrm{Cut}^*(I).$$

Let $J \in \mathrm{Cut}^*(I)$. We claim that $M_J^- = M_J^+$ if $M = \bigoplus_{i\in I} M_i$ and $M_J^- \neq M_J^+$ if $M = \prod_{i \in I} M_i$.

So suppose first that $M = \bigoplus_{i\in I} M_i$ and let $0 \neq m \in M_J^+$ and pick $k \in J$ maximal with $m_k \neq 0$ (this is possible as only finitely many m_i's are not 0). Since J has no maximal element there exists $j \in J$ with $k < j$. Then $m_i = 0$ for all $i \geq j$ and so $m \in M_J^-$.

Suppose next that $M = \prod_{i\in I} M_i$. For $j \in J$ pick $0 \neq m_j \in M_j$. For $i \in I \smallsetminus J$ let $m_i = 0$. Then $(m_i) \in M_J^+$ but $(m_i) \notin M_J^-$.

From the claim we conclude that in both cases

$$\mathcal{C} := \{M_J^+, M_J^- \mid J \in \mathrm{Cut}(I)\}$$

We will show now that $\mathcal{C}$ is a chain. For this let J and K be distinct cuts. Since $\mathrm{Cut}(I)$ is totally ordered we may assume $J \subset K$. Then

$$M_J^- \le M_J^+ \le M_K^- \le M_K^+.$$

and so $\mathcal{C}$ is totally ordered.

Also $0 = M_\varnothing^+$ and $M = M_I^+$.

Let $\mathcal{D}$ be a subset of $\mathcal{C}$. We need to show that both $\bigcap \mathcal{D}$ and $\bigcup \mathcal{D}$ are in $\mathcal{D}$. Let $D \in \mathcal{D}$. Then $D = M_{J_D}^{\epsilon_D}$ for some $J_D \in \mathrm{Cut}(I)$ and $\epsilon_D \in \{\pm\}$.

Put $J = \bigcap_{D\in\mathcal{D}} J_D$. Suppose first that $M_J^- \in \mathcal{D}$.

Then $M_J^- \subseteq D$ for all $D \in \mathcal{D}$ and

$$\bigcap \mathcal{D} = M_J^-.$$

So suppose that $M_J^- \notin \mathcal{D}$. Then $M_J^+ \le D$ for all $D \in \mathcal{D}$ and so $M_J^+ \subseteq \bigcap \mathcal{D}$. We claim that

$$\bigcap \mathcal{D} = M_J^+.$$

Indeed, let $m \in \bigcap \mathcal{D}$ and $i \in I \setminus J$. Then $i \notin J_D$ for some $D \in \mathcal{D}$. As

$$m \in D = M_{J_D}^{\epsilon_D} \le M_{J_D}^+$$

we get $m_i = 0$. Thus $m \in M_J^+$, proving the claim.

So $\mathcal{C}$ is closed under arbitrary unions.

Let $K = \bigcup\{J_D \mid D \in \mathcal{D}\}$.

Suppose that $M_K^+ \in \mathcal{D}$. Then $M \subseteq M_K^+$ for all $D \in \mathcal{D}$ and

$$\bigcup \mathcal{D} = M_K^+.$$

So suppose that $M_K^+ \notin \mathcal{D}$. Then $\bigcup \mathcal{D} \subseteq M_K^-$. We claim that

$$\bigcup \mathcal{D} = M_K^-.$$

If $K = \varnothing$ each J_D is the empty set. So we may assume $K \neq \varnothing$. Let $m \in M_K^-$. Then by definition there exists $k \in K$ with $m_i = 0$ for all $i \ge k$. Pick $D \in \mathcal{D}$ with $i \in J_D$. Then

$$m \in M_{J_D}^- \le M_{J_D}^{\epsilon_D} = D \le \bigcup \mathcal{D}.$$

So the claim is true and $\mathcal{C}$ is closed under unions.

Hence $\mathcal{C}$ is an R-series on M.

Next we investigate the jumps of $\mathcal{C}$. As seen above every cut is of the form (B^-, B) for some $B = M_J^\epsilon \in \mathcal{C}$ with $B \neq B^-$.

Suppose first that $J = k^+$ for $k \in I$. As $M^-_{k^+} = M^+_{k^-}$ we may and do assume $\epsilon = +$. Thus $M^-_{k^+} = M^+_{k^-} = (M^+_{k^+})^-$ and $M^+_{k^-}, M^+_{k^+})$ is a jump with factor isomorphic to M_k.

Suppose next that $J \in \mathrm{Cut}^*(I)$. Then $M^-_J = \bigcup_{j\in J} M_{j^+} \leq (M^-_J)^-$. We conclude that $(M^+_J)^- = (M^-_J)_= M^-_J$. If $M = \bigoplus_{i\in I} M_i$ then as seen above $M^-_J = M^+_J$. So we only get a jump if $\epsilon = +$ and $M = M = \prod_{i\in I} M_i$.

The factor M^+_J/M^-_J can be describes as follows. Identify M^+_J with $\prod_{j\in J} M_j$. Define $x, y \in \prod_{j\in J} M_j$ to be equivalent if and only if there exists $j \in J$ with $x_i = y_i$ for all $i \in J$ with $j \leq i$. It is easy to check that this is an equivalence relation, indeed x and y are equivalent if and only if $y - x \in M^-_J$. In particular, M^+_J/M^-_J is the set of equivalence classes. We claim that M^+_J/M^-_J is never a simple module. For this let $J = J_1 \cup J_2$ with $J_1 \cap J_2 = \varnothing$ so that for each $j_1 \in J_1$ there exists $j_2 \in J_2$ with $j_1 < j_2$, and vice versa. (We leave the existence of J_1 and J_2 as an exercise). Then M^+_J/M^-_J is the direct sum of the images of $\prod_{j\in J_i} M_j$ in M^+_J/M^-_J.

Finally we claim that every non-empty subset of I has a maximal element if and only if every non-empty cut of I has a maximal element. One direction is obvious. For the other let J be a non-empty subset of I and define $J^* = \{i \in I \mid i \leq j \text{ for some } j \in J\}$. Clearly J^* is a cut and $J \subseteq J^*$. Suppose J^* has a maximal element k. Then $k \leq j$ for some $j \in J$. As $j \in J^*$ we conclude $j \leq k$ and so $j = k$ and k is the maximal element of J.

It is now easy to see that (bc) and(cc) hold and all parts of the lemma are proved. □

Corollary 3.10.6. *Let R be a ring and I a set. Let M be one of $F_R(I)$ and R^I. Then there exists an R-series $\mathcal{C}$ of on M so that all factors of $\mathcal{C}$ are isomorphic to R and $|\mathrm{Jump}(\mathcal{C})| = |I|$. Moreover, if R is a division ring $\mathcal{C}$ is a composition series.*

Proof. By the well-ordering principalA.3.11 there exists a well ordering $\leq^*$ be a well ordering on I. Define a partial order $\leq$ on I by $i \leq j$ if and only if $j \leq^* i$. Then every non-empty subset of I has a maximal element and all non empty cuts of I are of the form k^+, $k \in K$. The result now follows from 3.10.5 □

As an example let $R = \mathbb{Q}$. If $I = \mathbb{Q}$ we see that the countable vector space $F_{\mathbb{Q}}(\mathbb{Q})$ as an uncountable composition series. But note that the number of jumps is countable. If $I = \mathbb{Z}^-$ we conclude that uncountable vector space $\mathbb{Q}^{\mathbb{Z}^-}$ as a countable composition series. So the number of jumps in a composition series can be smaller than the dimensions of the vector space. But the next proposition shows that the number of jumps never exceeds the dimension.

Proposition 3.10.7. *Let $\mathbb{D}$ be a division ring and V a vector space over $\mathbb{D}$. Let $\mathcal{C}$ be a $\mathbb{D}$ series on V, and $\mathcal{B}$ a $\mathbb{D}$-basis for V. Then*

$$|\mathrm{Jump}\mathcal{C}| \leq \mathcal{B}.$$

In particular, any two basis for V have the same cardinality.

Proof. Choose some well ordering on $\mathcal{B}$. Let $0 \neq v \in V$. Then $v = \sum_{b\in\mathcal{B}} d_b(v)b$ with $d_b(v) \in \mathbb{D}$, where almost all $d_b(v), b \in \mathcal{B}$ are zero. So we can choose $h(v) \in \mathcal{B}$ maximal with respect to $d_{h(v)}(v) \neq 0$.

Define a map

$$\phi : \mathrm{Jump}(\mathcal{C}) \to \mathcal{B}$$

$$(A,B) \to \min\{h(v) \mid v \in A \setminus B\}$$

We claim that ϕ is one to one. Indeed suppose that (A,B) and (E,F) are distinct jumps with $b = \phi((A,B)) = \phi((E,F))$. As $\mathcal{C}$ is totally ordered and (A,B) and (E,F) are jumps we may assume $A \leq B \leq E \leq F$. Let $v \in B \setminus A$ with $h(v) = b$ and $d_b(v) = 1$. Let $w \in F \setminus E$ with $h(w) = b$ and $d_b(w) = 1$. Since $v \in A \in E$, $w - v \in F \setminus E$. Also $d_b(w-v) = 1 - 1 = 0$ and so $h(w-v) < b$ a contradiction to $b = \phi(E,F)$.

So ϕ is one to one and $|\mathrm{Jump}(\mathcal{C})| \leq |\mathcal{B}|$.

The second statement follows from the first and 3.10.6. □

Lemma 3.10.8. *Let $\mathcal{C}$ be a series for R on M.*

(a) Let $0 \neq m \in M$. Then there exists a unique jump (A,B) of $\mathcal{C}$ with $m \in B$ and $m \notin A$.

(b) Let $D, E \in \mathcal{C}$ with $D < E$. Then there exists a jump (A,B) in $\mathcal{C}$ with

$$D \leq A < B \leq E$$

Proof. (a) Let $B = \bigcap\{C \in \mathcal{C} \mid m \in C\}$ and $A = \bigcup\{C \in \mathcal{C} \mid m \notin C\}$.

(b) Let $m \in E \setminus D$ and let (A,B) be as in (a). □

The following lemma shows how a series can be reconstructed from its jumps.

Lemma 3.10.9. *Let R be a ring, M an R-module and $\mathcal{C}$ an R-series on M. Let $\hat{\mathcal{C}} = \{C \in \mathcal{C} \mid C \neq C^-$. Then the map*

$$\alpha : \mathrm{Cut}(\hat{\mathcal{C}}) \to \mathcal{C},\ K \to \bigcup K$$

is a bijection.

Proof. Note first that as $\mathcal{C}$ is closed under unions $\alpha(K)$ is indeed in $\mathcal{C}$. We will show that the inverse of α is

$$\beta : \mathcal{C} \to \mathrm{Cut}(\hat{\mathcal{C}}),\ D \to \{A \in \hat{\mathcal{C}} \mid A \leq D\}.$$

It is easy to verify that $\beta(D)$ is a cut.

Clearly, $K \subseteq \beta(\alpha(K))$. Let $E \in \hat{\mathcal{C}}$ with $E \notin K$. Then as K is a cut, $A < E$ for all $A \in K$. But then $A \leq E^-$ and so $\alpha(K) \leq E^- < E$. Thus $E \nleq \alpha(K)$ and $E \notin \beta(\alpha(K))$. Hence $\beta(\alpha(K)) = K$.

Clearly $\alpha(\beta(D) \leq D$. Suppose that $\alpha(\beta(D)) < D$. Then by 3.10.8b there exists a jump (A,B) of $\mathcal{C}$ with $\alpha(\beta(D)) \leq A < B \leq D$. But then $B \in \beta(D)$ and so $B \leq \alpha(\beta(D))$, a contradiction. □

Lemma 3.10.10. *Let $\mathcal{C}$ be a series for R on M and W an R-submodule in M. Then*

(a)

$$\mathcal{C} \cap W := \{D \cap W \mid D \in \mathcal{C}\}$$

is an R-series on M.

(b) Let

$$\mathrm{Jump}^W(\mathcal{C}) = \{(A,B) \in \mathrm{Jump}(\mathcal{C}) \mid A \cap W \neq B \cap W\}.$$

Then the map

$$\mathrm{Jump}^W(\mathcal{C}) \to \mathrm{Jump}(\mathcal{C}) \cap W, \quad (A,B) \to (A \cap W, B \cap W)$$

is a bijection. Moreover,

$$B \cap W/A \cap W \cong (B \cap W) + A/A \leq B/A$$

(c) If $\mathcal{C}$ is a R-composition series on M then $\mathcal{C} \cap W$ is a R-composition series on W. Moreover, there exists an embedding $\phi : \mathrm{Jump}(\mathcal{C} \cap W) \to \mathrm{Jump}(\mathcal{C})$, so that so corresponding factors are R-isomorphic. The image of ϕ consists of all the jumps (A,B) of $\mathcal{C}$ with $B = A + (B \cap W)$.

Proof. (a) Clearly $\mathcal{C} \cap W$ is a chain of R-submodules in W. Also $0 = 0 \cap W \in \mathcal{C} \cap W$, $W = M \cap W \in \mathcal{C} \cap W$ and its is easy to verify that $\mathcal{M} \cap W$ is closed under unions and intersections.

(b) Let $(A,B) \in \mathrm{Jump}^W(\mathcal{C})$. We will first verify that $(A \cap W, B \cap W)$ is a jump of $\mathcal{C} \cap W$. Let $D \in \mathcal{C} \cap W$. Then $D = E \cap W$ for some $E \in \mathcal{C}$. As (A,B) is a jump, $E \leq A$ or $B \leq E$. Thus $D = E \cap W \leq A \cap W$ or $B \cap W \leq E \cap W = D$. To show that the map is bijective we will construct its inverse. For $D \in \mathcal{C} \cap W$ define

$$D^- = \bigcup\{C \in \mathcal{C} \mid C \cap W \leq D\} \text{ and } D^+ = \bigcap\{C \in \mathcal{C} \mid D \leq C \cap W\}.$$

Then it easy to verify that $D^+ \cap W = D = D^- \cap W$. Let (D,E) be a jump in $\mathcal{C} \cap W$. Let $C \in \mathcal{C}$. Since (D,E) is a jump in $\mathcal{C} \cap W$, $C \cap W \leq D$ or $E \leq C \cap W$. In the first case $C \leq D^+$ and in the second $E^- \leq C$. So (D^+, E^-) is a jump of $\mathcal{C}$. It is readily verified that maps $(D,E) \to (D^+, E^-)$ is inverse to the map $(A,B) \to (A \cap W, B \cap W)$.

The last statement in (b) follows from

$$B \cap W/A \cap W = (B \cap W)/(B \cap W) \cap A \cong (B \cap W) + A)/A.$$

(c) Note that $A \cap W \neq B \cap W$ if and only if $(B \cap W) + A/A \neq 0$. Since $\mathcal{C}$ is a composition series, B/A is simple. Thus $(B \cap W) + A/A \neq 0$ if and only if $B = (B \cap W) + A$. Thus by (b) all factors of $\mathcal{C} \cap W$ are simple and $\mathcal{C} \cap W$ is a R-composition series on W. □

Theorem 3.10.11 (Jordan-Hölder). *Let R be a ring and M a module. Suppose R has a finite composition series $\mathcal{C}$ on M and that $\mathcal{D}$ is any composition series for R on M. Then $\mathcal{D}$ is finite and there exists a bijection between the set of factors of $\mathcal{C}$ and the set of factors of $\mathcal{D}$ sending a factor of $\mathcal{C}$ to an R-isomorphic factor of $\mathcal{D}$.*

Proof. Let W be the maximal element of $\mathcal{D} - M$. Then $\mathcal{D} - M$ and (by 3.10.10 $\mathcal{C} \cap W$ are composition series for W. By induction on $|\mathcal{D}|$, $\mathcal{D} \cap W$ is finite and has the same factors as $\mathcal{D} - M$.

For $E \in \mathcal{C} \cap W$ define E^+ and E^- as in 3.10.10. Let $calE = \{E^+, E^- \mid E \in \mathcal{D} \cap W$. Then $\mathcal{E}$ is a finite series on M. Since $W^+ = M \nleq W$ we can choose $L \in \mathcal{E}$ minimal with respect to $L \nleq W$. Then $L = E^\epsilon$ for some $E \in \mathcal{C} \cap W$ and $\epsilon \in \{\pm\}$. Suppose first that $L = E^-$. Since $0^- = 0 \leq W$, $E \neq 0$ and so there exists $F \in \mathcal{C} \cap W$ such that (F,E) is a jump in $\mathcal{C} \cap W$. But then $(F^+, E^-) \in \mathrm{Jump}^W(\mathcal{C})$, $F^+ \leq W$

and by 3.10.10c, $E^- = F^+ + (E^- \cap W) \leq W$ a contradiction. So $E^+ = L \neq E^-$. By 3.10.8b there exists a jump (A, B) of $\mathcal{C}$ with $E^- \leq A < B \leq E^+$. Then $E = E^- \cap W \leq A \cap W \leq B \cap W \leq E^+ \cap W = E$ and so $E = A \cap W = B \cap W$. So by definition (see 3.10.8b), $(A, B) \notin \text{Jump}^W(\mathcal{C})$. Also $B \nleq W$ and so as M/W is simple, $M = B + W$. If $A \nleq W$, then also $M = A + W$ and $B = B \cap M = B \cap (A + W) = A + (B \cap W) \leq A$ a contradiction. Hence $A \leq W$ and $A = B \cap W$. Thus

$$B/A = B/B \cap W \cong B + W/W = M/W$$

We claim that $\text{Jump}(\mathcal{C}) = \text{Jump}^W(\mathcal{C}) \cup \{(A, B)\}$. So let (X, Y) be a jump of $\mathcal{C}$ not contained in $\text{Jump}^W(\mathcal{C})$. By 3.10.10c, $Y \nleq X + (Y \cap W)$ and so also $Y \nleq X + W$. Thus $Y \nleq W$ and $X \leq W$. As $A \leq W$, $Y \nleq A$. As (A, B) is a jump $B \leq Y$. As $B \nleq W$, $B \nleq X$ and so $X \leq A$. Thus $X \leq A < B \leq Y$ and as (X, Y) is a jump, $(A, B) = (X, Y)$.

By 3.10.10c, the factors of $\text{Jump}^W(\mathcal{C})$ are isomorphic to the factors of $\mathcal{C} \cap W$ and so with the factors of $\mathcal{D} - M$. As $B/A \cong M/W$ it only remains to show that $\mathcal{D}$ is finite. But thus follows from 3.10.9. □

Chapter 4

Fields

4.1 Extensions

Definition 4.1.1. *Let F be an integral domain, $\mathbb{K}$ a subfield of F and $a \in F$.*

(a) *F is called an* extension *of $\mathbb{K}$. We will also say that $\mathbb{K} \leq F$ is an extension.*

(b) *If F is a field, F is called* field extension *of $\mathbb{K}$ % li c A* vector space *over $\mathbb{K}$ is a unitary $\mathbb{K}$-module. A vector space over $\mathbb{K}$ is also called a* $\mathbb{K}$-space.

(c) *The extension $\mathbb{K} \leq \mathbb{F}$ is called a* finite *if* $\dim_{\mathbb{K}} F$ *finite, where F is viewed as a $\mathbb{K}$ space by left multiplication.*

(d) *If S is a ring, R a subring if S and $I \subseteq R$, then*

$$R[I] := \bigcap\{T \mid T \text{ is a subring of } S \text{ with } R \cup I \subseteq S\}$$

$R[I]$ is called the subring of S generated by R and I.

(e) *If F is a field and $I \subseteq F$, then*

$$\mathbb{K}(I) := \bigcap\{T \mid T \text{ is a field of } F \text{ with } \mathbb{K} \cup I \subseteq F\}$$

$\mathbb{K}(I)$ is called the subfield of $\mathbb{F}$ generated by $\mathbb{K}$ and I.

(f) *A polynomial $f \in \mathbb{K}[x]$ is called monic if its leading coefficient is $1_{\mathbb{K}}$.*

(g) *$\Phi_a = \Phi_a^{\mathbb{K}}$ denotes the unique ring homomorphism*

$$\Phi_a : \mathbb{K}[x] \to \mathbb{K}[a], \quad \text{with } \Phi_a(x) = a \text{ and } \Phi_a(k) \text{ for all } k \in \mathbb{K}..$$

So $\Phi_a(f) = f(a)$.

(h) *The unique zero or monic polynomial $m_a = m^{\mathbb{K}}(a) \in \mathbb{K}[x]$ with* $\ker \Phi_a = \mathbb{K}[x]m_a$ *is called the* minimal polynomial *of a over $\mathbb{K}$.*

(i) a is called algebraic *over $\mathbb{K}$ if $m_a \neq 0_F$.*

(j) The extension $\mathbb{K} \subseteq F$ is called algebraic *if all $b \in F$ are algebraic over $\mathbb{K}$.*

(k) a is called transcendental *over $\mathbb{K}$ if $m_a = 0_F$.*

Lemma 4.1.2. *Let $\mathbb{K} \leq F$ be an extension and $a \in F$. Then one of the following holds*

1. *Φ_a is not 1-1,* $\dim_{\mathbb{K}} \mathbb{K}[a] = \deg m_a$ *is finite, m_a is monic and irreducible, $\mathbb{K}[a] = \mathbb{K}(a)$ is a field, a is algebraic over $\mathbb{K}$, and $(a^i)_{0 \leq i < \deg m_a}$ is a basis for $K[a]$.*

2. *Φ_a is an isomorphism,* $\dim_{\mathbb{K}} \mathbb{K}[a] = \infty$, *$m_a = 0_{\mathbb{K}}$, a is not invertible in $\mathbb{K}[a]$, a is transcendental over $\mathbb{K}$, $(a^i)_{i \in \mathbb{N}}$ is a basis for $\mathbb{K}[a]$.*

Proof. Since F is an integral domain, $\mathbb{K}[a]$ is an integral domain. Clearly Φ_a is onto and so $\mathbb{K}[x]/\mathbb{K}[x]m_a \cong \mathbb{K}[x]/\ker \Phi_a \cong \mathbb{K}[a]$. Thus by 2.5.9 $\mathbb{K}[x]m_a$ is a prime ideal.

Suppose first that $m_a \neq 0$. Then a is algebraic over $\mathbb{K}[a]$ and Φ_a is not 1-1. Note that by 2.5.9 m_a is a prime. By Example 2.6.2(2), $\mathbb{K}[x]$ is am Euclidean domain and so also a PID. So we conclude from 2.5.17 that m_a is irreducible and $\mathbb{K}[a] \cong \mathbb{K}[x]/\mathbb{K}[x]m_a$ is a field. Let $f \in \mathbb{K}[x]$. As $\mathbb{K}[x]$ is a Euclidean domain, $f \equiv g \pmod{m_a}$ for a unique polynomial $g \in K[x]$ with $\deg g < \deg m_a$. Also g is a unique $\mathbb{K}$-linear combination of $(x^i)_{0 \leq i < \deg m_a}$ and so $(x^i + \mathbb{K}[x]m_a)_{0 \leq i < \deg m_a}$ is a basis for $\mathbb{K}[x]/\mathbb{K}[x]m_a$. Hence $(a^i)_{0 \leq i < \deg m_a}$ is basis for $\mathbb{K}[a]$. Thus (1) holds.

Suppose next that $m_a = 0$. Then a is transcendental. Moreover, Φ_a is 1-1 and so an isomorphism. Since x is not invertible in $\mathbb{K}[x]$ and $(x^i, i \in \mathbb{N})$ is a basis for $\mathbb{K}$ we conclude that a is not invertible in $\mathbb{K}[a]$ and $(a^i, i \in \mathbb{N})$ is a basis for $\mathbb{K}[a]$. So (2) holds in this case. □

Lemma 4.1.3. *Any finite extension is algebraic.*

Proof. Let $\mathbb{K} \leq F$ be an extension and $a \in F$. Then $\dim_{\mathbb{K}} \mathbb{K}[a] \leq \dim_{\mathbb{K}} F < \infty$ and 4.1.2 implies that a is algebraic over $\mathbb{K}$. □

Lemma 4.1.4. *(a) Let R be a ring and $(S_i)_{i \in I}$ a non-empty family of subring (subfields) of R. Suppose that for each $i, j \in I$ there exists $k \in I$ with $S_i \cup S_j \subseteq S_k$. Then $\bigcup_{i \in I} S_i$ is a subring (subfield) of R.*

(b) Let S be a ring, R a subring of S and $I \subseteq S$. Then

$$R[I] = \bigcup \{R[J] \mid J \subseteq I, J \textit{ is finite}\}.$$

(c) Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $I \subseteq \mathbb{F}$. Then

$$\mathbb{K}(I) = \bigcup \{\mathbb{K}(J) \mid J \subseteq I, J \textit{ is finite}\}.$$

Proof. (b) Let $T = \bigcup_{i \in I} S_i$. Let $a, b \in T$. Then $a \in S_i$ and $b \in S_j$ for some $i, j \in I$. By assumption, $S_i \cup S_j \subseteq S_k$ for some $k \in I$. Then $-a$, $a + b$, ab and (if $a \neq 0$ and S_i is a field) a^{-1} all are contained in S_k and so in T. Since $I \neq \varnothing$ and 0 is contained in any subring of R, $0 \in T$. So T is indeed a subring (subfield) of R.

(c) Let J, K be finite subsets of I. Then $J \cup K$ is finite and $R[J] \cup R[K] \subseteq R[J \cup K]$. Thus (c) follows from (b).

(a) also follows from (b). □

Lemma 4.1.5. *Let R be a ring. M an R-module and S a subring of R. Let $r = (r_i)_{i \in I}$ be a family of elements in R and $m = (m_j)_{j \in J}$ family of elements in M. Put $w = (r_i m_j)_{(i,j) \in I \times J}$.*

(a) If $R = \langle r \rangle_S$ and $M = \langle m \rangle_R$, then $M = \langle w \rangle_S$

(b) If r is linearly independent over S and m is linearly independent over R, then w is linearly independent over S.

(c) If r is an S-basis for R and m is an R-basis for M, then w is an S-basis for M.

Proof. (a) $M = \langle m \rangle_R = \langle Rm \rangle = \langle \langle S r \rangle m \rangle = \langle S w \rangle = \langle w \rangle_S$.

(b) Suppose that $\sum_{(i,j) \in I \times J} s_{ij} r_i m_j = 0$, for some $s \in S_{I \times J}$.

$$\sum_{j \in J} \left(\sum_{i \in I} s_{ij} r_i \right) m_j = 0$$

Since m is linearly independent over R, we conclude $\sum_{i \in I} s_{ij} r_i = 0$ for all j in J. As r is linearly independent over S we get $s_{ij} = 0$ for all $(i, j) \in I \times J$. Thus (b) holds.

(c) follows from (a) and (b). □

Corollary 4.1.6. *Let $\mathbb{K} \leq \mathbb{E}$ be a field extension.*

(a) Let V a vector space over $\mathbb{E}$. Then

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} \mathbb{E} \cdot \dim_{\mathbb{E}} V.$$

(b) Let $\mathbb{K} \leq \mathbb{E}$ be a field extension and $\mathbb{E} \leq F$ an extension. Then

$$\dim_{\mathbb{K}} F = \dim_{\mathbb{K}} \mathbb{E} \cdot \dim_{\mathbb{E}} F.$$

(c) If $\mathbb{E} \leq F$ are finite, also $\mathbb{K} \leq F$ is finite.

Proof. (a) follows from 4.1.5(c). (b) is a special case of (a). (c) follows from (b). □

Lemma 4.1.7. *Let $\mathbb{K} \leq F$ be an extension, let $a \in F$ be algebraic over $\mathbb{K}$ and let $f \in \mathbb{K}[x]$.*

(a) $f(a) = 0$ if and only if $m_a \mid f$ in $\mathbb{K}[x]$.

(b) If f is irreducible then $f(a) = 0$ if and only if $f \sim m_a$ in $\mathbb{K}[x]$. That is if and only if $f = k m_a$ for some $k \in \mathbb{K}^\sharp$.

(c) m_a is the unique monic irreducible polynomial in $\mathbb{K}[x]$ with a as a root.

Proof. (a) Since $f(a) = \Phi_a(f)$, $f(a) = 0$ if and only if $a \in \ker \Phi_a$. Since $\ker \Phi_a = \mathbb{K}[x]m_a$, this holds if and only if $m_a \mid f$.

(b) Let f be irreducible with $f(a) = 0$, then $m_a \mid f$. Since f is irreducible we get $m_a \sim f$. By 2.5.5 this means $f = km_a$ for some unit k in $\mathbb{K}[x]$. It is easy to see that the units in $\mathbb{K}[x]$ are exactly the non-zero constant polynomials. So $k \in \mathbb{K}^\sharp$.

(c) If in addition f is monic, then since also m_a is monic we conclude $k = 1$ and $f = m_a$. □

Lemma 4.1.8. *Let $\mathbb{K} \leq \mathbb{E}$ be a field extension, $\mathbb{E} \leq F$ an extension and $b \in F$. If b is algebraic over $\mathbb{K}$, then b is algebraic over $\mathbb{E}$ and $m_b^{\mathbb{E}}$ divides $m_b^{\mathbb{K}}$ in $\mathbb{E}[x]$.*

Proof. Note that $m_b^{\mathbb{K}}(b) = 0$ and $m_b^{\mathbb{K}} \in \mathbb{E}[x]$. So by 4.1.7 $m_a^{\mathbb{E}}$ divides $m_b^{\mathbb{K}}$ in $\mathbb{E}[x]$. Since b is algebraic over $\mathbb{K}$, $m_b^{\mathbb{K}} \neq 0$ and so also $m_b^{\mathbb{E}} \neq 0$. Hence b is algebraic over $\mathbb{E}$. □

Lemma 4.1.9. *Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x]$ a non-zero polynomial.*

Then there an integer m with $0 \leq m \leq \deg f$, $a_1, \dots a_m \in F$ and $q \in \mathbb{F}[x]$ such that

(a) $f = q \cdot (x - a_1) \cdot (x - a_2) \cdot (x - a_m)$.

(b) *q has no roots in F.*

(c) *$\{a_1, a_2, \dots a_m\}$ is the set of roots of f.*

In particular, the number of roots of f is at most $\deg f$.

Proof. Suppose that f has no roots. Then the theorem holds with $q = f$ and $m = 0$.

The proof is by induction on $\deg f$. Since polynomials of degree 0 have no roots, the theorem holds if $\deg f = 0$.

Suppose now that theorem holds for polynomials of degree k and let f be a polynomial of degree $k + 1$. If f has no root we are done by the above. So suppose f has a root a. By 2.6.3 there exists $g, r \in \mathbb{F}[x]$ with $f = g \cdot (x - a) + t$ and $\deg r < \deg(x - a) = 1$. Thus $r \in \mathbb{F}$ and $0 = f(a) = g(a) \cdot (a - a) + r$. Thus $r = 0$ and

$$(*) \qquad f = g \cdot (x - a)$$

Then $\deg g = k$ and so by the induction assumption there exists an integer n with $0 \leq n \leq \deg g$, $a_1, \dots a_n \in F$ and $q \in F[x]$ such that

(i) $g = q \cdot (x - a_1) \cdot (x - a_2) \cdot (x - a_n)$

(ii) q has no roots in F.

(iii) $\{a_1, a_2, \dots a_n\}$ is the set of roots of g.

Put $m = n + 1$ and $a_m = a$. From $f = g \cdot (x - a) = g \cdot (x - a_m)$ and (i) we conclude that (a) holds. By (ii), (b) holds.

Let $b \in F$. Then b is a root if and only if $f(b) = 0_R$ and so by (*) if and only $g(b)(b - a) = 0_F$. Since F is an integral domain this holds if and only if $g(b) = 0$ or $b - a = 0_F$. From $a = a_m$ and (iii) we conclude that the roots of f are $\{a_1, a_2 \dots, a_m\}$. So also (c) holds. □

Definition 4.1.10. *Let $\mathbb{K}$ be a field and $f \in \mathbb{K}[x]$. We say that f* splits *over $\mathbb{K}$ if*

$$f = k_0(x - k_1)(x - k_2)\dots(x - k_n)$$

for some $n \in \mathbb{N}$ and $k_i \in \mathbb{K}, 0 \leq i \leq n$..

Lemma 4.1.11. *Let $\mathbb{K}$ be a field and $f \in K[x]^\sharp$.*

(a) Suppose $\mathbb{K} \leq \mathbb{E}$ is a field extension, $f \in \mathbb{K}[x]$ is irreducible and $\mathbb{E} = \mathbb{K}[a]$ for some root a of f in $\mathbb{E}$, then the map

$$\mathbb{K}[x]/f\mathbb{K}[x] \to \mathbb{E}, h + f\mathbb{K}[x] \to h(a)$$

is ring isomorphism.

(b) If f is not constant, then there exists a finite field extension $\mathbb{K} \leq \mathbb{E}$ such that f has a root in $\mathbb{E}$ and $\dim_{\mathbb{K}} \mathbb{E} \leq \deg f$.

(c) There exists a finite field extension $\mathbb{K} \leq \mathbb{F}$ such that f splits over and $\dim_{\mathbb{K}} \mathbb{F} \leq (\deg f)!$.

Proof. (a) By 4.1.7(b), $f \sim m_a$. Thus $\ker \Phi_a = m_a\mathbb{K}[x]$. Also $h(a) = \Phi_a(h)$ and (a) follows from Isomorphism Theorem of Rings.

(b) Let g be an irreducible divisor of f in $\mathbb{K}[x]$. Put $\mathbb{E} = \mathbb{K}[x]/g\mathbb{K}[x]$. Then $\mathbb{E}$ is a field For $h \in \mathbb{K}[x]$ put $\overline{h} = h + g\mathbb{K}[x] \in \mathbb{E}$. Note that the map $h \to \overline{h}$ is a ring homomorphism. Put $a = \overline{x}$. We identify $k \in \mathbb{K}$ with $\overline{k} \in \mathbb{E}$. Then $\mathbb{K}$ is a subfield of $\mathbb{E}$ and $(a^i)_{i=0}^{\deg g - 1}$ is a $\mathbb{K}$ basis for $\mathbb{E}$. Thus $\dim_{\mathbb{K}} \mathbb{E} = \deg g \leq \deg f$. Let $f = \sum_{i=0}^n k_i x^i$ with $k_i \in \mathbb{K}$. Then

$$f(a) = \sum_{i=0}^n k_i a^i = \sum_{i=0}^n \overline{k_i}\overline{x}^i = \overline{\sum_{i=0}^n k_i x^i} = \overline{f}.$$

Since $g \mid f$, $f \in g\mathbb{K}[x]$ and so $\overline{f} = 0_{\mathbb{E}}$. Thus $f(a) = 0_{\mathbb{E}}$ and a is a root of f in $\mathbb{E}$.

(c) Let $\mathbb{E}$ be as in (b) and e a root of f in $\mathbb{E}$. Then $f = (x - e)g$ for some $g \in \mathbb{E}[x]$ with $\deg g = \deg f - 1$. By induction on $\deg f$ there exists a field extension $\mathbb{E} \leq \mathbb{F}$ such that g splits over $\mathbb{F}$ and $\dim_{\mathbb{E}} \mathbb{F} \leq (\deg g)! = (\deg f - 1)!$. Then f splits over $\mathbb{F}$ and

$$\dim_{\mathbb{K}} \mathbb{F} = \dim_{\mathbb{K}} \mathbb{E} \cdot \dim_{\mathbb{E}} \mathbb{F} \leq (\deg f - 1)! \deg f = \deg f!.$$

□

Example 4.1.12. Let $f = x^2 + 1 \in \mathbb{R}[x]$. Then f has no root in $\mathbb{R}$ and so is irreducible over $\mathbb{R}$. Thus $\mathbb{E} = \mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x]$ is a field. For $h \in \mathbb{R}[x]$ let $\overline{h} = h + f\mathbb{R}[x] \in \mathbb{E}$. We also identify $r \in \mathbb{R}$ with $\overline{r}$ in $\mathbb{E}$. Put $i = \overline{x}$. Then i is a root of f in $\mathbb{E}$ and so $i^2 + 1 = 0$ and $i^2 = -1$. Moreover $1, i$ is an $\mathbb{R}$ basis for $\mathbb{F}$. Let $a, b, c, d \in \mathbb{R}$. Then $(a + bi) + (c + di) = (a + b) + (c + d)i$ and

$$(a + bi)(c + di) = ac + bdi^2 + (ad + bc)i = (ac - bd) + (ad + bc)i$$

Hence $\mathbb{E}$ is isomorphic the field $\mathbb{C}$ of complex numbers.

Definition 4.1.13. *Let $\mathbb{K} \leq F$ be an extension. Then*

$$\mathbb{A}(\mathbb{K}, F) = \{b \in F \mid b \text{ is algebraic over } \mathbb{K}\}$$

Lemma 4.1.14. *Let $\mathbb{K} \leq F$ be an extension and $A \subseteq F$ be a set of elements in F algebraic over $\mathbb{K}$.*

(a) If A is finite, $\mathbb{K} \leq \mathbb{K}[A]$ is a finite field extension

(b) $\mathbb{K} \leq \mathbb{K}[A]$ is an algebraic field extension.

(c) $\mathbb{A}(\mathbb{K}, F)$ is a subfield of F.

Proof. (a) By induction on $|A|$. If $|A| = 0$, $\mathbb{K}[A] = \mathbb{K}$. So suppose $A \neq \varnothing$ and let $a \in A$. Put $B = A \smallsetminus \{a\}$. By induction $\mathbb{K} \leq \mathbb{K}[B]$ is finite field extension. As a is algebraic over $\mathbb{K}$, a is algebraic over $\mathbb{K}[B]$ (see 4.1.8) Thus by 4.1.2 $\mathbb{K}[B] \leq \mathbb{K}[B][a]$ is finite field extension. Hence by 4.1.6(b) also $\mathbb{K} \leq \mathbb{K}[B][a]$ is finite. Since $\mathbb{K}[B][a] = \mathbb{K}[A]$ we conclude that (a) holds.

(b) Let $b \in \mathbb{K}[A]$. By 4.1.4(b), $b \in \mathbb{K}[B]$ for some finite $B \subseteq A$. By (a) $\mathbb{K} \leq \mathbb{K}[B]$ is finite and so also algebraic (4.1.6(b)). So b is algebraic over $\mathbb{K}$.

(c) Follows from (b) applied with A the set of all elements in F which are algebraic over $\mathbb{K}$. □

Proposition 4.1.15. *Let $\mathbb{K} \leq \mathbb{E}$ and $\mathbb{E} \leq \mathbb{F}$ be algebraic field extensions. Then $\mathbb{K} \leq \mathbb{F}$ is algebraic.*

Proof. Let $b \in F$ and $m = m_b^{\mathbb{E}}$. Let $m = \sum_{i=0}^n e_i x^i$ and $A = \{e_0, e_2 \ldots, e_n\}$. Then A is a finite subset of $\mathbb{E}$.

Since $\mathbb{K} \leq \mathbb{E}$ is algebraic, 4.1.14 implies that $\mathbb{K} \leq \mathbb{K}[A]$ is finite. Also $m \in \mathbb{K}[A][x]$ and so b is algebraic over $\mathbb{K}[A]$. Hence (by 4.1.2) $\mathbb{K}[A] \leq \mathbb{K}[A][b]$ is finite. By 4.1.5c, $\mathbb{K} \leq \mathbb{K}[A][b]$ is finite and so by 4.1.6 also algebraic. Thus b is algebraic over $\mathbb{K}$. □

Proposition 4.1.16. *Let $\mathbb{K}$ be a field and P a set of non constant polynomials over $\mathbb{K}$. Then there exists an algebraic extension $\mathbb{K} \leq \mathbb{F}$ such that each $f \in P$ has a root in $\mathbb{F}$.*

Proof. Suppose first that P is finite. Put $f = \prod_{g \in P} g$. 4.1.11(c), there exists a finite extension $\mathbb{E}$ of $\mathbb{K}$ such that f splits over $\mathbb{E}$. Then each $g \in P$ has a root in $\mathbb{E}$.

In the general case, let $R = \mathbb{K}[X_P]$ be the polynomial ring of P over $\mathbb{K}$. Let I be the ideal in R generated by $f(x_f), f \in P$.

Suppose for a contradiction that that $I = R$. Then $1 \in I$ and so $1 = \sum_{f \in P} r_f f(x_f)$ for some $r \in R_P$. Let $Q = \{f \in P \mid r_f \neq 0\}$. Then

$$(*) \qquad 1 = \sum_{f \in Q} r_f f(x_f)$$

Then by the finite case there exists a field extension $\mathbb{K} \leq \mathbb{E}$ such that each $f \in Q$ has a root $e_f \in \mathbb{E}$. For $f \in P \in Q$ let $e_f \in \mathbb{E}$ be arbitray.

$$\Phi : \mathbb{K}[X_P] \to \mathbb{E}$$

be the unique ring homomorphism with $\Phi(x_f) = e_f$ for $f \in P$ and $\Phi(k) = k$ for all $k \in \mathbb{K}$. Since $f(x_f) = \sum_{i=0}^{n} k_i x_f^i$ for some $k_i \in \mathbb{K}$ we have $\Phi(f(x_f)) = \sum_{i=0}^{n} k_i e_f^i = f(e_f) = 0$ for all $f \in Q$. So applying Φ to (*) we get

$$1 = \Phi(1) = \sum_{f \in Q} \Phi(r_f) f(e_f) = 0$$

a contradiction.

Hence $I \neq R$ and by 2.4.18 I is contained in a maximal ideal M of R. Put $\mathbb{F} = R/M$. Then by 2.4.21 $\mathbb{F}$ is a field. Since $M \neq R$, M contains no units. Thus $\mathbb{K} \cap M = 0$. Thus the map $\mathbb{K} \to \mathbb{F}, k \to k + M$ is a 1-1 ring homomorphism. So we may view $\mathbb{K}$ as a subfield of $\mathbb{F}$ by identifying k with $k + M$. Put $a_f = x_f + M$. Then $f(a_f) = f(x_f) + M$. But $f(x_f) \in I \subseteq M$ and so $f(a_f) = M = 0_{\mathbb{F}}$. □

Lemma 4.1.17. *Let $\mathbb{K}$ be a field. Then the following statements are equivalent.*

(a) Every non-constant polynomial over $\mathbb{K}$ has a root in $\mathbb{K}$.

(b) Every polynomial over $\mathbb{K}$ splits over $\mathbb{K}$.

(c) Every irreducible polynomial in $\mathbb{K}[x]$ has degree one.

(d) $\mathbb{K}$ has no proper algebraic extension (that is if $\mathbb{K} \leq F$ is an algebraic extension, then $\mathbb{K} = F$.)

(e) $\mathbb{K}$ has no proper finite extension (that is if $\mathbb{K} \leq F$ is a finite extension, then $\mathbb{K} = F$.)

Proof. (a) $\Longrightarrow$ (b): Let $f \in \mathbb{K}[x]$. If $\deg f = 0$, f splits. So suppose $\deg f > 0$. Then by (a), f has root $a \in \mathbb{K}$ and so $f = (x - a)g$ for some $g \in \mathbb{K}[x]$. By induction on $\deg f$, g splits over $\mathbb{K}$ and so also f splits over $\mathbb{K}$.

(b) $\Longrightarrow$ (c): Let f be irreducible. Since f is irreducible, f is neither 0 nor a unit. So $\deg f > 0$. If (b) holds, f splits over $\mathbb{K}$ and so is divisible by some $x - a$, $a \in \mathbb{K}$. Since f is irreducible, $f \sim x - a$ and so $\deg f = \deg x - a = 1$.

(c) $\Longrightarrow$ (d): Let $\mathbb{K} \leq \mathbb{E}$ be algebraic and $e \in \mathbb{E}$. Since $m_e^{\mathbb{K}}$ irreducible, (c) implies that $m_e^{\mathbb{K}}$ has degree 1. Since $m_e^{\mathbb{K}}$ is monic this gives $m_e^{\mathbb{K}} = x - a$ for some $a \in \mathbb{K}$. Since e is a root of $m_e^{\mathbb{K}}$, $e = a \in \mathbb{K}$. Thus $\mathbb{K} = \mathbb{E}$.

(d) $\Longrightarrow$ (e): Just observe that by 4.1.6(a), every finite extension is algebraic.

(e) $\Longrightarrow$ (a): Let $f \in \mathbb{K}$. By 4.1.11 f has a root a in some finite extension $\mathbb{E}$ of K. By assumption $\mathbb{E} = \mathbb{K}$. So $a \in \mathbb{K}$ and (a) holds. □

Definition 4.1.18. *Let $\mathbb{K}$ be a field.*

(a) $\mathbb{K}$ is algebraically closed *if $\mathbb{K}$ fulfills one (and so all) of four equivalent statement in 4.1.17.*

(b) An algebraic closure *of $\mathbb{K}$ is a algebraically closed, algebraic extension of $\mathbb{K}$.*

Lemma 4.1.19. *Let $\mathbb{K} \leq \mathbb{E}$ be an algebraic field extension. Then the following two statements are equivalent.*

(a) $\mathbb{E}$ is an algebraic closure of $\mathbb{K}$.

(b) Every polynomials over $\mathbb{K}$ splits over $\mathbb{E}$.

Proof. If $\mathbb{E}$ is algebraic closed, every polynomial over $\mathbb{E}$ and so also every polynomial over $\mathbb{K}$ splits over $\mathbb{E}$. Thus (a) implies (b).

So suppose (a) holds. Let $\mathbb{F}$ be an algebraic extension of $\mathbb{E}$. Let $a \in \mathbb{F}$. Since $\mathbb{K} \leq \mathbb{E}$ and $\mathbb{E} \leq \mathbb{K}$ are algebraic we conclude from 4.1.15 that $\mathbb{K} \leq \mathbb{F}$ is algebraic. Thus $m_a^{\mathbb{K}}$ is not zero and has a as a root. By assumption, $m_a^{\mathbb{K}}$ splits over $\mathbb{E}$ and so $a \in \mathbb{E}$. Thus $\mathbb{E} = \mathbb{F}$. Hence by 4.1.17 and definition, $\mathbb{E}$ is algebraically closed. □

Theorem 4.1.20. *Every field has an algebraic closure.*

Proof. Let $\mathbb{K}$ be a field and P the set of non-constant polynomial in $\mathbb{K}[x]$. Define

$$\mathcal{F}\mathbb{K} = \{\mathbb{K}[X_P]/I \mid I \text{ a maximal ideal in } \mathbb{K}[X_P] \text{ with } f(x_f) \in I \text{ for all } f \in P\}$$

By (the proof of) 4.1.16 if $\mathbb{F} \in \mathcal{F}\mathbb{K}$ then $\mathbb{K} \leq \mathbb{F}$ is a algebraic field extension and each non-zero polynomial in $\mathbb{K}[x]$ has a root in $\mathbb{F}$. By A.4.11 there exists family of fields $(\mathbb{K}_i)_{i \in \mathbb{N}}$ with $\mathbb{K}_0 = \mathbb{K}$ and $\mathbb{K}_{i+1} = \mathcal{F}\mathbb{K}$. Let $\mathbb{E} = \bigcup_{i=0}^{\infty} \mathbb{K}_i$. By A.6.6 $\mathbb{E}$ is a field. By 4.1.15 and induction each $\mathbb{K}_i$ is algebraic over $\mathbb{K}_0$. So also $\mathbb{K}_0 \leq \mathbb{E}$ is algebraic. Let $f \in \mathbb{E}[x]$. Then $f \in \mathbb{K}_i[x]$ for some i. Hence f has a root in $\mathbb{K}_{i+1}$ and so in $\mathbb{E}$. Thus by 4.1.17 $\mathbb{E}$ is algebraically closed. □

Definition 4.1.21. *Let $\mathbb{K}$ be a field and P a set of polynomials over $\mathbb{K}$. A* splitting field *for P over $\mathbb{K}$ is an extension $\mathbb{E}$ of $\mathbb{K}$ such that*

(a) Each $f \in P$ splits over $\mathbb{E}$.

(b) $\mathbb{E} = \mathbb{K}[A]$, where $A := \{a \in \mathbb{E} \mid f(a) = 0$ for some $0 \neq f \in P\}$.

Corollary 4.1.22. *Let $\mathbb{K}$ be a field and P a set of polynomials over $\mathbb{K}$. Then there exists a splitting field for P over $\mathbb{K}$.*

Proof. Let $\overline{\mathbb{K}}$ be a algebraic closure for $\mathbb{K}$, $B := \{a \in \bar{\mathbb{K}} \mid f(a) = 0 \text{ for some } f \in P\}$ and put $\mathbb{E} = \mathbb{K}[B]$. Then $\mathbb{E}$ is a splitting field for P over $\mathbb{K}$. □

Corollary 4.1.23. *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension. Then $\mathbb{F}$ is an algebraic closure of $\mathbb{K}$ if and only if $\mathbb{F}$ is the splitting field of $\mathbb{K}[x]$ over $\mathbb{K}$.*

Proof. Suppose $\mathbb{F}$ is an algebraic closure of $\mathbb{K}$. Then each $f \in \mathbb{K}[x]$ splits over $\mathbb{K}$. Also $\mathbb{K} \leq \mathbb{F}$ is algebraic and so each $a \in \mathbb{F}$ is a root of some noon-zero $f \in \mathbb{K}[x]$. So $\mathbb{F}$ is the splitting field of $\mathbb{K}[x]$ over $\mathbb{F}$.

Now suppose that $\mathbb{F}$ is a splitting field of $\mathbb{K}[x]$ over $\mathbb{K}$. Then 4.1.19 shows that $\mathbb{F}$ is an algebraic closure of $\mathbb{K}$. □

4.2 Splitting fields, Normal Extensions and Separable Extensions

Lemma 4.2.1. *Let $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ be a 1-1 homomorphism of fields. Then*

(a) There exists a unique homomorphism $\tilde{\phi} : \mathbb{K}_1[x] \to \mathbb{K}_2[x]$ with $\tilde{\phi}(k) = \phi(k)$ and $\tilde{\phi}(x) = x$.

(b) $\tilde{\phi}\left(\sum_{i=0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} \phi(a_i)x^i$ for all $\sum_{i=0} a_i x^i \in \mathbb{K}_1[x]$

(c) $\tilde{\phi}$ is 1-1 and if ϕ is an isomorphism, $\tilde{\phi}$ is an isomorphism.

We will usually just write $\tilde{\phi}$ for ϕ.

Proof. (a) and (b) follow from 2.2.19. (c) is readily verified. □

Lemma 4.2.2. *Let $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ be an isomorphism of fields and for $i = 1$ and 2 let $\mathbb{K}_i \leq \mathbb{E}_i$ be a field extension. Let $f_1 \in \mathbb{K}_1[x]$ be irreducible and put $f_2 = \phi(f_1)$. Suppose e_i is a root of f_i in $\mathbb{K}_i$. Then there exists a unique isomorphism $\psi : \mathbb{K}_1[e_1] \to \mathbb{K}_2[e_2]$ with $\psi\mid_{\mathbb{K}_1} = \phi$ and $\psi(e_1) = e_2$.*

Proof. Using 4.1.11(a) we have the following three isomorphism:

$$\begin{array}{ccccccc}
\mathbb{K}_1[e_1] & \cong & \mathbb{K}_1[x]/f_1\mathbb{K}_1[x] & \cong & \mathbb{K}_2[x]/f_2\mathbb{K}_2[x] & \cong & \mathbb{K}_2[e_2] \\
g(e_1) & \to & g + f_1\mathbb{K}_1[x] & \to & \phi(g) + f_2\mathbb{K}_2[x] & \to & \phi(g)(e_2)
\end{array}$$

Let ψ be the composition of these three isomorphism. Then

$$\psi : e_1 \to x + f_1\mathbb{K}_1[x] \to x + f_2\mathbb{K}_2[x] \to e_2$$

and for $k \in \mathbb{K}_1$,

$$\psi : k \to k + f_1\mathbb{K}_1[x] \to \phi(k) + f_2\mathbb{K}_2[x] \to \phi(k)$$

This shows the existence of ψ. If $\tilde{\psi}$ is any such ring homomorphism then

$$\tilde{\psi}\left(\sum_{i=0}^{\deg f - 1} a_i e_1^i\right) = \sum_{i=0}^{\deg f - 1} \phi(a_i) e_2^i$$

and so ψ is unique. □

Definition 4.2.3. *Let $\mathbb{K}$ be a field and F and E extensions of $\mathbb{K}$.*

(a) A $\mathbb{K}$-homomorphism *from F to E is a $\mathbb{K}$-linear ring homomorphism from F to E. $\mathbb{K}$-isomorphisms and $\mathbb{K}$-automorphisms are defined similarly.*

(b) Aut$F$ *is the set of automorphism of F and* Aut$_{\mathbb{K}}F$ *is the set of $\mathbb{K}$-automorphism of $\mathbb{F}$.*

(c) $\mathbb{E}$ is an intermediate field of the extension $\mathbb{K} \leq F$ if $\mathbb{K}$ is a subfield of $\mathbb{E}$ and $\mathbb{E}$ is a subfield of F.

Lemma 4.2.4. *Let $\mathbb{F}$ be a field, E an integral domain and $\phi : \mathbb{F} \to E$ a non-zero ring homomorphism. Then ϕ is 1-1 and $\phi(1_{\mathbb{F}}) = 1_{\mathbb{E}}$.*

Proof. Since ϕ is non-zero, $\ker\phi \neq 0$. Since $\ker\phi$ is an ideal and $\mathbb{F}$ has no proper ideals, $\ker\phi = 0$ and so ϕ is 1-1.

We have

$$\phi(1_{\mathbb{F}})\phi(1_F) = \phi(1_{\mathbb{F}} 1_{\mathbb{F}}) = \phi(1_{\mathbb{F}}) = 1_{\mathbb{E}}\phi(1_{\mathbb{F}}).$$

Since ϕ is 1-1, $\phi(1_{\mathbb{F}}) \neq 0_{\mathbb{E}}$. Since E is an integral domain the Cancellation Law implies $\phi(1_{\mathbb{F}}) = 1_{\mathbb{E}}$ □

Lemma 4.2.5. *Let $\mathbb{K} \leq \mathbb{F}$ and $\mathbb{K} \leq \mathbb{E}$ be field extensions and $\phi : \mathbb{F} \to \mathbb{K}$ a non-zero ring homomorphism. Then ϕ is $\mathbb{K}$-linear if and only if $\phi\mid_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$.*

Proof. Let $k \in \mathbb{K}$ and $a \in \mathbb{F}$. If ϕ is $\mathbb{K}$-linear , then

$$\phi(k) = \phi(k1_F) = k\phi(1_F) = k1_E = k$$

and if $\phi\mid_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$, then

$$\phi(ka) = \phi(k)\phi(a) = k\phi(a).$$

□

Lemma 4.2.6. *Let $\mathbb{K} \leq F$ be a field extension. Then $\mathrm{Aut}(F)$ is a subgroup of $\mathrm{Sym}(F)$ and $\mathrm{Aut}_{\mathbb{K}}(F)$ is a subgroup of $\mathrm{Aut}(F)$.*

Proof. Readily verified. □

Lemma 4.2.7. *Let $\mathbb{K}$ be a field field and P a set of polynomials. Let $\mathbb{E}_1$ and $\mathbb{E}_2$ be splitting fields for P over $\mathbb{K}$*

(a) For $i = 1, 2$ let $\mathbb{L}_i$ be an intermediate field of $\mathbb{K} \leq \mathbb{E}_i$ and let $\delta : \mathbb{L}_1 \to \mathbb{L}_2$ be a $\mathbb{K}$-isomorphism. Then there exists a $\mathbb{K}$-isomorphism $\psi : \mathbb{E}_1 \to \mathbb{E}_2$ with $\psi|_{\mathbb{L}_i} = \delta$.

(b) $\mathbb{E}_1$ and $\mathbb{E}_2$ are $\mathbb{K}$-isomorphic.

(c) Let $f \in \mathbb{K}[x]$ be irreducible and suppose that, for $i = 1$ and 2, e_i is a root of f in $\mathbb{E}_i$. Then there exists a $\mathbb{K}$-isomorphism $\psi : \mathbb{E}_1 \to \mathbb{E}_2$ with $\psi(e_1) = \psi(e_2)$.

(d) Let $f \in \mathbb{K}[x]$ be irreducible and let e and d be roots of f in $\mathbb{E}_1$. Then there exists $\psi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)$ with $\psi(e) = d$.

(e) Any two algebraic closures of $\mathbb{K}$ are $\mathbb{K}$-isomorphic.

Proof. Let $\mathcal{M}$ be the set of all $\mathbb{K}$-linear isomorphism $\phi : \mathbb{F}_1 \to \mathbb{F}_2$ where, for $i = 1$ and 2, $\mathbb{F}_i$ is an intermediate field of $\mathbb{K} \leq \mathbb{E}_i$. Order $\mathcal{M}$ by $(\phi : \mathbb{F}_1 \to \mathbb{F}_2) \leq (\psi : \mathbb{L}_1 \to \mathbb{L}_2)$ if $\mathbb{F}_1 \subseteq \mathbb{L}_1$ and $\psi\mid_{\mathbb{F}_1} = \phi$. Let $\mathcal{M}^* = \{\phi \in \mathcal{M} \mid \delta \leq \phi\}$. Since $\delta \in \mathcal{M}^*$, $\mathcal{M}^*$ is not empty.

It is easy to verify that $\leq$ is a partial ordering on $\mathcal{M}$. Let $\mathcal{C} = \{\psi_s : \mathbb{F}_{s1} \to \mathbb{F}_{s2} \mid s \in S\}$ be a chain in $\mathcal{M}^*$. Define $\mathbb{F}_i = \bigcup_{s\in S} \mathbb{F}_{si}$ and define $\phi : \mathbb{F}_1 \to \mathbb{F}_2$ by $\phi(a) = \phi_s(a)$ if $s \in S$ with $a \in \mathbb{F}_{s1}$.

It is straightforward to verify that $\mathbb{F}_i$ is a field, ϕ is well-defined and ϕ is a isomorphism. Moreover, $\phi_s \leq \phi$ for all $s \in S$ and so ϕ is an upper bound for $\mathcal{C}$.

Zorn's Lemma A.3.8 implies that $\mathcal{M}^*$ has a maximal element $\phi : \mathbb{F}_1 \to \mathbb{F}_2$. It remains to show that $\mathbb{F}_i = \mathbb{E}_i$. For this put

$$A_i = \{e_i \in \mathbb{E}_i \mid f(e_i) = 0 \text{ for some } 0 \neq f \in P\}$$

By definition of a splitting field, $\mathbb{E}_i = \mathbb{K}[A_i]$. Since $\mathbb{K} \leq \mathbb{F}_i \leq \mathbb{E}_i$ we just need to show that $A_i \subseteq \mathbb{F}_i$.

So let $e_1 \in A_1$ and $0 \neq f \in P$ with $f(e_1) = 0$. Let f_1 be an irreducible divisor of f in $\mathbb{F}_1[x]$ with $f_1(e_1) = 0$. Put $f_2 = \phi(f_1)$. Since f_1 divides f in $\mathbb{F}_1[x]$, f_2 divides $\phi(f)$ in $\mathbb{F}_2[x]$. Since $f \in \mathbb{K}[x]$ and ϕ is a $\mathbb{K}$-homomorphism, $\phi(f) = f$. Thus f_2 divides f in $\mathbb{F}_2[x]$. Since f splits over $\mathbb{E}_2$, also f_2 splits over $\mathbb{E}_2$ and so f_2 has a root $e_2 \in \mathbb{E}_2$. By 4.2.2 there exists a field isomorphism $\psi : \mathbb{F}_1[e_1] \to \mathbb{F}_2[e_2]$ with $\psi|_{\mathbb{F}_1} = \phi$. The maximality of ϕ implies $\mathbb{F}_1 = \mathbb{F}_1[e_1]$. Thus $e_1 \in \mathbb{F}_1$. So $A_1 \subseteq \mathbb{F}_1$ and $\mathbb{F}_1 = \mathbb{E}_1$. Hence $\mathbb{F}_1$ is a splitting field for P over $\mathbb{K}$. Since ϕ is a $\mathbb{K}$-isomorphism we conclude that $\mathbb{F}_2$ is a splitting field for $P = \phi(P)$ over $\mathbb{K}$. Since $\mathbb{F}_2 \subseteq \mathbb{E}_2$ this implies $A_2 \subseteq \mathbb{F}_2$ and $\mathbb{F}_2 = \mathbb{E}_2$.

(b) Apply (b) to $\delta = \mathrm{id}_{\mathbb{K}}$.

(c) By 4.2.2 there exists a $\mathbb{K}$-linear isomorphisms $\delta : \mathbb{K}[e_1] \to \mathbb{K}[e_2]$ with $\delta(e_1) = e_2$. By (a) δ can be extended to an isomorphism $\psi : \mathbb{E}_1 \to \mathbb{E}_2$. So (a) holds.

(d) Follows from (c) with $\mathbb{E}_2 = \mathbb{E}_1$.

(e) By 4.1.23 an algebraic closure of $\mathbb{K}$ is a splitting field of $\mathbb{K}[x]$. So (e) Follows from (b) with $P = \mathbb{K}[x]$. □

Definition 4.2.8. *Let $\mathbb{E} \leq \mathbb{F}$ be field extension and $H \leq \mathrm{Aut}(\mathbb{F})$.*

*(a) $\mathbb{E}$ is called H-*stable *if $h(e) \in \mathbb{E}$ for all $h \in H, e \in \mathbb{E}$.*[1]

(b) If $\mathbb{E}$ is H-stable, then $H^{\mathbb{E}} := \{h|_{\mathbb{E}} \mid h \in H\}$.

(c) $\mathbb{E} \leq \mathbb{F}$ is called normal *if $\mathbb{E} \leq \mathbb{F}$ is algebraic and each irreducible $f \in \mathbb{E}[x]$, which has a root in $\mathbb{F}$, splits over $\mathbb{F}$.*

Lemma 4.2.9. *Let $\mathbb{K} \leq \mathbb{E} \leq \mathbb{F}$ be field extensions. If $\mathbb{K} \leq \mathbb{F}$ is normal, also $\mathbb{E} \leq \mathbb{F}$ is normal.*

Proof. Let $f \in \mathbb{E}[x]$ be irreducible and suppose f has root b in $\mathbb{F}$. Since $\mathbb{K} \leq \mathbb{F}$ is algebraic, $m^b_{\mathbb{K}} \neq 0$. By 4.1.8 $m^b_{\mathbb{E}}$ divides $m^{\mathbb{K}}_b$ in $\mathbb{E}[x]$. Since f is irreducible, $f \sim m^{\mathbb{E}}_b$ in $\mathbb{E}[x]$ and so f divides $m^{\mathbb{K}}_b$. Since $\mathbb{K} \leq \mathbb{F}$ is normal, $m^{\mathbb{K}}_b$ splits over $\mathbb{F}$ and so also f splits over $\mathbb{F}$. Thus $\mathbb{E} \leq \mathbb{F}$ is normal. □

Lemma 4.2.10. *(a) Let $\mathbb{K} \leq \mathbb{E} \leq \mathbb{F}$ be field extensions and suppose that $\mathbb{E}$ is the splitting field for some set P of polynomials over $\mathbb{K}$. Then $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ stable.*

(b) Let $\mathbb{K} \leq \mathbb{E} \leq \mathbb{F}$ be field extensions and suppose that $\mathbb{F}$ is the splitting field for some set of polynomials over $\mathbb{K}$. If $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$-stable, then $\mathbb{E} \leq \mathbb{K}$ is normal.

(c) $\mathbb{K} \leq \mathbb{E}$ is normal if and only if $\mathbb{E}$ is a splitting field of some set of polynomials over $\mathbb{K}$.

[1] Since also $h^{-1}(\mathbb{E}) \subseteq \mathbb{E}$, this is equivalent to $h(\mathbb{E}) = \mathbb{E}$ for all $h \in H$

(d) *Let $\mathbb{K} \le \mathbb{E} \le \mathbb{F}$ be field extensions. Suppose $\mathbb{K} \le \mathbb{F}$ is normal. Then $\mathbb{K} \le \mathbb{E}$ is normal if and only if $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ stable.*

Proof. (a) Let $A = \{e \in \mathbb{E} \mid f(e) = 0 \text{ for some } 0 \neq f \in P\}$. Let $0 \neq f \in P$, e a root of f in $\mathbb{E}$ and $\phi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then $\phi(e)$ is a root of $\phi(f) = f$ and as f splits over $\mathbb{E}$, $\phi(e) \in \mathbb{E}$. Thus $\phi(A) \subseteq \mathbb{E}$. By definition of a splitting field, $\mathbb{E} = \mathbb{K}[A]$ and so $\phi(\mathbb{E}) = \phi(\mathbb{K})[\phi(A)] = \mathbb{K}[\phi(A)] \le \mathbb{E}$. So $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$-stable.

(b) Let $e \in \mathbb{E}$ and $f = m_e^{\mathbb{K}}$. Let $\mathbb{L}$ be a splitting field for f over $\mathbb{E}$ and let d be a root of f in $\mathbb{F}$. By assumption $\mathbb{F}$ is the splitting field of some $P \subseteq \mathbb{K}[x]$ over $\mathbb{F}$. Then $\mathbb{L}$ is the splitting field for $P \cup \{f\}$ over $\mathbb{K}$ and so by 4.2.7(d) there exists $\phi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ with $\phi(e) = d$. By (a), $\mathbb{F}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$-stable and so $\phi \mid_{\mathbb{F}} \in \mathrm{Aut}_K(\mathbb{F})$. Since $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{K}}(F)$-stable this implies $d = \phi(e) = \phi \mid_{\mathbb{F}} (e) \in \mathbb{E}$ and so $d \in \mathbb{E}$. Hence f splits over $\mathbb{E}$ and $\mathbb{K} \le \mathbb{E}$ is normal.

(c) Suppose first that $\mathbb{K} \le \mathbb{E}$ is normal. Let P be the set of irreducible polynomials in $\mathbb{K}[x]$ with roots in $\mathbb{E}$. By definition of normal each $f \in P$ splits over $\mathbb{E}$. Also $\mathbb{K} \le \mathbb{E}$ is algebraic and so if $e \in \mathbb{E}$ is then e is the root of $m_e^{\mathbb{K}} \in P$. Thus $\mathbb{E}$ is the splitting field of P over $\mathbb{K}$.

Suppose next that $\mathbb{E}$ is the splitting field for some of polynomials over $\mathbb{K}$. Then $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$-stable and (b) applied with $\mathbb{F} = \mathbb{E}$ shows that $\mathbb{K} \le \mathbb{E}$ is normal.

(d) In view of (c), the forward direction of (d) follows from (a) and the backwards direction from (b). □

Lemma 4.2.11. *Let $\mathbb{K} \le \mathbb{E}$ be an algebraic field extension. Then the following two statements are equivalent:*

(a) *$\mathbb{K} \le \mathbb{E}$ is normal.*

(b) *If $\mathbb{E} \le \mathbb{L}$ is a field extension, $e \in \mathbb{E}$ and g is a monic divisors of $m_e^{\mathbb{K}}$ in $\mathbb{E}[x]$, then $g \in \mathbb{E}[x]$.*

Proof. (a) $\Longrightarrow$ (b): Since $\mathbb{K} \le \mathbb{E}$ is normal, $m_e^{\mathbb{K}}$ splits over $\mathbb{E}$ and so

$$m_e^{\mathbb{K}} = (x - e_1)(x - e_2)\dots(x - e_n)$$

for some $e_1, \dots e_n \in \mathbb{E}$. Since g is monic and divides $m_e^{\mathbb{K}}$ we get

$$g = (x - e_{i_1})(x - e_{i_2})\dots(x - e_{i_k})$$

for some $1 \le i_1 < \dots < i_k \le n$ and so $g \in \mathbb{E}[x]$.

(b) $\Longrightarrow$ (a): Let f be an irreducible polynomial in $\mathbb{K}[x]$ with a root $e \in \mathbb{E}$. Then $f = km_e^{\mathbb{K}}$ for some $k \in \mathbb{K}$. Let $\mathbb{L}$ be a splitting field for f over $\mathbb{E}$ and let a be a root of f in $\mathbb{L}$. Then a is also a root of $m_e^{\mathbb{K}}$ and thus $x - a$ divides $m_e^{\mathbb{K}}$ in $\mathbb{L}[x]$. Hence (b) implies $x - a \in \mathbb{E}[x]$ and so $a \in \mathbb{E}$. Thus f splits over $\mathbb{E}$ and $\mathbb{K} \le \mathbb{E}$ is normal. □

Lemma 4.2.12. *Let $\mathbb{K} \le \mathbb{L}$ be an algebraic field extension and $\mathbb{E}$ and $\mathbb{F}$ intermediate fields of $\mathbb{K} \le \mathbb{L}$. Suppose that $\mathbb{K} \le \mathbb{E}$ is normal, then $m_b^{\mathbb{F}} = m_b^{\mathbb{F}\cap\mathbb{E}}$ for all $b \in \mathbb{E}$.*

Proof. Let By 4.1.8, $m_e^{\mathbb{F}}$ divides $m_3^{\mathbb{K}}$ in $\mathbb{L}[x]$ As $\mathbb{K} \le \mathbb{E}$ is normal 4.2.11 shows that $m_e^{\mathbb{F}} \in \mathbb{E}[x]$. Hence $m_e^{\mathbb{F}} \in (\mathbb{E} \cap \mathbb{F})[x]$. Since $m_e^{\mathbb{F}}$ is irreducible in $\mathbb{F}[x]$ it is also irreducible in $(\mathbb{E} \cap \mathbb{F})[x]$. Since $m_e^{\mathbb{F}}$ is monic and has b as a root we conclude from 4.1.7(c) that $m_e^{\mathbb{F}} = m_b^{\mathbb{F}\cap\mathbb{E}}$. □

Definition 4.2.13. *Let $\mathbb{K}$ be a field, $k \in \mathbb{N}$ and $f = \sum_{i=0}^n f_i x^i \in \mathbb{K}[x]$.*

(a) Let $\mathbb{E}$ a splitting field of f over $\mathbb{K}$ and e a root of f in $\mathbb{E}$. Let $m \in \mathbb{N}$ be maximal such that $(x-e)^m$ divides f in $\mathbb{E}[x]$ (with $m = \infty$ if $f = 0$). Then m is called the multiplicity *of e as a root of f. If $m > 1$, then e is called a* multiple root *of f.*

(b) $f^{[k]} := \sum_{i=k}^n \binom{i}{k} f_i x^{i-k}$ is called the k-th derivation of f. [2]

(c) $f' := f^{[1]}$ is called the derivative of f.

Lemma 4.2.14. *Let $\mathbb{K}$ be a field and $f, g \in \mathbb{K}[x]$ and $k \in \mathbb{N}$.*

(a) The function

$$\mathbb{K}[x] \to \mathbb{K}[x], \quad f \to f^{[k]}$$

is $\mathbb{K}$-linear.

(b) $(fg)^{[k]} = \sum_{i=0}^k f^{[i]} g^{[k-i]}$.

(c) Let $a \in \mathbb{K}$. Then $(f(x+a))^{[k]} = f^{[k]}(x+a)$.

(d) $(f^k)' = kf^{k-1}f'$.

Proof. (a) is obvious.

(b) By (a) we may assume that $f = x^m$ and $g = x^n$ We compute

$$(x^m x^n)^{[k]} = (x^{m+n})^{[k]} = \binom{m+n}{k} x^{m+n-k}$$

and

$$\sum_{i+j=k} (x^m)^{[i]}(x^n)^{[j]} = \sum_{i+j=k} \binom{m}{i} x^{m-i} \binom{n}{j} x^{n-j} = \left(\sum_{i+j=k} \binom{m}{i}\binom{n}{j} \right) x^{n+m-k}$$

Let A and B be disjoint set of size m and n respectively. Then a subsets of size k of $A \cup B$ intersects A in i-elements and B in j elements. It follows that

$$\sum_{i+j=k} \binom{m}{i}\binom{n}{j} = \binom{n+m}{k}$$

and so (c) holds.

(c) Define $\Phi : \mathbb{K}[x] \to \mathbb{K}[x], f \to f(x+a)$ and observe that Φ is a $\mathbb{K}$-linear homomorphism. It follows that

[2] Note that $k! f^{[k]}$ is the k-th derivative of f

$$A := \{f \in \mathbb{K}[x] \mid \Phi(f^{[k]}) = \Phi(f)^{[k]} \text{ for all } k \in \mathbb{N}\}$$

is a $\mathbb{K}$-subspace of $\mathbb{K}[x]$. We claim that A is closed under multiplication. Indeed let $f, g \in A$. Then by (b)

$$\begin{aligned}\Phi\left((fg)^{[k]}\right) &= \Phi\left(\sum_{i+j=l} f^{[i]}g^{[j]}\right) = \sum_{i+j=k} \Phi\left(f^{[i]}\right)\Phi\left(g^{[j]}\right) = \sum_{i+j=k} \Phi(f)^{[i]}\Phi(g)^{[j]} \\ &= \left(\Phi(f)\Phi(g)\right)^{[k]} = \Phi(fg)^{[k]}\end{aligned}$$

So $fg \in A$. Hence A is closed under multiplication and so subring of $\mathbb{F}[x]$.

If $k \geq 2$, then both $x^{[k]}$ and $(x+a)^{[k]}$ are equal to 0. Also $x^{[1]} = 1 = (x+a)^{[1]}$ and $1^{[k]} = 0$ for all $k \geq 1$. Thus both 1 and x are in A and since A is a subring and $\mathbb{K}$-subspace of $\mathbb{F}[x]$, $\mathbb{F}[x] = A$.

(d) By (b), $(fg)' = f'g + fg'$ and so by induction on k:

$$(ff^k)' = f'f^k + f(f^k)' = f'f^k + f(kf^{k-1}f') = (k+1)f^kf'$$

□

Lemma 4.2.15. *Let $\mathbb{K}$ be a field, $f \in \mathbb{K}[x]$ and $c \in \mathbb{K}$.*

(a) Suppose that $f = g \cdot (x-c)^k$ for some $k \in \mathbb{N}$ and $g \in \mathbb{K}[x]$. Then $f^{[k]}(c) = g(c)$.

(b) Let $m \in \mathbb{N}$. Then $(x-c)^m$ divides f in $\mathbb{K}[x]$ if and only if $f^{[i]}(c) = 0$ for all $0 \leq i < m$.

(c) The multiplicity of c as a root of f is smallest $m \in \mathbb{N}$ with $f^{[m]}(c) \neq 0$.

(d) c is a multiple root of f if and only if $f'(c) = 0 = f(c)$.

Proof. (a) We compute

$$f^{[k]} = (g\cdot(x-c)^k)^{[k]} = \sum_{i=0}^{k} g^{[i]}\cdot((x-c)^k)^{[k-i]} = \sum_{i=0}^{k} g^{[i]}\cdot\binom{k}{i-k}(x-c)^i = g+(x-c)\sum_{i=1}^{k}\binom{k}{i}g^{[i]}(x-c)^{i-1}$$

and so $f^{[k]}(c) = g(c)$.

(b) This is certainly true for $m = 0$. Suppose its true for m and that $(x-c)^m$ divides f in $\mathbb{K}[x]$ (or equally well that $f^{[i]}(c) = 0$ for all $0 \leq i < m$.) Then $f = g \cdot (x-c)^m$ for some $g \in \mathbb{K}[x]$. Note that $(x-c)^{m+1}$ divides f if and only if $x-c$ divides g and so if and only if $g(c) = 0$. By (a) this holds if and only of $f^{[m+1]}(c) = 0$. Thus (b) holds for $m+1$ and so for all $m \in \mathbb{N}$.

(c) and (b) follow from (d). □

Example 4.2.16. Consider the polynomial $f = x^p$ in $\mathbb{Z}_p[x]$. Then 0 is a root of multiplicity p of f. Also $f^{[k]} = \binom{p}{k}x^{p-k}$ and so 0 is root of $f^{[k]}$ for all $0 \leq k < p$. Finally $f^{[p]} = \binom{p}{p}x^0 = 1$ and so 0 is not a root of $f^{[p]}$.

Note that for any $g \in \mathbb{Z}_p[x]$ the p-derivative of g is $p!g^{[p]} = 0$ since $p = 0$ in $\mathbb{Z}_p$. So higher derivatives cannot be used to compute the multiplicity of a root in fields of positive characteristic.

Definition 4.2.17. *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension.*

(a) An irreducible polynomial $f \in \mathbb{K}[x]$ is called separable *over $\mathbb{K}$ if f has no multiple roots (in a splitting field of f). An arbitrary polynomial in $\mathbb{K}[x]$ is called* separable *over $\mathbb{K}$ if $f = 0$ or all irreducible divisors of f in $\mathbb{F}[x]$ are separable over $\mathbb{K}$.*

(b) $b \in \mathbb{F}$ is called separable *over $\mathbb{K}$, if b is algebraic over $\mathbb{K}$ and $m_b^{\mathbb{K}}$ is separable over $\mathbb{K}$.*

(c) $\mathbb{K} \leq \mathbb{F}$ is called separable if each $b \in \mathbb{F}$ is separable over $\mathbb{K}$.

Lemma 4.2.18. *Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$ and suppose that* $\operatorname{char}\mathbb{K} = p$ *with $p \neq 0$.*

(a) For each $n \in \mathbb{Z}^+$, the map $\mathrm{Frob}_{p^n}^{\mathbb{K}} : \mathbb{K} \to \mathbb{K},\ k \to k^{p^n}$ is a 1-1 ring homomorphism.

(b) For each $b \in \mathbb{K}$ and $n \in \mathbb{Z}^+$ there exists a unique $d \in \bar{K}$ with $d^{p^n} = b$. We will write $b^{p^{-n}}$ for d.

(c) For each $n \in \mathbb{Z}^+$, $\mathrm{Frob}_{p^n}^{\overline{\mathbb{K}}} : \overline{\mathbb{K}} \to \overline{\mathbb{K}},\ k \to k^{p^n}$ is a field automorphism.

(d) For each $n \in \mathbb{Z}$, the map $\mathrm{Frob}_{p^n}^{\mathbb{K}} : \mathbb{K} \to \overline{\mathbb{K}},\ k \to k^{p^n}$ is a 1-1 ring homomorphism.

(e) If $f \in \mathbb{K}[x]$ and $n \in \mathbb{N}$, then $f^{p^n} = \mathrm{Frob}_{p^n}(f)(x^{p^n})$.

Proof. (a) Clearly $(ab)^p = a^p b^p$. Note that p divides $\binom{p}{i}$ for all $1 \leq i < p$. So by the Binomial Theorem $(a+b)^p = a^p + b^p$. Hence Frob_p is a ring homomorphism. If $a \in \mathbb{K}$ with $a^p = 0$, then $a = 0$. So $\ker \mathrm{Frob}_p = 0$ and Frob_p is 1-1. Since $\mathrm{Frob}_{p^n} = \mathrm{Frob}_p^n$, (a) holds.

(b) Let d be a root of $x^{p^n} - b = 0$. Then $d^{p^n} = b$. The uniqueness follows from (a).

(c) Let $n \in \mathbb{N}$. Note that $\mathrm{Frob}_{p^{-n}}^{\overline{\mathbb{K}}}$ is an inverse of $\mathrm{Frob}_{p^n}^{K}$. Thus (c) follows from (a).

(d) Follows from (c).

(e) Let $f = \sum a_i x^i$. Then $\mathrm{Frob}_{p^n}(f) = \sum a_i^{p^n} x^i$ and so

$$\mathrm{Frob}_{p^n}(f)(x^{p^n}) = \sum a_i^{p^n} x^{p^n i} = \left(\sum a_i x^i\right)^{p^n} = f^{p^n}$$

□

Example 4.2.19. Let $\mathbb{K} = \mathbb{Z}_p(x)$, the field of fractions of the polynomial ring $\mathbb{Z}_p[x]$. If $a \in \mathbb{Z}_p$, then $a^p = a$. (Indeed since $(\mathbb{Z}_p^\sharp, \cdot)$ is a group of order $p-1$, $a^{p-1} = 1$ for all $a \in \mathbb{Z}_p^\sharp$. Thus $a^p = a$). It follows that $f^p = f(x^p)$ for all $f \in \mathbb{Z}_p[x]$. Hence

$$\mathrm{Frob}_p(\mathbb{K}) = \left\{ \frac{f(x^p)}{g(x^p)} \,\middle|\, f, g \in \mathbb{Z}_p[x], g \neq 0 \right\} = \mathbb{Z}_p(x^p)$$

So $\mathbb{Z}_p(x^p)$ is a proper subfield of $\mathbb{Z}_p(x)$ isomorphic to $\mathbb{Z}_p(x)$.

Let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$. Consider the polynomial ring $\mathbb{K}[t]$ over $\mathbb{K}$ in the indeterminate t and $f = t^p - x \in \mathbb{K}[t]$. We claim that f is irreducible. Note that $x^{\frac{1}{p}}$ is a root of f in $\overline{\mathbb{K}}$ and $f = (t - x^{\frac{1}{p}})^p$. Let g be a non-constant monic polynomial in $\mathbb{K}[x]$ dividing f. Then $g = (t - x^{\frac{1}{p}})^k$ for some $1 \leq k \leq p$. Then $x^{\frac{k}{p}} = \pm g(0) \in \mathbb{K}$ and so $k = p$. Thus f is irreducible. Since $x^{\frac{1}{p}}$ is a root of multiplicity p of f, f is not separable over $\mathbb{K}$.

Lemma 4.2.20. *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension such that $p := \operatorname{char}\mathbb{K} \neq 0$ and $b \in \mathbb{F}$. Suppose that $b^{p^n} \in \mathbb{K}$ for some $n \in \mathbb{N}$. Then*

(a) b is the only root of $m_b^{\mathbb{K}}$ (in any splitting field of $m_b^{\mathbb{K}}$).

(b) If b is separable over $\mathbb{K}$, $b \in \mathbb{K}$.

(c) $d^{p^n} \in \mathbb{K}$ for all $d \in \mathbb{K}[b]$.

Proof. Put $q = p^n$.

(a) Note that b is a root of $x^q - b^q$, so by 4.1.7 $m_b^{\mathbb{K}}$ divides $x^q - b^q = (x-b)^q$. Thus (a) holds.

(b) If $m_b^{\mathbb{K}}$ is separable, we conclude from (a) that $m_b^{\mathbb{K}} = x - b$. Thus $b \in \mathbb{K}$.

(c) Let $\phi = \operatorname{Frob}_q$. Then $\{d^q \mid d \in \mathbb{K}[b]\} = \phi([\mathbb{K}[b]]) = \phi(\mathbb{K})[\phi(b)] \leq \mathbb{K}[b^q] \leq \mathbb{K}$. □

Lemma 4.2.21. *Let $\mathbb{K} \leq \mathbb{E} \leq \mathbb{F}$ be field extensions and $b \in \mathbb{F}$. If $b \in \mathbb{F}$ is separable over $\mathbb{K}$, then b is separable over $\mathbb{E}$*

Proof. By 4.1.8 $m_b^{\mathbb{E}}$ divides $m_b^{\mathbb{K}}$. As b is separable over $\mathbb{K}$, $m_b^{\mathbb{K}}$ has no multiple roots. So also $m_b^{\mathbb{E}}$ has no multiple roots and b is separable over $\mathbb{E}$. □

Lemma 4.2.22. *Let $\mathbb{K}$ be a field and let $f \in \mathbb{K}[x]$ be irreducible.*

(a) f is separable if and only if $f' \neq 0$.

(b) If $\operatorname{char}\mathbb{K} = 0$, all polynomials over $\mathbb{K}$ are separable.

Proof. (a) Let b be a root of f in splitting field of f over $\mathbb{K}$. By 4.2.15(c) b is a multiple root of f if and only if $f'(b) = 0$. Since f is irreducible, $f \sim m_b^{\mathbb{K}}$. So b is a root of f' if and only if f divides f'. As $\deg f' < \deg f$ this the case if and only if $f' = 0$.

(b) Note that f is constant. Since $\operatorname{char}\mathbb{K} = 0$ we conclude that $f' \neq 0$. So (b) follows from (a) □

Lemma 4.2.23. *Let $\mathbb{K}$ be a field and $f \in \mathbb{K}[x]$ monic and irreducible. Suppose $p := \operatorname{char}\mathbb{K} \neq 0$ and let $b_1, b_2, \dots b_d$ be the distinct roots of f in an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. Let b be any root of f. Then there exist an irreducible separable polynomial $g \in \mathbb{K}[x]$, $n \in \mathbb{N}$ and a polynomial $h \in \operatorname{Frob}_{p^{-n}}(\mathbb{K})[x]$ such that*

(a) $g = \operatorname{Frob}_{p^n}(h)$.

(b) $f = g(x^{p^n}) = h^{p^n}$.

(c) $g = (x - b_1^{p^n})(x - b_2^{p^n}) \dots (x - b_d^{p^n})$.

(d) $h = (x - b_1)(x - b_2) \dots (x - b_d) \in \mathbb{K}[b_1, \dots, b_d][x]$.

(e) $f = (x - b_1)^{p^n}(x - b_2)^{p^n} \dots (x - b_d)^{p^n}$.

(f) f *is separable over* $\mathbb{K}$ *if and only if* $n = 0$.

(g) $\dim_{\mathbb{K}[b^{p^n}]} \mathbb{K}[b] = p^n$.

(h) b *is separable over* $\mathbb{K}$ *if and only if* $\mathbb{K}[b] = \mathbb{K}[b^p]$.

(i) b^{p^n} *is separable over* $\mathbb{K}$.

Proof. We will first show that $f = g(x^{p^n})$ for some irreducible and separable $g \in \mathbb{K}[x]$ and $n \in \mathbb{N}$. If f is separable, this is true with $g = f$ and $n = 0$. So suppose f is not separable. By 4.2.22(a) $f' = 0$. Let $m = \deg f$. Then $f = \sum_{i=0}^{m} f_i x^i$ and $0 = f' = \sum_{i=0}^{m} i a_i x^{i-1}$. Hence $i a_i = 0$ for all $0 \leq i \leq m$ and so p divides i for all $0 \leq i \leq m$ with $a_i \neq 0$. In particular, $m = pl$ for some $l \in \mathbb{N}$. Put $\tilde{f} = \sum_{i=0}^{l} a_{pi} x^i$. Then $\tilde{f}(x^p) = \sum_{i=0}^{l} a_{pi} x^{pi} = f$. If $\tilde{f} = st$ for some $s \in \mathbb{K}[x]$, then $f = s(x^p)t(x^p)$. Since f is irreducible we conclude that $\tilde{f}$ is irreducible. By induction on $\deg f$, $\tilde{f} = g(x^{p^{\tilde{n}}})$ for some $\tilde{n} \in \mathbb{N}$ and an irreducible and separable $g \in \mathbb{K}[x]$. Put $n = \tilde{n} + 1$, then $f = g(x^{p^n})$.

(a): Put $h = \mathrm{Frob}_{p^{-n}}(g) \in \bar{\mathbb{K}}[x]$. Then $g = \mathrm{Frob}_{p^n}(h)$ and so (a) holds.

(b): By 4.2.18(e), $h^{p^n} = g(x^{p^n}) = f$. Let $b \in -K$. Then b is a root of f if and only if b^{p^n} is a root of g. So $\{b_1^{p^n}, \dots, b_d^{p^n}\}$ is the set of roots of g. As Frob_{p^n} is one to one, the $b_i^{p_n}$ are pairwise distinct. Since g is separable, $g = \prod\{x - e \mid e \text{ a root of } g\}$ and so (b) holds.

(c): Since $h = \mathrm{Frob}_{p^{-n}}(g)$ follows from (b).

(d) By (b) $f = h^{p^n}$ and so (d) implies (e).

(f) follows from (e)

(g) Note that g is the minimal polynomial of b^{p^n} over $\mathbb{K}$, f is the minimal polynomial of b over $\mathbb{K}$ and $\deg f = p^n \deg g$. Thus

$$\dim_{\mathbb{K}[b^{p^n}]} \mathbb{K}[b] = \frac{\dim_{\mathbb{K}} \mathbb{K}[b]}{\dim_{\mathbb{K}} \mathbb{K}[b^{p^n}]} = \frac{\deg f}{\deg g} = p^n$$

(h) Suppose b is not separable. Then $n > 0$ and b^p is a root of $g(x^{p^{n-1}})$. So $\dim_{\mathbb{K}} \mathbb{K}[b^p] \leq p^{n-1}$ and $\mathbb{K}[b] \neq \mathbb{K}[b^p]$.

Suppose that b is separable over. Then by 4.2.21 b is separable over $\mathbb{K}[b^p]$. So by 4.2.20, $b \in \mathbb{K}[b^p]$. Thus $\mathbb{K}[b] = \mathbb{K}[b^p]$.

(i) follows since $b_i^{p^n}$ is a root of the separable g. □

Definition 4.2.24. *Let* $\mathbb{K} \leq \mathbb{F}$ *be a field extension* *(a) Let $b \in \mathbb{F}$. Then b is* purely inseparable *over $\mathbb{K}$ if b is algebraic over $\mathbb{K}$ and b is the only root of $m_b^{\mathbb{K}}$ in a splitting field of $m_b^{\mathbb{K}}$.*

(b) $\mathbb{K} \leq \mathbb{F}$ is called purely inseparable if all elements in $\mathbb{F}$ are purely inseparable over $\mathbb{K}$.

(c) $\mathbb{S} = \mathbb{S}(\mathbb{K}, \mathbb{F})$ is the set of the elements in $\mathbb{F}$ which are separable over $\mathbb{K}$.

(d) $\mathbb{P} = \mathbb{P}(\mathbb{K}, \mathbb{F})$ is the set of the elements in $\mathbb{F}$ which are purely inseparable over $\mathbb{K}$.

Lemma 4.2.25. *Any purely inseparable extension is normal*

Proof. Let $\mathbb{K} \leq \mathbb{F}$ be an purely inseparable extension and $b \in \mathbb{F}$. Then b is the only root of $m_\beta^{\mathbb{K}}$ and so m_β^{K} splits over $\mathbb{F}$. □

Lemma 4.2.26. *Let $\mathbb{K} \leq \mathbb{F}$ be an algebraic field extension. Let $p = \operatorname{char} \mathbb{K}$. Put $\mathbb{S} = \mathbb{S}(\mathbb{K}, \mathbb{F})$ and $\mathbb{P} = \mathbb{P}(\mathbb{K}, \mathbb{F})$.*

(a) Let $b \in \mathbb{K}$. If $p = 0$, then b is purely inseparable over $\mathbb{K}$ if and only $b \in \mathbb{K}$. If $p > 0$ then b is purely inseparable over $\mathbb{K}$ if and only if $b^{p^n} \in \mathbb{K}$ for some $n \in \mathbb{N}$

(b) $\mathbb{K} \cap \mathbb{P} = \mathbb{S}$.

(c) If $\mathbb{K} \leq \mathbb{F}$ is separable and purely inseparable, then $\mathbb{K} = \mathbb{F}$.

(d) $\mathbb{K} \leq \mathbb{F}$ is purely inseparable if and only if $\mathbb{K} = \mathbb{S}$.

(e) $\mathbb{P}$ is a subfield of $\mathbb{F}$.

(f) If $\mathbb{K} \leq \mathbb{F}$ is normal, then $\mathbb{P} \leq \mathbb{F}$ is separable.

(g) If $b \in \mathbb{F}$ is separable over $\mathbb{K}$, then $m_b^{\mathbb{P}} = m_b^{\mathbb{K}}$.

(h) $\mathbb{P} \leq \operatorname{Fix}_{\mathbb{F}} \operatorname{Aut}_{\mathbb{K}}(\mathbb{F})$ with equality if $\mathbb{K} \leq \mathbb{F}$ is normal.

Proof. Let $b \in \mathbb{F}$ and put $f := m_b^{\mathbb{K}}$. If $p > 0$, then by 4.2.23 $f = g(x^{p^n})$ with $g \in \mathbb{K}[x]$ irreducible and separable. Moreover, if $b_1, b_2, \ldots, b_k$ are the distinct roots of f in an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$, then $g = (x - b_1^q)(x - b_2^q) \ldots (x - b_k^q)$, where $q = p^n$. If $p = 0$, then f is separable. So the same statements holds with $g = f$ and $q = 1$.

(a) If $p = 0$ and $b \in \mathbb{K}$, then b is only root of $x - b$. If $p > 0$ and $b^{p^m} \in \mathbb{K}$ for some $m \in \mathbb{K}$, then by 4.2.20(a), b is the only root of f. In either case b is purely inseparable over $\mathbb{K}$.

Suppose b is purely inseparable over $\mathbb{K}$. Then b is the only root of f. Then $k = 1$ and $g = x - b^q$. Since $g \in \mathbb{K}[x]$, $b^q \in \mathbb{K}$ So (a) holds.

(c) Suppose b is separable and purely inseparable over $\mathbb{F}$. Thus b is the only root of f and f has no multiple root. Hence $f = x - b$ and $b \in \mathbb{K}$.

(b) follows from (c).

(d) Suppose first that $\mathbb{K} = \mathbb{S}$. Note that b^q is a root of the separable polynomial g and so $b^q \in \mathbb{S} = \mathbb{K}$. Thus by (a) , b is purely inseparable over $\mathbb{K}$

Suppose $\mathbb{K} \leq \mathbb{F}$ is purely inseparable, then $\mathbb{F} = \mathbb{P}$ and so $\mathbb{S} = \mathbb{S} \cap \mathbb{P} = \mathbb{K}$.

(e) Let $\overline{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$. Then by (a)

$$\mathbb{P} = \mathbb{F} \cap \bigcup_{n \in \mathbb{N}} \mathrm{Frob}^{\overline{\mathbb{F}}}_{p^{-n}}(\mathbb{K})$$

and so $\mathbb{P}$ is subfield of $\mathbb{F}$.

(f) Since b is a root of $f \in \mathbb{F}$ and $\mathbb{K} \leq \mathbb{F}$ is normal, f splits over $\mathbb{F}$. So the distinct roots $b_1, \dots b_k$ of f all are contained in $\mathbb{F}$. Put $h = \mathrm{Frob}_{\frac{1}{q}}(g)$. By 4.2.23(d) $h^q = f$ and $h = (x - b_1)(x - b_2) \dots (x - b_k)$. Thus h splits over $\mathbb{F}$ and $h \in \mathbb{F}[x]$. Also $\mathrm{Frob}_q(h) = g \in \mathbb{K}[x]$ and so $d^q \in \mathbb{K}$ for each coefficient d of f. Thus by (a) $d \in \mathbb{P}$ and hence $h \in \mathbb{P}[x]$. Since h has no multiple roots and $h(b) = 0$ we conclude that h is separable over $\mathbb{P}$. Hence also b is separable over $\mathbb{P}$.

(g) By 4.2.25, $\mathbb{K} \leq \mathbb{P}$ is normal. Since $b \in \mathbb{S}$, 4.2.12 gives $m_b^{\mathbb{P}} = m_b^{\mathbb{P} \cap \mathbb{S}}$. By (b) $\mathbb{S} \cap \mathbb{P} = \mathbb{K}$ and so $m_b^{\mathbb{P}} = m_b^{\mathbb{K}}$.

(h) Let $b \in \mathbb{P}$ and $\phi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then $\phi(b)$ is a root of $\phi(f) = f$ and since $b \in \mathbb{P}$, b is the only root of f. Thus $\phi(b) = b$ and $b \in \mathrm{Fix}_{\mathbb{F}}\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$

Suppose that $\mathbb{K} \leq \mathbb{F}$ is normal and $b \in \mathrm{Fix}_{\mathbb{F}}\mathrm{Aut}_{\mathbb{K}}(\mathbb{F}))$. Since $\mathbb{K} \leq \mathbb{F}$ is normal, f splits over $\mathbb{K}$. Let $\tilde{b}$ be a root of f in $\mathbb{F}$. Since $\mathbb{K} \leq \mathbb{F}$ is normal 4.2.10(c) implies that $\mathbb{F}$ is a splitting field over $\mathbb{K}$ of some set of polynomials. Thus by 4.2.7(d) there exists $\phi \in \mathrm{Aut}_{\mathbb{K}}\mathbb{F}$ with $\phi(b) = \tilde{b}$. Since $b \in \mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{K}}F)$ we conclude that $\tilde{b} = b$. Thus b is the only root of f in $\mathbb{F}$ and so $b \in \mathbb{P}$. □

Lemma 4.2.27. *Let $\mathbb{K} \leq \mathbb{E} \leq \mathbb{F}$ be field extensions and suppose that $\mathbb{K} \leq \mathbb{E}$ is purely inseparable. Then $\mathbb{K} \leq \mathbb{F}$ is normal if and only if $\mathbb{E} \leq \mathbb{F}$ is normal.*

Proof. If $\mathbb{K} \leq \mathbb{F}$ is normal, 4.2.9 shows that $\mathbb{E} \leq \mathbb{F}$ is normal.

So suppose that $\mathbb{E} \leq \mathbb{F}$ is normal. If $\mathrm{char}\,\mathbb{K} = 0$, then $\mathbb{K} = \mathbb{E}$. So suppose $\mathrm{char}\,\mathbb{K} = p > 0$. Let $b \in \mathbb{E}$ and put $f = m_b^{\mathbb{E}}$. Since $\mathbb{K} \leq E$ is purely inseparable, 4.2.26(a) shows that there exists $n \in \mathbb{N}$ with $f_i^{p^m} \in \mathbb{K}$ for all coefficients f_i of f. Hence $f^{p^n} = (\mathrm{Frob}_{p^n} f)(x^{p^n}) \in \mathbb{K}[x]$. Since b is a root of f^{p^n} we conclude that $m_b^{\mathbb{K}}$ divides f^{p^n} in $\mathbb{K}[x]$. Since $\mathbb{E} \leq \mathbb{F}$ is normal, f splits over $\mathbb{F}$. Hence also f^{p^n} and $m_b^{\mathbb{K}}$ split over $\mathbb{F}$. Thus $\mathbb{K} \leq \mathbb{F}$ is normal. □

Lemma 4.2.28. *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $\mathbb{S} = \mathbb{S}(\mathbb{K}, \mathbb{F})$.*

(a) Let $\mathbb{E}$ an intermediate field of $\mathbb{K} \leq \mathbb{F}$. Then $\mathbb{K} \leq \mathbb{F}$ is separable if and only $\mathbb{K} \leq \mathbb{E}$ and $\mathbb{E} \leq \mathbb{F}$ are separable.

(b) $\mathbb{K} \leq \mathbb{F}$ is separable if and only if $\mathbb{F} = \mathbb{K}[S]$ for some $S \subseteq \mathbb{S}$.

(c) $\mathbb{S}$ is an intermediate field of $\mathbb{K} \leq \mathbb{F}$.

Proof. Put $p := \operatorname{char} \mathbb{K}$. If $p = 0$ then by 4.2.22(a)ll algebraic extensions are separable. Hence $\mathbb{K} \leq \mathbb{F}$ is separable if and only if $\mathbb{K} \leq \mathbb{F}$ is algebraic. So 4.1.14 and 4.1.15 show that (a)-(c) hold. a.

So suppose $p > 0$. Before proving (a) and (b) we prove

(*) Let $\mathbb{K} \leq \mathbb{L}$ be a field extension, $I \subset \mathbb{L}$ and $b \in \mathbb{L}$. If all elements in I are separable over $\mathbb{K}$ and b is separable over $\mathbb{K}[I]$, then b is separable over $\mathbb{K}$.

Let $s = m_b^{K(I)}$. By 4.1.4 $\mathbb{K}(I) = \bigcup\{\mathbb{K}(J) \mid J \subseteq I, J \text{ finite}\}$. Hence there exists a finite subset J of I with $s \in \mathbb{K}[J][x]$. So b is separable over $\mathbb{K}[J]$. We know proceed by induction on $|J|$. If $J = \emptyset$, b is separable over $\mathbb{K}$ and $(*)$ holds. So suppose $J \neq \emptyset$ and let $a \in J$. Then b is separable over $\mathbb{K}[a][J - a]$ and so by induction b is separable over $\mathbb{K}[a]$. Hence by 4.2.23(h), $\mathbb{K}[a][b] = \mathbb{K}[a]b^p]$. Let $\mathbb{E} = \mathbb{K}[b^p]$. Then $b \in \mathbb{K}[a][b] = \mathbb{K}[a][b^p] = \mathbb{E}[a]$ and so

$$\mathbb{E}[b] \leq \mathbb{E}[a] = \mathbb{E}[b][a]$$

Since a is separable over $\mathbb{K}$, 4.2.21 shows that a is separable over $\mathbb{E}$. Put $\mathbb{P} = \mathbb{P}(\mathbb{E}, \mathbb{F})$. Then 4.2.26(g) $m_a^{\mathbb{E}} = m_b^{\mathbb{P}}$. Since $b^p \in \mathbb{E}$, 4.2.26(a) shows that $b \in \mathbb{P}$. By 4.2.26(e), $\mathbb{P}$ is a subfield of $\mathbb{F}$ and so $\mathbb{E} \leq \mathbb{E}[b] \leq \mathbb{P}$. Thus $m_\alpha^{E[b]}$ divides $m_a^{\mathbb{E}}$, and m_a^P divides $m_a^{E[b]}$. Since $m_a^{\mathbb{E}} = m_b^{\mathbb{P}}$ this gives $m_a^{\mathbb{E}} = m_a^{\mathbb{E}[b]}$ and

$$\dim_{\mathbb{E}} \mathbb{E}[a] = \deg m_a^{\mathbb{E}} = \deg m_a^{E[b]} = \dim_{\mathbb{E}[b]} \mathbb{E}[b][a] = \dim_{\mathbb{E}[b]} \mathbb{E}[a]$$

Since $\dim_{\mathbb{E}} \mathbb{E}[a] = \dim_{\mathbb{E}} \mathbb{E}[b] \cdot \dim \mathbb{E}[b]\mathbb{E}[a]$ this implies, $\dim_{\mathbb{E}} \mathbb{E}[b] = 1$ and $\mathbb{E}[b] = \mathbb{E}$. Thus So $\mathbb{K}[b] = \mathbb{K}[b^p][b] = \mathbb{E}[b] = \mathbb{E} = \mathbb{K}[b^p]$ and by 4.2.23(h), b is separable over $\mathbb{K}$.

(a) Suppose that $\mathbb{K} \leq \mathbb{E}$ and $\mathbb{E} \leq \mathbb{F}$. are separable. Let $b \in \mathbb{F}$ and let $I = \mathbb{E}$. Then by (*), b is separable over $\mathbb{K}$. So $K \leq \mathbb{F}$ is separable.

Conversely suppose $\mathbb{K} \leq \mathbb{F}$ is separable. Then clearly $\mathbb{K} \leq \mathbb{E}$ is separable. By 4.2.21 also $\mathbb{E} \leq \mathbb{F}$ is separable.

(b) If $\mathbb{K} \leq \mathbb{F}$ is separable, then $\mathbb{F} = \mathbb{K}[S]$ with $S = \mathbb{F}$. So suppose $\mathbb{F} = \mathbb{K}[S]$ with all elements in S separable over $\mathbb{K}$. Let $b \in \mathbb{F} = \mathbb{K}[S]$. Then b is separable over $\mathbb{K}[S]$ and so by (*), b is separable over $\mathbb{K}$. Thus $\mathbb{K} \leq \mathbb{F}$ is separable.

(c) By (b) $\mathbb{K} \leq \mathbb{K}[\mathbb{S}]$ is separable. Thus $\mathbb{K}[\mathbb{S}] = \mathbb{S}$ and (c) holds. □

Lemma 4.2.29. *Let $\mathbb{K} \leq \mathbb{F}$ be an algebraic field extension with intermediate fields $\mathbb{E}$ and $\mathbb{F}$. Then $\langle \mathbb{E}\mathbb{L} \rangle$ is a subfield of $\mathbb{F}$.*

Proof. Since $\mathbb{F}$ is commutative,

$$\langle \mathbb{E}\mathbb{L} \rangle \langle \mathbb{E}\mathbb{L} \rangle = \langle \mathbb{E}\mathbb{L}\mathbb{E}\mathbb{L} \rangle = \langle \mathbb{E}\mathbb{E}\mathbb{L}\mathbb{L} \rangle \leq \langle \mathbb{E}\mathbb{L} \rangle$$

and so $\langle \mathbb{E}\mathbb{L} \rangle$ is a subring of $\mathbb{F}$. Let $0 \neq a \in \langle \mathbb{E}\mathbb{L} \rangle$. Since $\mathbb{K} \leq \mathbb{F}$ is algebraic and $\mathbb{K} \leq \langle \mathbb{E}\mathbb{L} \rangle$, $a^{-1} \in \mathbb{K}[a] \leq \langle \mathbb{E}\mathbb{L} \rangle$ for all $0 \neq a \in \mathbb{E}\mathbb{L}$. Thus $\langle \mathbb{E}\mathbb{L} \rangle$ is a subfield of $\mathbb{F}$. □

Lemma 4.2.30. *Let $\mathbb{K} \leq \mathbb{E} \leq\leq \mathbb{F}$ be field extensions. Then $\mathbb{K} \leq \mathbb{F}$ is purely inseparable if and only if $\mathbb{K} \leq \mathbb{E}$ and $\mathbb{E} \leq \mathbb{F}$ are purely inseparable.*

Proof. We may assume that $p = \operatorname{char}\mathbb{K} > 0$. Let $b \in \mathbb{F}$.

Suppose $\mathbb{K} \le \mathbb{F}$ is purely inseparable. Then also $\mathbb{K} \le \mathbb{E}$ is purely inseparable. Since $m_b^{\mathbb{K}}$ has only one root and since $m_b^{\mathbb{E}}$ divides $m^{\mathbb{K}}b$, $m_{\mathbb{E}}^{b}$ has only one root. Thus b is purely inseparable over $\mathbb{E}$.

Suppose that $\mathbb{K} \le \mathbb{E}$ and $\mathbb{E} \le \mathbb{F}$ are purely inseparable. Then by 4.2.26(a) $b^{p^m} \in \mathbb{E}$ and then $(b^{p^m})^n \in \mathbb{K}$ for some $m, n \in \mathbb{N}$. Thus $b^{p^{n+m}} \in \mathbb{K}$ and $K \le \mathbb{F}$ is purely inseparable. □

Lemma 4.2.31. *Let $\mathbb{K} \le \mathbb{F}$ be an algebraic field extension. Put $\mathbb{P} = \mathbb{P}(\mathbb{K}, \mathbb{F})$ and $\mathbb{S} = \mathbb{S}(\mathbb{K}, \mathbb{F})$.*

(a) $\mathbb{S} \le \mathbb{F}$ is purely inseparable.

(b) If $\mathbb{K} \le \mathbb{F}$ is normal, then $\mathbb{F} = \langle \mathbb{S}\mathbb{P} \rangle$.

Proof. (a) Let $b \in \mathbb{F}$. By 4.2.23(i),b^{p^n} is separable over $\mathbb{K}$ for some $n \in \mathbb{N}$. Thus $b^{p^n} \in \mathbb{S}$ and so by 4.2.26(a)m b is purely inseparable over $\mathbb{S}$.

(b) By 4.2.29 $\langle \mathbb{S}\mathbb{P} \rangle$ is a subfield of $\mathbb{F}$. By (a) $\mathbb{S} \le \mathbb{F}$ and so by 4.2.30 also $\langle \mathbb{S}\mathbb{P} \rangle \le \mathbb{F}$ is purely inseparable. Since $\mathbb{K} \le \mathbb{F}$ is normal,4.2.26(f) implies that $\mathbb{S} \le \mathbb{F}$ and so also $\mathbb{S}\mathbb{P} \le \mathbb{F}$ is separable. 4.2.26(b) applied with $\mathbb{K} = \langle \mathbb{S}\mathbb{P} \rangle$ now shows that $\mathbb{F} = \langle \mathbb{S}\mathbb{P} \rangle$. □

Example 4.2.32. *Construct a purely inseparable field extension $\mathbb{E} \le \mathbb{F}$ such that $\dim_{\mathbb{E}} \mathbb{F}$ is an arbitrary infinite cardinality.*

Let $\mathbb{K}$ be a field with $\operatorname{char} K = p \ne 0$, I an arbitrary set and $\mathbb{F} = \mathbb{K}(X_I)$, the field of fractions of the polynomial ring $\mathbb{K}[X_I]$. Put

$$\mathbb{E} = \mathbb{K}(x_i^p \mid i \in I)$$

Then $x_i \in \mathrm{Frob}^{\overline{\mathbb{F}}}_{p^{-1}}(\mathbb{E})$ and so $\mathbb{F} \le \mathrm{Frob}^{\overline{\mathbb{F}}}_{p^{-1}}(\mathbb{E})$, that is $a^p \in \mathbb{E}$ for all $a \in \mathbb{F}$. In particular, $\mathbb{E} \le \mathbb{F}$ is purely inseparable over $\mathbb{E}$. Recall that $\mathbb{N}_I = \bigoplus_{i \in I} \mathbb{N}$ and for $n \in \mathbb{N}_I$, $x^n = \prod_{i \in I} x_i^{n_i}$. Also $(x_n)_{n \in \mathbb{N}_I}$ is a $\mathbb{K}$-basis for $\mathbb{K}[X_I]$. Put $R = \{i \in \mathbb{N} \mid r < p\}$. We will show We will show that

$$(*) \qquad (x^r)_{r \in R_I} \text{ is an } \mathbb{E}- \text{ for basis for } \mathbb{F}$$

Let $n = (n_i)_{i \in I} \in \mathbb{N}_I$. For $i \in I$ choose $q_i, r_i \in \mathbb{N}$ with $n_i = pq_i + r_i$ and $0 \le r_i < p$. Put

$$q = (q_i)_{i \in I}, pq = (pq_i)_{i \in I} \text{ and } r = (r_i)_{i \in I}$$

Then $q \in N_I$ and $r \in R_I$ are unique with respect to $n = pq + r$. Put $W = \langle x^r \mid r \in R_I \rangle_{\mathbb{E}}$. Since $x^{pq} = (x^q)^p \in \mathbb{E}$ we get

$$x^n = x^{pq+r} = x^{pq} x^r \in W$$

Thus also

$$\mathbb{K}[X_I] = \langle x^n \mid n \in \mathbb{N}_I \rangle_{\mathbb{K}} \le W$$

Let $f \in \mathbb{F}$. Then $f = \frac{g}{h}$ with $f, g \in R$, $g \ne 0$. Then

$$\frac{f}{g} = \left(\frac{1}{g}\right)^p fg^{p-1}$$

Since $\left(\frac{1}{g}\right)^p \in \mathbb{E}$ and $fg^{p-1} \in \mathbb{K}[X_I] \in W$ we get $f \in W$ and so $W = \mathbb{F}$.

Thus $(x^r)_{r\in R_I}$ is spans $\mathbb{F}$ as $\mathbb{E}$-space. To show that $(x^r)_{r\in R_I}$ is linearly independent, let $e \in \mathbb{E}_{R_I}$ with

$$\sum_{r\in R_I} e_r x^r = 0$$

W e need to show that $e = 0$. Put $S = \mathbb{K}[x_i^p \mid i \in I]$. Then $e_r = \frac{g_r}{h_r}$ for some $g_r, h_r \in S$ with $h_r \neq 0$. We need to show that $e = 0$. Multiplying with $\prod_{\substack{r\in R_I \\ e_r\neq 0}} h_r$ we may assume that $e_r \in S$ for all $r \in R_I$. So $e_r = \sum_{q\in\mathbb{N}_I} k_{rq}x^{pq}$ for some $k_r = (k_{rq})_{q\in\mathbb{N}_I} \in \mathbb{K}_{\mathbb{N}_I}$. Thus

$$\sum_{r\in R_I}\sum_{q\in\mathbb{N}_I} k_{qr}x^{pq+r} = 0$$

As observed above each $n \in \mathbb{N}$ can by uniquely written as $pq + r$ with $q \in J$ and $r \in J_p$. Thus the linear independence of the $(x^n)_{n\in\mathbb{N}_I}$ over $\mathbb{K}$ shows that

$$k_{qr} = 0$$

for all $q \in \mathbb{N}_I$ and $r \in R_I$. Hence also $e_r = 0 =$ and so $(x^r)_{r\in R_I}$ is linearly independent over $\mathbb{E}$ and so a basis of $\mathbb{F}$ over $\mathbb{E}$. In particular, $\dim_{\mathbb{E}} \mathbb{F} = |R_I|$ and thus

$$\dim_{\mathbb{E}} \mathbb{F} = \begin{cases} p^{|I|} & \text{if } |I| \text{ finite} \\ |I| & \text{if } |I| \text{ infinite} \end{cases}$$

Example 4.2.33. *Construct a field extension $\mathbb{K} \leq \mathbb{F}$ such that $\mathbb{P}(\mathbb{K},\mathbb{F}) = \mathbb{K}$ and $\mathbb{S}(\mathbb{K},\mathbb{F}) \neq \mathbb{F}$. So 4.2.26(g) and 4.2.31(b) may be false if $\mathbb{K} \leq \mathbb{F}$ is not normal.*

Let $\mathbb{F}_4$ be a splitting field for $x^2 + x + 1$ over $\mathbb{Z}_2$ and a a root of $x^2 + x + 1$ in $\mathbb{F}_4$. Then $a \neq 0, 1$ and so $\mathbb{F}_4 \neq \mathbb{Z}_2$ and $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$, Since $(x^2 + x + 1)' = 2x + 1 = 1 \neq 0$, $x^2 + x + 1$ is separable and so a is separable over $\mathbb{Z}_2$.

Let y and z be indeterminates over $\mathbb{F}_4$. Put $\mathbb{E} = \mathbb{F}_4(y,z)$, $\mathbb{K} = \mathbb{Z}_2(y^2,z^2)$, $\mathbb{S} = \mathbb{F}_4(y^2,z^2)$ and $\mathbb{P} = \mathbb{F}_2(y,z)$. Note that $\mathbb{S} = \mathbb{K}[a]$ and $\mathbb{E} = \mathbb{P}[a]$. Since a is separable over $\mathbb{Z}_2$, α is also separable over $\mathbb{K}$ and $\mathbb{P}$ and so $\mathbb{K} \leq \mathbb{S}$ and $\mathbb{P} \leq \mathbb{E}$ are separable. separable.

By 4.2.32 applied with $\mathbb{K} = \mathbb{F}_4$:

$\mathbb{S} \leq \mathbb{E}$ is purely inseparable, $d^2 \in \mathbb{S}$ for all $d \in \mathbb{E}$ and

$$(1, y, z, yz) \quad \text{is a } \mathbb{S}\text{-basis for } \mathbb{E}$$

and applied with $\mathbb{K} = \mathbb{F}_2$:

$\mathbb{K} \leq \mathbb{P}$ is purely inseparable, $d^2 \in \mathbb{K}$ for all $d \in \mathbb{P}$ and

$$(1, y, z, yz) \quad \text{is a } \mathbb{K}\text{-basis for } \mathbb{P}$$

It follows that $\mathbb{S} \leq \mathbb{S}(\mathbb{K}, \mathbb{E})$ and $\mathbb{P} \leq \mathbb{P}(\mathbb{K}, \mathbb{E})$ are both separable and purely inseparable. Thus $\mathbb{S} = \mathbb{S}(\mathbb{K}, \mathbb{E})$ and $\mathbb{P} = \mathbb{P}(\mathbb{K}, \mathbb{E})$

Put $b = y + az$. Then $b \notin \mathbb{S}$ and $b^2 \in \mathbb{S}$. Thus $x^2 - b^2$ is the minimal polynomial of b over $\mathbb{S}$. Put $\mathbb{F} = \mathbb{S}[b]$. Then $(1, b)$ is an $\mathbb{S}$ basis for $\mathbb{F}$. Let $d \in \mathbb{F} \cap \mathbb{P}$. Then there exists $s, t \in \mathbb{S}$ and $k_1, k_2, k_3, k_4 \in \mathbb{K}$ with

$$s + ty + taz = s + tb = d = k_1 + k_2 y + k_3 z + k_4 yz$$

Since $\{1, y, z, yz\}$ is linearly independent over $\mathbb{S}$ we conclude that $s = k_1, t = k_2$, $at = k_3$ and $0 = k_4$. So s, t and at are in $\mathbb{K}$. If $t \neq 0$ we get $a = att^{-1} \in \mathbb{K}$, a contradiction. Thus $t = 0$ and $d = s \in \mathbb{K}$. Thus $\mathbb{F} \cap \mathbb{P} = \mathbb{K}$. Hence

$$\mathbb{P}(\mathbb{K}, \mathbb{F}) = \mathbb{F} \cap \mathbb{P} = \mathbb{K} \text{ and } \mathbb{S}(\mathbb{K}, \mathbb{F}) = \mathbb{F} \cap \mathbb{S} = \mathbb{S} \neq \mathbb{F}$$

4.3 Galois Theory

Hypothesis 4.3.1. *Throughout this section $\mathbb{F}$ is a field and $G \leq \mathrm{Aut}(\mathbb{F})$.*

Definition 4.3.2. *Let $H \leq G$ and $\mathbb{E}$ a subfield of $\mathbb{F}$.*

(a) $\mathcal{F}H := \mathrm{Fix}_{\mathbb{F}}(H)$.

(b) $\mathcal{G}E := G \cap \mathrm{Aut}_{\mathbb{E}}(F)$.

(c) We say that H is $(G, \mathbb{F})$-closed *(or that H is closed in G with respect to $\mathbb{F}$) if $H = \mathcal{G}\mathcal{F}H$.*

(d) $\mathbb{E}$ is $(G, \mathbb{F})$-closed *(or that $\mathbb{E}$ is closed in $\mathbb{F}$ with respect to G) if $\mathbb{E} = \mathcal{F}\mathcal{G}\mathbb{E}$.*

(e) ”closed” means $(G, \mathbb{F})$-closed.

(f) Stable means G-stable.

Lemma 4.3.3. *Let $T \leq H \leq G$ and $\mathbb{L} \leq \mathbb{E} \leq \mathbb{F}$. Then*

(a) $\mathcal{F}H$ is a subfield of $\mathbb{F}$ containing $\mathcal{F}G$

(b) $\mathcal{G}E$ is a subgroup of G

(c) $\mathcal{F}H \leq \mathcal{F}T$.

(d) $\mathcal{G}\mathbb{E} \leq \mathcal{G}\mathbb{L}$.

(e) $H \leq \mathcal{G}\mathcal{F}H$

(f) $\mathbb{E} \leq \mathcal{F}\mathcal{G}\mathbb{E}$.

(g) $\mathcal{F}H$ is closed.

(h) $\mathcal{G}\mathbb{E}$ is closed.

Proof. (a) and (b) are obvious. The remaining statements follow from A.1.13 applied to the relation $\{(g, m) \in G \times M \mid g(m) = m\}$.

□

Proposition 4.3.4. *$\mathcal{F}$ induces an inclusion reversing bijection between the closed subgroups of G and the closed subfields of $\mathbb{F}$. The inverse is induced by $\mathcal{G}$.*

Proof. By 4.3.3 all closed subsets of G are subgroups and all closed subsets of $\mathbb{F}$ are subfields. The proposition now follows from A.1.13(f). □

Lemma 4.3.5. *Let $H \leq T \leq G$ with T/H finite. Then* $\dim_{\mathcal{F}T} \mathcal{F}H \leq |T/H|$.

Proof. Let $k \in \mathcal{F}H$ and $W = tH \in T/H$. Define $W(k) := t(k)$. Since $(th)(k) = t(h(k)) = t(k)$ for all $h \in H$, this is well defined. Define

$$\Phi : \mathcal{F}H \to \mathbb{F}^{T/H},\ k \to \big(W(k)\big)_{W \in T/H}$$

Let $L \subseteq \mathcal{F}H$ be a basis for $\mathcal{F}H$ over $\mathcal{F}T$. We claim that $\big(\Phi(l)\big)_{l \in L}$ is linear independent in $\mathbb{F}^{T/H}$ over $\mathbb{F}$. Otherwise choose $I \subseteq L$ minimal such that $(\Phi(i))_{i \in I}$ is linear dependent over $\mathbb{F}$. Then $|I|$ is finite and there exists $0 \neq k_i \in \mathbb{F}$, with

$$(*) \qquad \sum_{i \in I} k_i \Phi(i) = 0.$$

Fix $b \in I$. Dividing by k_b we may assume that $k_b = 1$.

Note that (*) means

$$(**) \qquad \sum_{i \in I} k_i W(i) = 0, \quad \text{for all } W \in T/H.$$

Let $s \in T$. Then for $W = tH \in T/H$ and $i \in I$,

$$s(W(i)) = s(t(i)) = (st)(i) = (stH)(i) = (sW)(i)$$

Thus applying s to $(**)$ we obtain.

$$\sum_{i \in I} s(k_i)(sW)(i) = 0, \quad \text{for all } W \in T/H.$$

As every $W \in T/H$ is of the form sW' for some $W' \in T/H$, (namely $W' = s^{-1}W$) we get

$$(***) \qquad \sum_{i \in I} s(k_i) W(i) = 0, \quad \text{for all } W \in T/H.$$

Subtracting (**) form (***) we conclude:

$$\sum_{i \in I} (s(k_i) - k_i) W(i) = 0, \quad \text{for all } W \in T/H.$$

and so

$$\sum_{i\in I}(s(k_i)-k_i)\Phi(i)=0.$$

The coefficient of $\Phi(b)$ in this equation is $s(1)-1=0$. The minimality of $|I|$ now implies that $s(k_i)-k_i=0$ for all $s\in T$ and $i\in I$. Thus $s(k_i)=k_i$ and $k_i\in\mathcal{F}T$ for all $i\in I$. Note that $H(i)=\mathrm{id}_{\mathbb{F}}(i)=i$ for all $i\in I$. So using $W=H$ in (**) we get $\sum_{i\in I}k_i i=0$, a contradiction to the linear independence of L over $\mathcal{F}T$.

This contradiction proves that $\left(\Phi(l)\right)_{l\in L}$ is linear independent in $\mathbb{F}^{T/H}$ over $\mathbb{F}$. hence

$$\dim_{\mathcal{F}T}\mathcal{F}H=|L|\le\dim_{\mathbb{F}}\mathbb{F}^{T/H}=|T/H|$$

So the theorem is proved. □

Note that last equality in the last equation is the only place where we used that $|T/H|$ is finite.

Lemma 4.3.6. *Let $b\in\mathbb{F}$ and $H\le G$.*

(a) b is algebraic over $\mathcal{F}H$ if and only if $Hb:=\{\phi(b)\mid\phi\in H\}$ is finite.

(b) Suppose that b is algebraic over $\mathcal{F}H$ and let m_b be the minimal polynomial of b over $\mathcal{F}H$. Then

- *(a) $m_b=\prod_{e\in Hb}x-e$.*
- *(b) m_b is separable and b is separable over $\mathcal{F}H$.*
- *(c) m_b splits over $\mathbb{F}$.*
- *(d) Put $H_b:=\{\phi\in H\mid\phi(b)=b\}$. Then*

$$|H/H_b|=\deg m_b=|Hb|=\dim_{\mathcal{F}H}(\mathcal{F}H)[b]$$

Proof. Put $m_b=m_b^{\mathcal{F}H}$ and, if Hb is finite, $f=\prod_{e\in Hb}x-e$.

(a) Suppose that b is algebraic over $\mathcal{F}H$. Then $m_b\neq 0$. Let $\phi\in H$. Then $\phi(b)$ is a root of $\phi(m_b)=m_b$. Since m_b has only finitely many roots, Hb is finite. Note also that f divides m_b in this case.

Suppose next that Hb is finite. Since the map $Hb\to Hb, e\to\phi(e)$ is a bijection with inverse $e\to\phi^{-1}(e)$,

$$\phi(f)=\prod_{e\in Hb}x-\phi(e)=\prod_{e\in Hb}x-e=f.$$

Hence all coefficient of f are fixed by ϕ and so $f\in(\mathcal{F}H)[x]$. Clearly b is a root of f. Thus b is algebraic over $\mathcal{F}H$. Note also that m_b divides f in this case.

(b) Suppose now that b is algebraic over $\mathcal{F}H$. Then Hb is finite. As seen above m_b divides f and f divides m_b. Since both f and m_b are monic $f=m_b$ and so (b:a) hold. Since f is no multiple roots, f is separable and so (b:b) is proved. Since f splits over $\mathbb{F}$, (b:c) holds.

By 1.7.20 $|H/H_b|=|Hb|$, By 4.1.2(1) $\dim_{\mathcal{F}H}(\mathcal{F}H)[b]=\deg m_b=\deg f=|Hb|$ and so also (b:d) holds. □

Corollary 4.3.7. *Put $\mathbb{K} = \mathcal{F}G$ and let $\mathbb{E}$ be an intermediate field of $\mathbb{K} \leq \mathbb{F}$ with $\mathbb{K} \leq \mathbb{E}$ algebraic. Then $\mathbb{E}$ is G-stable if and only if $\mathbb{K} \leq \mathbb{E}$ is normal.*

Proof. Suppose first that $\mathbb{E}$ is stable. Let $b \in E$ and $f = m_b^{\mathbb{K}}$. By 4.3.6, $f = \prod_{e \in Gb} x - d$. So f splits over $\mathbb{F}$ and Gb is the set of roots of f. As $\mathbb{E}$ is stable, $Gb \subseteq \mathbb{E}$ and so f splits over $\mathbb{E}$.

Suppose next that $\mathbb{K} \leq \mathbb{E}$ is normal, then by 4.2.10 $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$-stable. Since $G \leq \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$, $\mathbb{E}$ is also G- stable. □

Lemma 4.3.8. *Let $\mathbb{L} \leq \mathbb{E} \leq \mathbb{F}$ with $\mathbb{L} \leq \mathbb{E}$ finite. Then*

$$|\mathcal{G}\mathbb{L}/\mathcal{G}\mathbb{E}| \leq \dim_{\mathbb{L}} \mathbb{E}$$

Proof. If $\mathbb{E} = \mathbb{L}$, this is obvious. So we may assume $\mathbb{E} \neq \mathbb{L}$. Pick $e \in \mathbb{E} \setminus \mathbb{L}$. Since $\mathbb{L} \leq \mathbb{E}$ is finite, e is algebraic over $\mathbb{L}$ and since $\mathbb{L} \leq \mathcal{F}\mathcal{G}\mathbb{L}$, e is also algebraic over $\mathcal{F}\mathcal{G}\mathbb{L}$. Moreover, $g = m_e^{\mathcal{F}\mathcal{G}\mathbb{L}}$ divides $f = m_e^{\mathbb{L}}$. Put $H = \mathcal{G}\mathbb{L}$. By 4.3.6 $|H/H_e| = \deg g$. Since $\mathcal{F}H_e$ is subfield of $\mathbb{F}$, $\mathbb{L}[e] \leq \mathcal{F}_e$ and

$$H_e \leq \mathcal{G}(\mathbb{L}[e]) \leq H_e$$

Hence $H_e = \mathcal{G}(\mathbb{L}[e])$ and so

$$|\mathcal{G}\mathbb{L}/\mathcal{G}(\mathbb{L}[e])| = |H/H_e| = \deg g \leq \deg f = \dim_{\mathbb{L}} \mathbb{L}[e].$$

By induction on $\dim_{\mathbb{L}} \mathbb{E}$,

$$|\mathcal{G}(\mathbb{L}[e])/\mathcal{G}\mathbb{E}| \leq \dim_{\mathbb{L}[e]} \mathbb{E}.$$

Multiplying the two inequalities we obtain the result. □

Theorem 4.3.9. *(a) Let $H \leq T \leq G$ with H closed and T/H finite. Then T is closed and*

$$\dim_{\mathcal{F}T} \mathcal{F}H = |T/H|.$$

(b) Let $\mathbb{L} \leq \mathbb{E} \leq \mathbb{F}$ with $\mathbb{L}$ closed and $\mathbb{L} \leq \mathbb{E}$ finite. Then $\mathbb{E}$ is closed and

$$|\mathcal{G}\mathbb{L}/\mathcal{G}\mathbb{E}| = \dim_{\mathbb{L}} \mathbb{E}.$$

Proof. (a) We have

$$|T/H| \overset{4.3.5}{\geq} \dim_{\mathcal{F}T} \mathcal{F}H \overset{4.3.8}{\geq} |\mathcal{G}(\mathcal{F}T)/\mathcal{G}(\mathcal{F}H)| \overset{H \text{ closed}}{=} |\mathcal{G}(\mathcal{F}T)/H| \overset{4.3.3(g)}{=} |T/H|.$$

So all the inequalities are equalities. Hence $T = \mathcal{G}\mathcal{F}T$ and

$$\dim_{\mathcal{F}T} \mathcal{F}H = |T/H|.$$

(b) This time we have

$$\dim_{\mathbb{L}} \mathbb{E} \overset{4.3.8}{\geq} |\mathcal{G}\mathbb{L}/\mathcal{G}\mathbb{E}| \overset{4.3.5}{\geq} \dim_{\mathcal{F}\mathcal{G}\mathbb{L}} \mathcal{F}\mathcal{G}\mathbb{E} \overset{\mathbb{L} \text{ closed}}{=} \dim_{\mathbb{L}} \mathcal{F}\mathcal{G}\mathbb{E} \overset{4.3.3(f)}{=} \geq \dim_{\mathbb{L}} \mathbb{E}$$

So all the inequalities are equalities. Hence $\mathbb{E} = \mathcal{F}\mathcal{G}\mathbb{E}$ and

$$\dim_{\mathbb{L}} \mathbb{E} = |\mathcal{G}\mathbb{L}/\mathcal{G}\mathbb{E}|$$

□

Proposition 4.3.10. *(a) Let $H \leq G$ with H finite. Then H is closed and* $\dim_{\mathcal{F}H} \mathbb{F} = |H|$.

(b) Put $\mathbb{K} = \mathcal{F}G$ and let $\mathbb{K} \leq \mathbb{E} \leq \mathbb{F}$ with $\mathbb{K} \leq \mathbb{E}$ finite. Then $\mathbb{E}$ is closed and $\dim_{\mathbb{K}} \mathbb{E} = |G/\mathcal{G}\mathbb{E}|$.

Proof. (a) Note that $\mathcal{F}\{\mathrm{id}_{\mathbb{F}}\} = \mathbb{F}$ and so $\mathcal{G}\mathcal{F}\{\mathrm{id}_{\mathbb{F}}\} = \{\mathrm{id}_{\mathbb{F}}\}$. Hence the trivial group is closed and has finite index in H. So (a) follows from 4.3.9a

(b) By 4.3.3(g), $\mathbb{K} = \mathcal{F}G$ is closed. Moreover, $\mathcal{G}\mathbb{K} = G \cap \mathrm{Aut}_{\mathbb{K}}(\mathbb{F}) = G$. Thus by 4.3.9(b), applied with $\mathbb{L} = \mathbb{K}$, $\mathbb{E}$ is closed and

$$\dim_{\mathbb{K}} \mathbb{E} = |\mathcal{G}\mathbb{K}/\mathcal{G}\mathbb{E}| = |G/|\mathcal{G}\mathbb{E}|$$

□

Definition 4.3.11. *A field extension $\mathbb{L} \leq \mathbb{E}$ is called* Galois *if $\mathbb{L}$ is closed in $\mathbb{E}$ with respect to* $\mathrm{Aut}(\mathbb{E})$*, that is if* $\mathbb{L} = \mathrm{Fix}_{\mathbb{E}}(\mathrm{Aut}_{\mathbb{L}}(\mathbb{E}))$.

Lemma 4.3.12. *Put $\mathbb{K} = \mathcal{F}G$. Then $\mathbb{K} \leq \mathbb{F}$ is a Galois Extension. Moreover, if $\mathbb{K} \leq \mathbb{F}$ is finite, then* $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$.

Proof. By 4.3.3(h) applies with $(\mathrm{Aut}(\mathbb{F}), G)$ in place of (G, H), $\mathrm{Fix}_{\mathbb{F}}(G)$ is closed in $\mathbb{F}$ with respect to $\mathrm{Aut}(\mathbb{E})$. So $\mathbb{L} \leq \mathbb{E}$ is Galois.

Moreover, if $\mathbb{K} \leq \mathbb{F}$ is finite, then by 4.3.10 applied to G and to $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ in place of H.

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})| = \dim_{\mathbb{K}} \mathbb{F} = |G|$$

Since $G \leq \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$, this implies $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. □

Theorem 4.3.13 (Fundamental Theorem Of Galois Theory)**.** *Let $\mathbb{K} \leq \mathbb{F}$ be a finite Galois extension and put $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then*

(a) $\mathcal{F}$ is inclusion reversing bijection from the set of subgroups of G to the set of intermediate field of $\mathbb{K} \leq \mathbb{F}$.

(b) Let $H \leq G$ and $\mathbb{E} = \mathcal{F}H$. Then $\dim_{\mathbb{E}} \mathbb{F} = |H|$ *and* $H = \mathrm{Aut}_{\mathbb{E}}(\mathbb{F})$.

Proof. (a) Since $\mathbb{K} \leq \mathbb{F}$ is Galois, $\mathbb{K}$ is closed. Since $\mathbb{K} \leq \mathbb{F}$ is finite, 4.3.10(b) implies that G is finite and so by 4.3.10 all intermediate field of $\mathbb{K} \leq \mathbb{F}$ and all subgroups of G are closed. So by 4.3.4, $\mathcal{F}$ induces a inclusion reversing bijection between the subgroups of G and intermediate fields of $\mathbb{K} \leq \mathbb{F}$.

(b) By 4.3.10(a) $\dim_{\mathbb{E}} \mathbb{F} = |H|$. By 4.3.12 applied to H in place of G, $H = \mathrm{Aut}_{\mathbb{F}}(K)$. □

Lemma 4.3.14. *Put $\mathbb{K} = \mathbb{F}G$ and let $\mathbb{E}$ be a G-stable intermediate field of $\mathbb{K} \leq F$.*

(a) $\mathrm{Fix}_{\mathbb{E}}(G^{\mathbb{E}}) = \mathbb{K}$ *and* $\mathbb{K} \le \mathbb{E}$ *is Galois.*

(b) If $\mathbb{K} \le \mathbb{E}$ *is finite, then* $G^{\mathbb{E}} = \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$.

Proof. (a) $\mathrm{Fix}_{\mathbb{E}}(G^{\mathbb{E}}) = \mathrm{Fix}_{\mathbb{F}} G \cap \mathbb{E} = \mathbb{K} \cap \mathbb{E} = \mathbb{K}$

(b) Follows from (a) and 4.3.124.3.13. □

Lemma 4.3.15. *(a) Let* $\mathbb{E} \le \mathbb{F}$ *and* $g \in G$. *Then* ${}^{g}(\mathcal{G}\mathbb{E}) = \mathcal{G}(g(\mathbb{E}))$.

(b) Let $H \le G$ *and* $g \in G$. *Then* $\mathcal{F}({}^{g}H) = g(\mathcal{F}H)$.

(c) Let $H \trianglelefteq G$. *Then* $\mathcal{F}H$ *is G-stable.*

(d) Let $\mathbb{E} \le \mathbb{F}$ *and suppose* $\mathbb{E}$ *is G-stable. Then* $\mathcal{G}\mathbb{E} \trianglelefteq G$ *and* $G^{\mathbb{E}} \cong G/\mathcal{G}\mathbb{E}$.

(e) Let $H \le G$ *be closed. Then* $H \trianglelefteq G$ *if and only if* $\mathcal{F}H$ *is G-stable.*

(f) Let $\mathbb{E}$ *be a closed subfield of* $\mathbb{F}$. *Then* $\mathbb{E}$ *is stable if and only if* $\mathcal{G}\mathbb{E}$ *is normal in G.*

Proof. (a) Since $\mathcal{G}\mathbb{E} = \mathrm{Stab}_G(\mathbb{E})$, (a) follows from 1.7.11(e).

(b) Since $\mathcal{F}H = \mathrm{Fix}_{\mathbb{F}}(H)$, (b) follows from 1.7.11(f)

(c) If $H \trianglelefteq G$ then by (b), $\mathcal{F}H = g(\mathcal{F}H)$.

(d) Follows from 1.7.10(a) and b.

(e) The forward direction follows from (c). By (d), if $\mathcal{F}H$ is stable , then $\mathcal{G}\mathcal{F}H \trianglelefteq G$. If H is closed, then $\mathcal{G}\mathcal{F}H = H$ and so the backward direction holds.

(f) Follows from (e) applied to $H = \mathcal{G}\mathbb{E}$. □

Lemma 4.3.16. *Put* $\mathbb{K} = \mathcal{F}G$ *and let* $\mathbb{K} \le \mathbb{E} \le \mathbb{F}$ *with* $\mathbb{K} \le \mathbb{E}$ *algebraic. Then*

(a) $\mathbb{K} \le \mathbb{E}$ *is separable.*

(b) If $\mathbb{E}$ *is closed, then the following are equivalent:*

- *(a)* $\mathcal{G}\mathbb{E} \trianglelefteq G$.
- *(b)* $\mathbb{E}$ *is stable*
- *(c)* $\mathbb{K} \le \mathbb{E}$ *is normal.*

Proof. (a) follows from 4.3.6(b:b) (applied to $H = G$ and so $\mathcal{F}H = \mathbb{K}$).

(b) By 4.3.15(f) (b:a) and (b:b) are equivalent. By 4.3.7 (b:b) and (b:c) are equivalent. □

Theorem 4.3.17. *Let* $\mathbb{K} \le \mathbb{F}$ *be an algebraic field extension. Then the following are equivalent:*

(a) $\mathbb{K} \le \mathbb{F}$ *is Galois*

(b) $\mathbb{K} \le \mathbb{F}$ *is separable and normal.*

(c) $\mathbb{F}$ *is the splitting field of a set over separable polynomials over* $\mathbb{K}$.

Proof. (a) $\Longrightarrow$ (b): Suppose first that $\mathbb{K} \le \mathbb{F}$ is Galois and put $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then $\mathbb{K} = \mathcal{F}G$. So by 4.3.16(a) $\mathbb{K} \le \mathbb{F}$ is separable. Since $\mathbb{F}$ is closed and $\mathcal{G}\mathbb{F} = \{\mathrm{id}_{\mathbb{F}}\} \trianglelefteq G$, 4.3.16(b) gives that $\mathbb{K} \le \mathbb{F}$ is normal.

(b) $\Longrightarrow$ (a): Suppose next that $\mathbb{K} \le \mathbb{F}$ is normal and separable. Since $\mathbb{K} \le \mathbb{F}$ is normal 4.2.26(h), shows that $\mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})) = \mathbb{P}(\mathbb{K}, \mathbb{F})$. Since $\mathbb{K} \le \mathbb{F}$ is separable, $\mathbb{P}(\mathbb{K}, \mathbb{F}) = \mathbb{K}$ and so $\mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})) = \mathbb{K}$ and $\mathbb{K} \le \mathbb{F}$ is Galois.

(b) $\Longrightarrow$ (c): By 4.2.10(c) , $\mathbb{F}$ is the splitting field of some $P \subseteq \mathbb{K}[x]$ over $\mathbb{K}$. Let $0 \neq f \in P$ and g an irreducible factor of f. Then $g(b) = 0$ for some $b \in \mathbb{F}$. Since $\mathbb{K} \le \mathbb{F}$ is seperable, b and so also g is seperable over $\mathbb{K}$. So f is separable over $\mathbb{K}$ and (c) holds.

(b) $\Longrightarrow$ (c): Suppose $\mathbb{F}$ is the the splitting field of a set P of separable polynomials over $\mathbb{K}$. 4.2.10(c) implies that $\mathbb{K} \le \mathbb{F}$ is normal. Put

$$A = \{b \in \mathbb{F} \mid f(b) = 0 \text{ for some } 0 \neq f \in P\}$$

By definition of a splitting field, $\mathbb{F} = \mathbb{K}[A]$. Since each $f \in P$ is separable, each $a \in A$ is separable over $\mathbb{F}$. Thus by 4.2.28(b), $\mathbb{K} \le \mathbb{F}$ is separable. □

Proposition 4.3.18. *Suppose that $\mathbb{K} \le \mathbb{F}$ is algebraic and Galois. Let $\mathbb{K} \le \mathbb{E} \le \mathbb{F}$ and put $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ and $H = \mathcal{G}(\mathbb{E})$. Then*

(a) $H = \mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$, $\mathbb{E} \le \mathbb{F}$ is Galois and $\mathbb{E} = \mathcal{F}(H)$ is closed .

(b) $\mathbb{K} \le \mathbb{E}$ is Galois if and only if $\mathcal{G}\mathbb{E}$ is normal in G.

(c) $\mathbb{E}$ is $\mathrm{N}_G(H)$-stable and $\mathrm{N}_G(H)/H \cong \mathrm{N}_G(H)^{\mathbb{E}} = \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$

Proof. (a) We have $H = \mathcal{G}E = \mathrm{Stab}_G(\mathbb{E}) = \mathrm{Aut}_{\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})}(\mathbb{F}) = \mathrm{Aut}_{\mathbb{E}}(\mathbb{F})$. By 4.3.17(a),(b) $\mathbb{K} \le \mathbb{F}$ is normal and separable. Hence by 4.2.9 $\mathbb{E} \le \mathbb{F}$ is normal and by 4.2.21 $\mathbb{E} \le \mathbb{F}$ is separable. So by 4.3.17, $\mathbb{E} \le \mathbb{F}$ is Galois. This implies that

$$\mathbb{E} = \mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{E}}(\mathbb{F})) = \mathcal{F}(\mathcal{G}\mathbb{E}) = \mathcal{F}H$$

and so $\mathbb{E}$ is closed.

(b) As $\mathbb{K} \le \mathbb{F}$ is separable, $\mathbb{K} \le \mathbb{E}$ is separable. Hence by 4.3.17 $\mathbb{K} \le \mathbb{E}$ is Galois if and only if $\mathbb{K} \le \mathbb{E}$ is normal. Since $\mathbb{E}$ is closed, (b) now follows from 4.3.16(b).

(c) Let $g \in \mathrm{N}_G(\mathcal{G}E)$-stable. Since $\mathcal{F}(H) = \mathbb{E}$ we conclude from 4.3.15(b) that

$$g(\mathbb{E}) = g(\mathcal{F}H) = \mathcal{F}({}^gH) = \mathcal{F}(H) = \mathbb{E}$$

So $\mathbb{E}$ is $\mathrm{N}_G(\mathcal{G}E)$-stable. Hence by 1.7.10(b) $\mathrm{N}_G(H)/\mathcal{G}E \cong \mathrm{N}_G(H)^{\mathbb{E}}$.

Clearly $\mathrm{N}_G(H)^{\mathbb{E}} \le \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$. Let $h \in \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$. Since $\mathbb{K} \le \mathbb{F}$ is normal, $\mathbb{F}$ is a splitting filed over $\mathbb{K}$ and so by 4.2.7 $h = g|_{\mathbb{E}}$ for some $g \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then $g(\mathbb{E}) = \mathbb{E}$ and so by 4.3.15(a),

$${}^gH = {}^g\mathcal{G}(\mathbb{E}) = \mathcal{G}(g(\mathbb{E})) = \mathcal{G}(\mathbb{E}) = H.$$

Thus $g \in \mathrm{N}_G(H)$ and $h \in \mathrm{N}_G(H)^{\mathbb{E}}$. Hence (c) holds. □

Definition 4.3.19. *Let $\mathbb{K} \leq \mathbb{E}$ be an algebraic field extension. A* normal closure *of $\mathbb{K} \leq \mathbb{E}$ is an extension $\mathbb{L}$ of $\mathbb{E}$ such that $\mathbb{K} \leq \mathbb{L}$ is normal and no proper proper subfield of $\mathbb{L}$ containing $\mathbb{E}$ is normal over $\mathbb{K}$.*

Lemma 4.3.20. *Let $\mathbb{K} \leq \mathbb{E}$ be an algebraic field extension.*

(a) Suppose $\mathbb{E} = \mathbb{K}(I)$ for some $I \subseteq \mathbb{E}$ and let $\mathbb{E} \leq \mathbb{L}$ be a field extension. Then the following are equivalent:

  (a) $\mathbb{L}$ is a normal closure of $\mathbb{K} \leq \mathbb{E}$.

  (b) $\mathbb{L}$ is a splitting field for $\{m_b^{\mathbb{K}} \mid b \in I\}$ over $\mathbb{K}$.

  (c) $\mathbb{L}$ is a splitting field for $\{m_b^{\mathbb{K}} \mid b \in I\}$ over $\mathbb{E}$.

(b) There exists a normal closure $\mathbb{L}$ of $\mathbb{K} \leq \mathbb{E}$ and $\mathbb{L}$ is unique up to $\mathbb{E}$-isomorphism.

(c) Let $\mathbb{L}$ be a normal closure of $\mathbb{K} \leq \mathbb{E}$. Then

  (a) $\mathbb{K} \leq \mathbb{L}$ is finite if and only if $\mathbb{K} \leq \mathbb{E}$ is finite.

  (b) $\mathbb{K} \leq \mathbb{L}$ is Galois if and only if $\mathbb{K} \leq \mathbb{L}$ is separable and if and only if $\mathbb{K} \leq \mathbb{E}$ is separable.

(d) Let $\overline{\mathbb{E}}$ be an algebraic closure of $\mathbb{E}$. Then

  (a) $\overline{\mathbb{E}}$ is an algebraic closure of $\mathbb{K}$.

  (b) $\overline{\mathbb{E}}$ contains a unique normal closure $\mathbb{L}$ of $\mathbb{K} \leq \mathbb{E}$. $\mathbb{L}$ is called the normal closure of $\mathbb{K} \leq \mathbb{E}$ in $\overline{\mathbb{E}}$.

Proof. (a) Put $P = \{m_b^{\mathbb{K}} \mid b \in I\}$, $A = \{b \in \mathbb{L} \mid f(b) = 0_{\mathbb{K}} \text{ for some } b \in \mathbb{L}\}$ and $\mathbb{D} = \mathbb{K}(A)$. Note that $b \in A$ for all $b \in I$ and so

$$(*) \qquad \mathbb{E} = \mathbb{K}(I) \leq \mathbb{D}$$

Next we show:

(**) Let $\mathbb{K} \leq \mathbb{F} \leq \mathbb{L}$ such that $\mathbb{K} \leq \mathbb{F}$ is normal. Then $\mathbb{D} \subseteq \mathbb{F}$ and $\mathbb{K} \leq \mathbb{D}$ is normal.

Note that each $m_b^{\mathbb{K}}, b \in I$ has a root in $\mathbb{L}$, namely b. Since $\mathbb{K} \leq \mathbb{F}$ is normal each $m_b^{\mathbb{K}}$ splits over $\mathbb{L}$. So $A \subseteq \mathbb{F}$, $\mathbb{D} = \mathbb{K}[A] \leq \mathbb{F}$ and $\mathbb{D}$ is a splitting field for P over $\mathbb{K}$. Thus by 4.2.10(c), $\mathbb{K} \leq \mathbb{D}$ is normal.

(a:a) $\Longrightarrow$ (a:b): Suppose first that $\mathbb{L}$ is a normal closure of $\mathbb{K} \leq \mathbb{E}$. Then $\mathbb{K} \leq \mathbb{L}$ is normal and so by (**) $\mathbb{K} \leq \mathbb{D}$ is normal. By (*) $\mathbb{E} \leq \mathbb{D}$ and so the definition of a normal closure implies $\mathbb{L} = \mathbb{D}$.

(a:b) $\Longrightarrow$ (a:c): Suppose next $\mathbb{L}$ is a splitting field of P over $\mathbb{K}$. Then $\mathbb{L} = \mathbb{K}[\mathbb{A}] = \mathbb{E}[A]$ and $\mathbb{L}$ is also a splitting field for P over $\mathbb{E}$.

(a:c) $\Longrightarrow$ (a:a): Suppose next that $\mathbb{L}$ is a splitting field of P over $\mathbb{E}$. Then $\mathbb{L} = \mathbb{E}[A]$ and $\mathbb{D}$ is a splitting field for P over $\mathbb{E}$. Hence by 4.2.10(c), $\mathbb{K} \leq \mathbb{D}$ is normal. By (*) $\mathbb{E} \leq \mathbb{D}$ and so $\mathbb{L} = \mathbb{E}[A] \leq \mathbb{D} \leq \mathbb{L}$. Thus $\mathbb{L} = \mathbb{D}$ and $\mathbb{K} \leq \mathbb{L}$ is normal. If $\mathbb{K} \leq \mathbb{F} \leq \mathbb{L}$ and $\mathbb{K} \leq \mathbb{F}$ is normal, then by (**) $\mathbb{D} \leq \mathbb{F}$. Since $\mathbb{D} = \mathbb{L}$ and $\mathbb{F} \leq \mathbb{L}$ we get $\mathbb{F} = \mathbb{L}$ and so $\mathbb{L}$ is a normal closure of $\mathbb{K} \leq \mathbb{E}$.

(b) By (a) applied with $I = \mathbb{E}$ a normal closure of $\mathbb{K} \le \mathbb{E}$ is the same as splitting field of $\{m_b^{\mathbb{K}} \mid b \in \mathbb{E}\}$. Thus by 4.1.22 $\mathbb{K} \le \mathbb{E}$ has a normal closure and by 4.2.7(b), the normal closure is unique up to $\mathbb{K}$-isomorphism.

(c:a) If $\mathbb{K} \le \mathbb{E}$ is finite, then $\mathbb{E} = \mathbb{K}(I)$ for some finite subset I of $\mathbb{E}$. Note the splitting field of a finite set of polynomials over $\mathbb{K}$ is a finite extension of $\mathbb{K}$ So $\mathbb{K} \le \mathbb{L}$ is finite by (a).

(c:b) Suppose that if $\mathbb{K} \le \mathbb{L}$ is Galois. Then by 4.3.17 $\mathbb{K} \le \mathbb{L}$ is separable. If $\mathbb{K} \le \mathbb{L}$ is separable, then also $\mathbb{K} \le \mathbb{E}$ is separable. So suppose $\mathbb{K} \le \mathbb{E}$ is separable, then by (a), $\mathbb{L}$ is the splitting field of the set of separable polynomials $\{\{m_b^{\mathbb{K}} \mid b \in \mathbb{E}\}$ and so by 4.3.17, $\mathbb{K} \le \mathbb{L}$ is Galois.

(d:a) Since $\mathbb{K} \le \mathbb{E}$ and $\mathbb{E} \le \overline{\mathbb{E}}$ are algebraic, $\mathbb{K} \le \overline{\mathbb{E}}$ is algebraic (4.1.15. Also $\overline{\mathbb{E}}$ is algebraicly closed and thus (d:a) holds.

(d:b) Let $\mathbb{E} \le \mathbb{L} \le \overline{\mathbb{E}}$. Then by (a) $\mathbb{L}$ is a normal closure of $\mathbb{K} \le \mathbb{E}$ if and only if $\mathbb{L}$ is generated by $\mathbb{K}$ and all the roots of the $m_b^{\mathbb{K}}, b \in \mathbb{E}$. So (d:b) holds. □

Lemma 4.3.21. *Let* $\mathbb{K} \le \mathbb{E}$ *be a normal field extension. Put* $\mathbb{P} = \mathbb{P}(\mathbb{K}, \mathbb{E})$ *and* $\mathbb{S} = \mathbb{S}(\mathbb{K}, \mathbb{E})$. *Then* $\mathbb{P} = \mathrm{Fix}_{\mathbb{E}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}))$, $\mathbb{K} \le \mathbb{P}$ *is purely inseparable,* $\mathbb{P} \le \mathbb{E}$ *is Galois,* $\mathbb{K} \le \mathbb{S}$ *is Galois and the map*

$$\tau : \mathrm{Aut}_{\mathbb{K}}(\mathbb{E}) \to \mathrm{Aut}_{\mathbb{K}}(\mathbb{S}), \phi \to \phi|_{\mathbb{E}}$$

is an isomorphism of groups.

Proof. By definition $\mathbb{K} \le \mathbb{P}$ is purely inseparable. By 4.2.26(e), 4.2.26 f, $\mathbb{P} = \mathrm{Fix}_{\mathbb{E}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}))$ and so by 4.3.12 (applied with $\mathbb{F} = \mathbb{E}$ and $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$) $\mathbb{P} \le \mathbb{E}$ is Galois.

Let $\phi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$ and $s \in \mathbb{S}$. Then $\phi(s)$ is a root of $m_s^{\mathbb{K}}$. Since s is separable over $\mathbb{K}$, we conclude that $\phi(s)$ is separable over $\mathbb{K}$. So $\phi(s) \in \mathbb{K}$. Thus $\mathbb{S}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$ stable and so by 4.3.7, $\mathbb{K} \le \mathbb{S}$ is normal. $\mathbb{K} \le \mathbb{S}$ is separable and thus by 4.3.17, $\mathbb{K} \le \mathbb{S}$ is Galois. Let $\phi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$ with $\phi|_{\mathbb{S}} = \mathrm{id}_{\mathbb{S}}$. Then $\mathbb{S} \subseteq \mathrm{Fix}_{\mathbb{F}}(\phi)$. By definition of $\mathbb{P}$, $\mathbb{P} \le \mathrm{Fix}_{\mathbb{F}}(\phi)$. By 4.2.31(b), $\mathbb{E} = \mathbb{S}\mathbb{P}$. Hence $\mathbb{E} \le \mathrm{Fix}_{\mathbb{E}}(\phi)$ and $\phi = \mathrm{id}_{\mathbb{E}}$. Thus τ is 1-1. Let $\psi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{S})$. Since $\mathbb{K} \le \mathbb{E}$ is normal is normal, we conclude from 4.2.7(a) that $\psi = \phi|_{\mathbb{S}}$ for some $\phi \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$. So τ is onto. □

4.4 The Fundamental Theorem of Algebra

In this section we show that the field $\mathbb{C}$ of complex numbers is algebraically closed. Our proof is based on the following well known facts from analysis which we will not prove:

Every polynomial $f \in \mathbb{R}[x]$ of odd degree has a root in $\mathbb{R}$.
Every polynomials of degree 2 over $\mathbb{C}$ is reducible.
$\dim_{\mathbb{R}} C = 2$.

Some remarks on this assumptions. The first follows from the intermediate value theorem and the fact that any odd polynomial has positive and negative values. The second follows from the quadratic formula and the fact that every complex number has a complex square root ($\sqrt{re^{\phi i}} = \sqrt{r}e^{\frac{\phi}{2}i}$). The last property follows from $\mathbb{C} = \mathbb{R} + \mathbb{R}i$.

Definition 4.4.1. *Let s be a prime,* $\mathbb{K} \le \mathbb{F}$ *a finite field extension and* $f \in \mathbb{K}[x]$.

(a) f is a s'-polynomial if s does not divide $\deg f$

(b) $\mathbb{K} \le \mathbb{E}$ is a s'-extension s does not divide $\dim_{\mathbb{K}} \mathbb{F}$.

Lemma 4.4.2. *Let $\mathbb{K}$ be a field and s a prime. Then the following are equivalent.*

(a) Every irreducible s'-polynomial over $\mathbb{K}$ has degree 1.

(b) Every s'-polynomial over $\mathbb{K}$ has a root in $\mathbb{K}$

(c) If $\mathbb{K} \le \mathbb{E}$ is a s' extension then $\mathbb{K} = \mathbb{E}$.

Proof. (a) $\Longrightarrow$ (b): Let $f \in \mathbb{K}[x]$ with $s \nmid \deg f$. Let $f = f_1 \dots f_k$ with f_i irreducible. Then $\deg f = \sum_{i=1}^{k} \deg f_i$ and so $s \nmid f_i$ for some $1 \le i \le k$. By (a) , f_i has degree 1. Hence f_i and so also f has a root in $\mathbb{K}$.

(b) $\Longrightarrow$ (c): Let $\mathbb{K} \le \mathbb{E}$ be an s'-extension and $b \in \mathbb{E}$. Then $\deg m_b^{\mathbb{K}} = \dim_{\mathbb{K}} \mathbb{K}[b]$ divides $\dim_{\mathbb{K}} \mathbb{E}$. Hence $m_b^{\mathbb{K}}$ is an irreducible s' polynomial and so by (a) has a root d in $\mathbb{K}$. As f is irreducible we get $b = d \in \mathbb{K}$ and $\mathbb{E} = \mathbb{K}$.

(c) $\Longrightarrow$ (a): Let f be irreducible s'-polynomial. Then $\mathbb{K}[x]/f\mathbb{K}[x]$ is an extension of degree $\deg f$. So its is an s'-extension of $\mathbb{K}$ and by (c), $\deg f = 1$. □

Lemma 4.4.3. *Let $\mathbb{K} \le \mathbb{F}$ be a finite purely inseparable extension. Put $p = \operatorname{char} \mathbb{K}$. If $p = 0$, then $\mathbb{K} = \mathbb{F}$ and if $p \neq 0$, then $\dim_{\mathbb{K}} \mathbb{F} = p^m$ for some $m \in \mathbb{N}$.*

Proof. If $p = 0$, then $\mathbb{K} \le \mathbb{F}$ is separable and so $\mathbb{K} = \mathbb{F}$. So suppose $p \neq 0$. We proceed by induction on $\dim_{\mathbb{K}} \mathbb{F}$. If $\dim_{\mathbb{K}} \mathbb{F} = 1$, then $\mathbb{K} = \mathbb{F}$. So suppose $\dim_{\mathbb{K}} \mathbb{F} > 1$ and let $b \in \mathbb{F} \smallsetminus \mathbb{K}$. By 4.2.23 there exists $n \in \mathbb{N}$ such that b^{p^n} is separable over $\mathbb{K}$ and $\dim_{\mathbb{K}[b^{p^n}]} \mathbb{K}[b] = p^n$. Since $b^{p^n} \in \mathbb{F}$ and $\mathbb{K} \le \mathbb{F}$ is purely inseparable, $b^{p^n} \in \mathbb{K}$ and so $\dim_{\mathbb{K}} \mathbb{K}[b] = p^n$. By Homework 3#6 $\mathbb{K}[b] \le \mathbb{F}$ is purely inseparable and so by induction $\dim_{\mathbb{K}[b]} \mathbb{E} = p^l$ for some $l \in \mathbb{N}$. Thus by the dimension formula 4.1.5(c), $\dim_{\mathbb{K}} \mathbb{E} = p^n p^l = p^{k+l}$. □

Proposition 4.4.4. *Let $\mathbb{K} \le \mathbb{F}$ be an algebraic extension and s a prime. Suppose that*

(i) Every s'-polynomial over $\mathbb{K}$ has a root in $\mathbb{K}$.

(ii) All polynomials of degree s over $\mathbb{F}$ are reducible.

Then $\mathbb{F}$ is algebraically closed.

Proof. Let $\overline{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$ and $b \in \overline{\mathbb{F}}$. We need to show that $b \in \mathbb{F}$. For this let $\mathbb{E}$ a normal closure of $\mathbb{K} \le \mathbb{K}[b]$ in $\overline{F}$. By 4.3.20(c:a), $K \le \mathbb{E}$ is finite.

Put $\mathbb{P} = \mathbb{P}(\mathbb{K}, \mathbb{E})$. By 4.3.21 $\mathbb{K} \le \mathbb{P}$ is purely inseparable and $\mathbb{P} \le \mathbb{E}$ is Galois. We will show that

$$(*) \qquad \mathbb{P} \le \mathbb{F}$$

If $\operatorname{char} p = 0$, then $\mathbb{P} = \mathbb{K}$. So suppose $\operatorname{char} K = p$, p a prime. Assume first that $p \neq s$, then by 4.4.3 $\mathbb{K} \le \mathbb{P}$ is an s'-extension and so by 4.4.2 $\mathbb{P} = \mathbb{K}$. Assume next that $p = s$ and suppose first exits

$b \in \mathbb{P} \smallsetminus \mathbb{F}$. By 4.2.26(a),$b^{p^n} \in \mathbb{K}$ for some $n \in \mathbb{N}$. Hence we can choose $n \in \mathbb{Z}^+$ minimal with $b^{p^n} \in \mathbb{F}$. Put $a = b^{pn-1}$. Then $a \in \mathbb{P} \smallsetminus \mathbb{F}$ and $a^p \in \mathbb{F}$. 4.2.20 implies $\deg m_a^{\mathbb{K}} = p = s$, a contradiction to (ii). Thus (*) holds.

Put $\mathbb{S} = \mathbb{S}(\mathbb{K}, \mathbb{E})$. Then by 4.3.21, $\mathbb{K} \le \mathbb{S}$ is Galois. Put $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{S})$. Since $\mathbb{K} \le \mathbb{E}$ is finite, G is finite.

By 1.10.9 there exists a Sylow s-subgroup S of G. Put $\mathbb{L} = \mathrm{Fix}_{\mathbb{S}}(S)$. Then by the FTGT, 4.3.13 $\dim_{\mathbb{L}} \mathbb{S} = |S|$ and so

$$\dim_{\mathbb{K}} \mathbb{L} = \frac{\dim_{\mathbb{K}} \mathbb{S}}{\dim_{\mathbb{K}} \mathbb{L}} = \frac{|G|}{|S|}$$

Since S is a Sylow s-subgroup we conclude that $\mathbb{K} \le \mathbb{L}$ is a s' extension. Thus by 4.4.2 $\mathbb{L} = \mathbb{K}$ and so $G = S$. Thus G is a s-group. Since $\mathbb{K} \le \mathbb{S} \cap \mathbb{F} \le \mathbb{S}$, 4.3.13 implies $\mathbb{S} \cap \mathbb{F} = \mathrm{Fix}_{\mathbb{S}}(H)$ for some $H \le G$.

Suppose for a contradiction that $H \neq \{\mathrm{id}_{\mathbb{S}}\}$. Let T be a maximal subgroup of H. By 1.7.38(b), $T \not\trianglelefteq \mathrm{N}_H(T)$. Since T is maximal we get $T \trianglelefteq H$ and $|H/T| = s$. Put $\mathbb{D} = \mathrm{Fix}_{\mathbb{S}}(T)$. Then $\dim_{\mathbb{S} \cap \mathbb{F}} \mathbb{D} = |H/T| = p$. Let $d \in \mathbb{D} \smallsetminus (\mathbb{S} \cap \mathbb{F})$. Then $\deg m_d^{\mathbb{S} \cap \mathbb{F}} = s$. By 4.2.12 $m_d^{\mathbb{S} \cap \mathbb{F}} = m_d^{\mathbb{F}}$ and so $\deg m_d^{\mathbb{F}} = s$ a contradiction to (ii).

Thus $H = \{\mathrm{id}_{\mathbb{S}}\}$ and so $\mathbb{S} \cap \mathbb{F} = \mathrm{Fix}_{\mathbb{S}}(\mathrm{id}_{\mathbb{S}}) = \mathbb{S}$. Thus $\mathbb{S} \le \mathbb{F}$. Together with (*) we get $\mathbb{S}\mathbb{P} \le \mathbb{F}$. By 4.2.31(b), $\mathbb{E} = \mathbb{P}\mathbb{S}$ and so $\mathbb{E} \le \mathbb{F}$. Since $b \in \mathbb{E}$ we have $b \in \mathbb{F}$. As $b \in \overline{\mathbb{F}}$ was arbitrary this means, $\mathbb{F} = \overline{\mathbb{F}}$ and so $\mathbb{F}$ is algebraically closed. □

Theorem 4.4.5. *The field of complex numbers is algebraically closed.*

Proof. By the three properties of $\mathbb{R} \le \mathbb{C}$ listed above we can apply 4.4.4 with $s = 2$. Hence $\mathbb{C}$ is algebraically closed. □

Lemma 4.4.6. *Let $\mathbb{K} \le \mathbb{E}$ be algebraic and $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$. Then $\mathbb{E}$ is $\mathbb{K}$-isomorphic to some intermediate field $\tilde{\mathbb{E}}$ of $\mathbb{K} \le \overline{\mathbb{K}}$.*

Proof. Let $\overline{\mathbb{E}}$ be an algebraic closure of $\mathbb{E}$. Then by 4.3.20(d:a) $\overline{\mathbb{E}}$ is an algebraic closure of $\mathbb{K}$. By 4.2.7(e) there exists an $\mathbb{K}$-isomorphism $\phi : \overline{\mathbb{E}} \to \overline{\mathbb{K}}$. Put $\tilde{\mathbb{E}} = \phi(\mathbb{E})$. □

Lemma 4.4.7. *Up to $\mathbb{R}$-isomorphisms, $\mathbb{C}$ is the only proper algebraic extension of $\mathbb{R}$*

Proof. Note that $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. So by 4.4.6 any algebraic extension of $\mathbb{R}$ is $\mathbb{R}$-isomorphic to an intermediate field $\mathbb{E}$ of $\mathbb{R} \le \mathbb{C}$. As $\dim_{\mathbb{R}} \mathbb{C} = 2$, we get $\mathbb{E} = \mathbb{R}$ or $\mathbb{E} = \mathbb{C}$. □

4.5 Finite Fields

In this section we study the Galois theory of finite fields.

Lemma 4.5.1. *Let $\mathbb{F}$ be a finite field and $\mathbb{F}_0$ the subring generated by 1. Then $\mathbb{F}_0 \cong \mathbb{Z}_p$ for some prime p. In particular, $\mathbb{F}$ is isomorphic to a subfield of the algebraic closure of $\mathbb{Z}_p$.*

Proof. Let $p = \operatorname{char}\mathbb{F}$. Then $p\mathbb{Z}$ is the kernel of the homomorphism $\mathbb{Z} \to \mathbb{F}$, $n \to n1_{\mathbb{F}}$. Also $\mathbb{F}_0$ is its image and so $\mathbb{F}_0 \cong \mathbb{Z}_p$. □

Theorem 4.5.2. *Let p be a prime, $\mathbb{F}_0$ a field of order p, $\mathbb{F}$ an algebraic closure of $\mathbb{F}_0$ and $G := \{\operatorname{Frob}^{\mathbb{F}}_{p^n} \mid n \in \mathbb{Z}\}$*

(a) Let $n \in \mathbb{Z}^+$ and $q = p^n$. Let $\mathbb{F}_q$ be the set of roots of $x^q - x$. Then

$$\mathbb{F}_q = \{a \in \mathbb{F} \mid a^q = a\} = \operatorname{Fix}_{\mathbb{F}}(\operatorname{Frob}_q) = \mathcal{F}(\langle \operatorname{Frob}_q \rangle)$$

and $\mathbb{F}_q$ is a subfield field of order q.

(b) $\mathbb{F}_0 = \mathbb{F}_p = \mathcal{F}G = \operatorname{Fix}_{\mathbb{F}}(\operatorname{Frob}_p)$.

(c) G is an infinite cyclic subgroup of $\operatorname{Aut}(\mathbb{F})$.

(d) Let $\mathbb{E}$ be a proper subfield of $\mathbb{F}$. Then $\mathbb{E}$ is closed if and only if $\mathbb{E} = \mathbb{F}_{p^n}$ for some $n \in \mathbb{Z}^+$ and if and only if $\mathbb{F}$ is finite.

(e) All subgroups of G are closed.

(f) $\mathcal{G}$ is a inclusion reversing bijection between the finite subfields of $\mathbb{F}$ and the non-trivial subgroups of G.

(g) $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$ if and only if m divides n.

(h) Let $n, m \in \mathbb{Z}^+$ and $q = p^n$. Then $\mathbb{F}_q \leq \mathbb{F}_{q^m}$ is a Galois extension and

$$\operatorname{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = \{\operatorname{Frob}_{q^i} \mid 0 \leq i < m.\}$$

In particular, $\operatorname{Aut}_{\mathbb{F}_q}\mathbb{F}_{q^m}$ is cyclic of order m.

Proof. (a) Note that $(x^q - x)' = qx^{q-1} - 1 = -1$ has no roots and so by 4.2.15(d) $x^q - x$ has no multiple roots. Hence $|\mathbb{F}_q| = q$. Since $a^q - a = 0$ if and only if $a^q = a$ and if and only if $\operatorname{Frob}_q(a) = a$ we see that (a) holds.

(b) Since $\mathbb{F}_0 \leq \mathbb{F}_p$ and $|\mathbb{F}_0| = p = |\mathbb{F}_p|$, $\mathbb{F}_0 = \mathbb{F}_p$. Also $G = \langle \operatorname{Frob}_p \rangle$ and so (c) follows from (a).

(c) Since $\mathbb{F}_q \neq \mathbb{F}$, $\operatorname{Frob}_q = \operatorname{Frob}_p^n \neq \operatorname{id}_{\mathbb{F}}$ and so Frob_p has infinite order. This proves (c).

(d) Let $\mathbb{E}$ be a proper field of $\mathbb{F}$. Then $E = \mathbb{F}H$ for some $1 \neq H \leq G$. Since $G = \langle \operatorname{Frob}_p \rangle$. Then $H = \langle \operatorname{Frob}_p^n \rangle = \langle \operatorname{Frob}_{p^n} \rangle$ for some $n \in \mathbb{Z}^+$ and so by (a), $\mathbb{E} = \mathcal{F}(\langle \operatorname{Frob}_{p^n} \rangle) = \mathbb{F}_{p^n}$.

By (b) $\mathbb{F}_{p^n}$ has order p^n and so is finite.

Suppose $\mathbb{E}$ is finite. Then $\mathbb{F}_0 \leq \mathbb{E}$ is finite. finite. Since $\mathbb{F}_0$ is closed, 4.3.10(b) shows that $\mathbb{E}$ is closed. Thus (d) holds.

(e) Let $H \leq G$. If $H = 1$, then H is closed. So suppose $H \neq 1$. Then $H = \langle \operatorname{Frob}_q \rangle$, where $q = p^n$ with $n \in \mathbb{Z}^+$. Since $\mathbb{F}_q$ is closed we have

$$\mathcal{F}({}^{G}\mathbb{F}_q) = \mathbb{F}_q$$

Note that $\langle \mathrm{Frob}_q \rangle$ is the only subgroup of G with fixed field of order q and so $\mathcal{G}(\mathbb{F}_q) = \langle \mathrm{Frob}_q \rangle = H$. Thus H is closed and (e) is proved.

(f) Since $\mathcal{G}$ is an inclusion reversing bijection between the non-trivial closed subgroups of G and the proper closed subfields of $\mathbb{F}$, (f) follows from (d) and (e).

(a) Note that

$$\mathbb{F}_{p^m} \le \mathbb{F}_{p^n} \qquad \Longleftrightarrow \qquad \mathcal{G}\mathbb{F}_{p^n} \le \mathcal{G}\mathbb{F}_{p^m} \qquad \Longleftrightarrow \qquad \langle \mathrm{Frob}_{p^n} \rangle \le \langle \mathrm{Frob}_{p^m} \rangle.$$

Since $\mathrm{Frob}_{p^n} = \mathrm{Frob}_p^n$ and Frob_p has infinite order this holds if and only if $m \mid n$.

(h) Since H is abelian, all subgroups of H are normal. Hence by 4.3.16 (applied to $(\mathbb{F}, \mathbb{F}_q, H)$ in place of $(\mathbb{F}, \mathbb{K}, G)$) $\mathbb{F}_{q^m}$ is H-stable. Thus by 4.3.14 (again applied with H in place of G) $\mathbb{F}_q \le \mathbb{F}_{q^m}$ is Galois and $\mathrm{Aut}_{\mathbb{F}_q}\mathbb{F}_{q^m} = H^{\mathbb{F}_{qm}}$. By 4.3.15b,

$$H^{\mathbb{F}_{q^m}} \cong H/\mathcal{F}\mathbb{F}_{q^m} = \langle \mathrm{Frob}_q \rangle / \langle \mathrm{Frob}_{q^m} \rangle \cong \mathbb{Z}/m\mathbb{Z}.$$

Thus (h) holds. □

4.6 Transcendence Basis

Definition 4.6.1. *Let $\mathbb{K} \le \mathbb{F}$ be a field extension and $s = (s_i)_{i \in I}$ a family of elements in $\mathbb{F}$. We say that $(s_i)_{i \in I}$ is* algebraically independent *over $\mathbb{K}$ if the evaluation homomorphism:*

$$\Phi_s : \mathbb{K}[X_I] \to \mathbb{K}[s_i, i \in I], \ f \to f(s)$$

is isomorphism.

A subset S of $\mathbb{F}$ is called algebraically independent over $\mathbb{K}$, if $(s)_{s \in S}$ is algebraically independent.

s is called algebraically dependent over $\mathbb{K}$ if s is not algebraically independent over $\mathbb{K}$.

Remark 4.6.2. *Let $\mathbb{K} \le \mathbb{F}$ be a field and $s = (s_i)_{i \in I}$ a family of elements in $\mathbb{F}$.*

(a) s is algebraically dependent over $\mathbb{K}$ if and only if Φ_s is not 1-1 and only if there exists $0 \ne f \in \mathbb{K}[X_I]$ with $f(s) = 0$

(b) s is algebraically independent over $\mathbb{K}$ if and only if $s_i \ne s_j$ for all $i \ne j$ and $\{s_i \mid i \in I\}$ is algebraically independent over $\mathbb{K}$.

(c) s is algebraically dependent over $\mathbb{K}$ if and only if for a finite subsets J of I, $(s_j)_{j \in J}$ is algebraically independent over $|K$.

(d) Let $b \in \mathbb{K}$. Then $\{b\}$ is algebraically independent over $\mathbb{K}$ if and only if b is transcendental over $\mathbb{K}$.

Lemma 4.6.3. *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $s = (s_i)_{i \in I}$ be algebraically independent family in $\mathbb{F}$ over $\mathbb{K}$. Then there exists a unique $\mathbb{K}$-isomorphism $\tilde{\Phi}_s : \mathbb{K}(X_I) \to \mathbb{K}(s_i | i \in I)$ with $\Phi(x_i) = s_i$ for all $i \in I$. Moreover, $\tilde{\Phi}_s(\frac{f}{g}) = f(s)g(s)^{-1}$ for all $f, g \in \mathbb{K}[X_I]$, $g \neq 0$.*

Proof. Since s is algebraic independent, $f(s) \neq 0$ for all $0 \neq f \in \mathbb{K}[x]$. So $f(s)$ is invertible in $\mathbb{F}$. Hence by 2.7.1(h) there exists a unique ring homomorphism

$$\tilde{\Phi}_s : \mathbb{K}(X_I) \to \mathbb{F}$$

with $\tilde{\Phi}_s(f) = f(s)$ for all $f \in \mathbb{K}[X_I]$. Moreover,

$$\tilde{\Phi}_s\left(\frac{f}{g}\right) = f(s)g(s)^{-1}$$

Since $\tilde{\Phi}_s$ is non-zero homomorphism of fields, Φ is 1-1. Clearly $\operatorname{Im}\Phi_s = \mathbb{K}(s_i \mid i \in I)$ and so the lemma is proved. □

Lemma 4.6.4. *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension.*

(a) Let S and T disjoint subsets of $\mathbb{F}$. Then $S \cup T$ is algebraically independent over $\mathbb{K}$ if and only if S is algebraically independent over $\mathbb{K}$ and T is algebraically independent over $\mathbb{K}(S)$.

(b) Let $S \subseteq \mathbb{F}$ be algebraically independent over $\mathbb{K}$ and let $b \in \mathbb{F} \setminus S$. Then $S \cup \{b\}$ is algebraically independent over $\mathbb{K}$ if and only if b is transcendental over $\mathbb{K}$.

Proof. (a) By 4.6.3 $S \cup T$ is algebraically independent over $\mathbb{K}$ if and only if the there exists an $\mathbb{K}$-isomorphism

$$\mathbb{K}(X_{S \cup T}) \to \mathbb{K}(S \cup T) \text{ with } x_r \to r, \forall r \in S \cup T.$$

Applying 4.6.3 two more times, S is algebraically independent over $\mathbb{K}$ and T is algebraically independent over $\mathbb{K}(S)$ if and only if there exists $\mathbb{K}$-isomorphism

$$\mathbb{K}(X_S)(X_T) \to \mathbb{K}(S)(T) \text{ with } x_s \to s, \forall s \in S \text{ and } x_t \to t, \forall t \in T.$$

Since $\mathbb{K}(S \cup T) = \mathbb{K}(S)(T)$ and $\mathbb{K}(X_{S \cup T})$ is canonically isomorphic to $\mathbb{K}(X_S)(X_T)$ we conclude that (a) holds.

(b) Follows from (a) applied to $T = \{b\}$. □

Definition 4.6.5. *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension. A* transcendence basis *for $\mathbb{K} \leq \mathbb{F}$ is a algebraically independent subset S of $\mathbb{K} \leq \mathbb{F}$ such that $\mathbb{F}$ is algebraic over $\mathbb{K}(S)$.*

Lemma 4.6.6. *Let $\mathbb{K} \leq \mathbb{F}$ be field extension ,$S \subseteq \mathbb{F}$ and suppose that S algebraically independent over $\mathbb{K}$.*

(a) S is a transcendence basis if and only if S is a maximal $\mathbb{K}$-algebraically independent subset of $\mathbb{F}$.

(b) S is contained in a transcendence basis for $\mathbb{K} \le \mathbb{F}$.

(c) $\mathbb{K} \le \mathbb{F}$ has a transcendence basis.

Proof. (a) S is a maximal algebraically independent set if and only if $S \cup \{b\}$ is algebraically dependent for all $b \in \mathbb{F} \setminus S$. By 4.6.4b, this is the case if and only if each $b \in \mathbb{F}$ is algebraic over $\mathbb{K}(S)$.

(b) Let $\mathcal{M}$ be the set of $\mathbb{K}$-algebraically independent subsets of $\mathbb{F}$ containing S. Since $S \in \mathcal{M}$, $\mathcal{M}$ is not empty. Order $\mathcal{M}$ by inclusion. Then $\mathcal{M}$ is a partially ordered set. We would like to apply Zorn's lemma. So we need to show that every chain $\mathcal{D}$ of $\mathcal{M}$ has an upper bound. Note that the elements of $\mathcal{D}$ are subsets on $\mathbb{F}$. So we can build the union $D := \bigcup \mathcal{D}$. Then $E \subseteq D$ for all $E \in \mathcal{D}$. Thus D is an upper bound for $\mathcal{D}$ once we establish that $D \in \mathcal{M}$. That is we need to show that D is algebraically independent over $\mathbb{K}$. As observed before we just this amounts to showing that each finite subset $J \subseteq D$ is algebraically independent. Now each $j \in J$ lies in some $E_j \in \mathcal{D}$. Since $\mathcal{D}$ is totally ordered, the finite subset $\{E_s \mid j \in J\}$ of $\mathcal{D}$ has a maximal element E. Then $j \in E_j \subseteq E$ for all $j \in J$. So $J \subseteq E$ and as E is algebraically independent, J is as well.

Hence every chain in $\mathcal{M}$ has an upper bound. By Zorn's Lemma A.3.8 $\mathcal{M}$ has a maximal element T. By (a) T is a transcendence basis and by definition of $\mathcal{M}$, $S \subseteq T$.

(c) follows from (b) applied to $S = \varnothing$. □

Proposition 4.6.7. *Let $\mathbb{K} \le \mathbb{F}$ be a field extension and S and T transcendence basis for $\mathbb{K} \le \mathbb{F}$. Then $|S| = |T|$. $|S|$ is called the* transcendence degree *of $\mathbb{F} \le \mathbb{K}$ and is denoted by* $\text{tr-deg}_{\mathbb{K}} \mathbb{F}$.

Proof. Well order S and T. For $s \in S$ define $s^- := \{b \in S \mid b < s\}$ and $s^+ := \{b \in S \mid b \le s\}$. Similarly define $t^\pm$ for $t \in T$. Let $s \in S$. As $\mathbb{K}(T) \le \mathbb{F}$ is algebraic, $m_s^{\mathbb{K}(T)} \neq 0$ and we can choose a subset $J \subseteq T$ such that $m_s^{\mathbb{K}(T)} \in \mathbb{K}(J)$. Then s is algebraic over $\mathbb{K}(J)$ and so also algebraic over $\mathbb{K}(s^-, J)$. Let j be the maximal element of J. Then $J \subseteq j^+$ and so s is algebraic over $\mathbb{K}(s^-, j^+)$. Hence we can choose $\phi(s) \in T$ minimal such that s being algebraic over $\mathbb{K}(s^-, \phi(s)^+)$. Similarly for $t \in T$ let $\psi(t) \in S$ be minimal such that t is algebraic over $\mathbb{K}(t^-, \psi(r)^+)$.

We will show that functions $\phi : S \to T$ and $\psi : T \to S$ are inverse to each other. For this let $s \in S$. Put $t = \phi(s)$ and $\mathbb{L} := \mathbb{K}(s^-, t^-)$

We claim that s is transcendental over $\mathbb{L}$. Otherwise, there exists a finite subset J of t^- such that s is transcendental over $\mathbb{K}(s^-, J)$. Let j be the maximal element of J. Then s is algebraic over $\mathbb{K}(s^-, j^+)$ and $j < t$, a contradiction to the minimal choice of $t = \phi(s)$. t.

Thus s is transcendental over $\mathbb{L}$. Note that s is algebraic over $\mathbb{K}(s^-, t^+) = \mathbb{L}(t)$, So if t would be algebraic over $\mathbb{L}$ also s would be algebraic over $\mathbb{L}$, a contradiction. Hence t is transcendental over $\mathbb{L} = \mathbb{K}(t^-, s^-)$. Since t is algebraic over $\mathbb{K}(t^-, \psi(t)^+)$ we get $\psi(t)^+ \nsubseteq s^-$ and so $\psi(t) \nless s$.

Since s is algebraic over $\mathbb{L}(t)$, 4.6.6(b) implies that $\{t, s\}$ is algebraic dependent over $\mathbb{L}$. Since s is transcendental over $\mathbb{L}$ another application of 4.6.6(b) shows that t is algebraic over $\mathbb{L}(s) = \mathbb{K}(s^+, t^-)$. Thus by definition of ψ, $\psi(t) \le s$. Together with $\psi(t) \nless s$ this gives, $\psi(t) = s$. Therefore $\psi \circ \phi = \mathrm{id}_S$. By symmetry $\phi \circ \psi = \mathrm{id}_T$ and so ϕ is a bijection. Hence $|T| = |S|$. □

Example 4.6.8. Let $\mathbb{K}$ be a field and let s be transcendental over $\mathbb{K}$. Let $\mathbb{F}$ be an algebraic closure of $\mathbb{K}(s)$. Put $s_0 = s$ and inductively let s_{i+1} be a root of $x^2 - s_i$ in $\mathbb{F}$. Then $s_i = s_{i+1}^2$ and so

$\mathbb{K}(s_i) \leq \mathbb{K}(s_{i+1})$. Note that s_{i+1} is transcendental over $\mathbb{K}$ and so $\mathbb{K}(s_i) = \mathbb{K}(s_{i+1}^2) \neq \mathbb{K}(s_i)$. Put $\mathbb{E} = \bigcup_{i=0}^{\infty} \mathbb{K}(s_i)$. Then $\mathbb{K}(s_i) \leq \mathbb{E}$ is algebraic. Thus for all $i \in I$, $\{s_i\}$ is a transcendence basis for $\mathbb{E}$ over $\mathbb{K}$. We claim that that $\mathbb{K}(b) \neq \mathbb{E}$ for all $b \in \mathbb{E}$. Indeed, $b \in \mathbb{K}(s_i)$ for some i and so $\mathbb{K}(b) \leq \mathbb{K}(s_i) \subseteq \mathbb{E}$.

4.7 Algebraically Closed Fields

In this section we study the Galois theory of algebraically closed field.

Lemma 4.7.1. *Let $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ be a field isomorphism and $\mathbb{F}_i$ an algebraically close field with $\mathbb{K}_i \leq \mathbb{F}_i$. Suppose that* $\text{tr-deg}_{\mathbb{K}_1} \mathbb{F}_1 = \text{tr-deg}_{\mathbb{K}_2} \mathbb{F}_2$. *Let S_i be a transcendence basis for $\mathbb{F}_i$ over $\mathbb{K}_i$ and $\lambda : S_1 \to S_2$ a bijection. Then there exists an isomorphism $\psi : \mathbb{F}_1 \to \mathbb{F}_2$ with $\psi|_{\mathbb{K}_1} = \phi$ and $\psi|_{S_1} = \lambda$.*

Proof. By 4.6.3 we obtain an isomorphism δ:

$$\begin{tikzcd}
\mathbb{K}_1(S_1) \arrow[r] & \mathbb{K}_1(X_{S_1}) \arrow[r] & \mathbb{K}_2(X_{S_2}) \arrow[r] & \mathbb{K}_2(S_2) \\
\mathbb{K}_1 \ni k \arrow[r] & k \arrow[r] & \phi(k) \arrow[r] & \phi(k) \\
S_1 \ni s \arrow[r] & x_s \arrow[r] & x_{\lambda(s)} \arrow[r] & \lambda(s)
\end{tikzcd}$$

Since $\mathbb{K}_i(S_i) \leq \mathbb{F}_i$ is algebraic and $\mathbb{F}_i$ is algebraic closed, $\mathbb{F}_i$ is an algebraically closure of $\mathbb{K}_i(S_i)$. Hence by 4.2.7(a), δ extends to an isomorphism $\psi : \mathbb{F}_1 \to F_2$. □

Lemma 4.7.2. *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and suppose that $\mathbb{F}$ is algebraically closed. Then* $\text{Aut}_{\mathbb{K}}(\mathbb{F})$ *acts transitively on the set of elements in $\mathbb{F}$ transcendental over $\mathbb{K}$.*

Proof. Let $s_i \in \mathbb{F}$, i=1,2, be transcendental over $\mathbb{K}$. By 4.6.6b there exists a transcendence basis S_i for $\mathbb{K} \leq \mathbb{F}$ with $s_i \in S_i$. Let $\lambda : S_1 \to S_2$ be a bijection with $\lambda(s_1) = s_2$. By 4.7.1 applied with $\phi = \text{id}_{\mathbb{K}}$ there exists $\psi \in \text{Aut}_{\mathbb{K}}(\mathbb{F})$ with $\psi(s) = \lambda(s)$ for all $s \in S_1$. Then $\psi(s_1) = s_2$. □

Example 4.7.3. By results from analysis, both π and e are transcendental over $\mathbb{Q}$. Since $\mathbb{C}$ is algebraically closed we conclude from 4.7.2 that there exists $\alpha \in \text{Aut}_{\mathbb{Q}}(\mathbb{C})$ with $\alpha(\pi) = e$.

Definition 4.7.4. *Let $\mathbb{K}$ be the field and $\mathbb{K}_0$ the intersection of all the subfield. Then $\mathbb{K}_0$ is called the* base field *of* $\mathbb{K}$. *of* $\mathbb{K}$.

Lemma 4.7.5. *Let $\mathbb{K}$ be the field and $\mathbb{K}_0$ the base field of $\mathbb{K}$. Put $p = \text{char}\,\mathbb{K}$. If* $\text{char}\, p = 0$ *then $\mathbb{K}_0 \cong \mathbb{Q}$ and if p is a prime then $\mathbb{K}_0 \cong \mathbb{Z}/p\mathbb{Z}$*

Proof. Let $Z = \{n1_F \mid n \in \mathbb{Z}\}$. The Z is a subring and $\mathbb{K}_0$ is the field of fraction of Z. If $p = 0$, then $Z \cong \mathbb{Z}$ and so $\mathbb{K}_0 \cong \mathbb{Q}$ and if $p > 0$, then $Z \cong Z_p$ and $\mathbb{K}_0 = Z$. □

Corollary 4.7.6. *(a) Let $\mathbb{K}$ be a field. Then for each cardinality c there exists a unique (up to $\mathbb{K}$-isomorphism) algebraically closed $\mathbb{F}$ with $\mathbb{K} \leq \mathbb{F}$ and* $\text{tr-deg}_{\mathbb{K}} \mathbb{F} = c$. *Moreover, $\mathbb{F}$ is isomorphic to the algebraic closure of $\mathbb{K}(X_I)$, where I is a set with $|I| = c$.*

(b) Let $p = 0$ or a prime and c a cardinality. Then there exists a unique (up to isomorphism) algebraically closed field $\mathbb{F}$ with characteristic p and transcendence degree c over its base field. Moreover, if $\mathbb{K} = \mathbb{Q}$ (for $p = 0$) and $\mathbb{K} = \mathbb{Z}_p$ (for $p > 0$) and I is a set of cardinality c, then the algebraic closure of $\mathbb{K}(X_I)$ is such a field.

Proof. Follows immediately from 4.7.1 □

Lemma 4.7.7. *Let $\mathbb{K}$ be a field. Then the following are equivalent.*

(a) $\mathbb{K}$ has no proper purely inseparable field extension.

(b) Let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$. Then $\mathbb{K} \leq \overline{\mathbb{K}}$ is Galois.

(c) All polynomials over $\mathbb{K}$ are separable.

(d) $\operatorname{char}\mathbb{K} = 0$ or ($\operatorname{char}\mathbb{K} = p \neq 0$ and for each $b \in \mathbb{K}$ there exists $d \in \mathbb{K}$ with $d^p = b$).

(e) $\operatorname{char}\mathbb{K} = 0$ or ($\operatorname{char}\mathbb{K} = p \neq 0$ and $\operatorname{Frob}_p^{\mathbb{K}}$ is an automorphism of $\mathbb{K}$.)

Proof. Put $p = \operatorname{char}\mathbb{K}$.

(a) $\Longrightarrow$ (b): Since $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$, $\mathbb{K} \leq \overline{\mathbb{K}}$ is algebraic and normal. Put $\mathbb{P} := \mathbb{P}(\mathbb{K}, \overline{\mathbb{K}})$. Since $\mathbb{K} \leq \overline{\mathbb{K}}$ is normal, 4.2.26(g) implies that $\mathbb{P} \leq \overline{\mathbb{K}}$ is separable. Since $\mathbb{K} \leq \mathbb{P}$ is purely inseparable (a) gives $\mathbb{K} = \mathbb{P}$. Hence $\mathbb{K} \leq \overline{\mathbb{K}}$ is normal and separable and thus by 4.3.17 $\mathbb{K} \leq \overline{\mathbb{K}}$ is Galois.

(b) $\Longrightarrow$ (c): Since $\mathbb{K} \leq \overline{\mathbb{K}}$ is Galois, 4.3.17 implies that $\mathbb{K} \leq \overline{\mathbb{K}}$ is separable. Let $f \in \mathbb{K}[x]$ be irreducible. Then f has root in $\overline{\mathbb{K}}$. This root is separable over $\mathbb{K}$ and so f is separable.

(c) $\Longrightarrow$ (d): We may assume $p > 0$. Let $b \in \mathbb{K}$ and f an irreducible monic factor of $x^p - b$. Then f has a unique root in $\bar{\mathbb{K}}$ and f is separable. Thus $f = x - d$ for some $d \in \mathbb{K}$. Then d is a root of $x^p - b$ and so $d^p = b$.

(d) $\Longrightarrow$ (e): We may assume $p > 0$. By 4.2.18 $\operatorname{Frob}_p^{\mathbb{K}}$ is a monomorphism. By (d) Frob_p is onto.

(e) $\Longrightarrow$ (a): If $p = 0$, all field extensions are separable. So we may assume $p > 0$. Let $\mathbb{K} \leq \mathbb{F}$ be purely inseparable. Let $b \in \mathbb{F}$. Then $d := b^{p^n} \in \mathbb{K}$ for some $n \in \mathbb{N}$. Since $\operatorname{Frob}_p^{\mathbb{K}}$ is onto also $\operatorname{Frob}_{p^n}^{\mathbb{K}} = (\operatorname{Frob}_b^{\mathbb{K}})^n$ is onto. So $d = e^{p^n}$ for some $e \in \mathbb{K}$. Since $\operatorname{Frob}_{p^n}^{\mathbb{F}}$ is 1-1 we get $b = e \in \mathbb{K}$. Hence $\mathbb{F} = \mathbb{K}$. □

Definition 4.7.8. *A field $\mathbb{K}$ which fulfills one and so all of the equivalent conditions in 4.7.7 is called* perfect.

Lemma 4.7.9. *(a) All field of characteristic 0 are perfect.*

(b) All algebraically closed fields are perfect.

(c) All finite fields are perfect.

Proof. (a) follows for example from 4.7.7(d). If $\mathbb{K}$ is an algebraically closed field, then Frob_p is an automorphism by 4.2.18(c). If $\mathbb{K}$ is a finite field, then as Frob_p is 1-1, its onto and so an automorphism. □

Lemma 4.7.10. . *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $\mathbb{A} = \mathbb{A}(\mathbb{K}, \mathbb{F})$.*

(a) Let $b \in \mathbb{F} \smallsetminus \mathbb{A}$ and $a \in \mathbb{A}$. Then $a + b \notin \mathbb{A}$.

(b) If $K \leq \mathbb{F}$ is not algebraic, then $\mathbb{F} = \langle \mathbb{F} \smallsetminus \mathbb{A} \rangle$.

Proof. (a) Suppose $a + b \in \mathbb{A}$. Since $\mathbb{A}$ is a subfield of $\mathbb{F}$ we get $b = (a + b) - a \in \mathbb{A}$, a contradiction. (b) Let $a \in A$. Since $\mathbb{K} \leq \mathbb{F}$ is not algebraic, there exists $b \in \mathbb{F} \smallsetminus \mathbb{A}$. By (a), $a + b \notin \mathbb{A}$ and so $a = (a + b) - b \in \langle \mathbb{F} \smallsetminus \mathbb{A} \rangle$. □

Proposition 4.7.11. *Let $\mathbb{K} \leq \mathbb{F}$ field extension with $\mathbb{F}$ algebraically closed. Put $G := \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$, $\mathbb{P} := \mathbb{P}(\mathbb{K}, \mathbb{F})$ and $\mathbb{A} = \mathbb{A}(\mathbb{K}, \mathbb{F})$. Let $\mathbb{K} \leq \mathbb{E} \leq \mathbb{F}$ with $\mathbb{E} \neq \mathbb{F}$*

(a) $\mathbb{A}$ is an algebraic closure of $\mathbb{K}$ and $\mathbb{K} \leq \mathbb{A}$ is normal.

(b) If $\mathbb{E}$ is G-stable then $G^{\mathbb{E}} = \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$.

(c) $\mathbb{E}$ is G-stable if and only $\mathbb{K} \leq \mathbb{E}$ is normal.

(d) $\mathrm{Fix}_{\mathbb{F}}(G) = \mathbb{P}$.

(e) $\mathbb{E}$ is G-closed if and only if $\mathbb{E} \leq \mathbb{F}$ is Galois and if only if $\mathbb{E}$ is perfect.

(f) Suppose $\mathbb{A} \neq \mathbb{F}$. Then $\mathrm{Aut}_{\mathbb{A}}\mathbb{F}$ is the unique minimal non-trivially closed normal subgroup of G.

Proof. (a) Note that $\mathbb{K} \leq \mathbb{A}$ is algebraic. Let $f \in \mathbb{K}[x]$ be a non-constant polynomial. Since $\mathbb{F}$ is algebraically closed, f has a root $b \in \mathbb{F}$. Then b is algebraic over $\mathbb{K}$ and so $b \in \mathbb{A}$. Thus f has a root in $\mathbb{A}$ and so by definition (see 4.1.18), $\mathbb{A}$ is an algebraic closure of $\mathbb{K}$. In particular, $\mathbb{K} \leq \mathbb{A}$ is normal.

(b) By 4.7.1 every $\phi \in \mathrm{Aut}_{\mathbb{K}}\mathbb{E}$ can be extended to some $\psi \in \mathrm{Aut}_{\mathbb{K}}\mathbb{F}$. So (b) holds.

(c) Suppose $\mathbb{K} \leq \mathbb{E}$ is normal, then by 4.2.10(a), $\mathbb{E}$ is G-stable.

Suppose that $\mathbb{K} \leq \mathbb{E}$ is G-stable. We will first show that $\mathbb{E} \leq \mathbb{A}$. Suppose not and pick $e \in \mathbb{E} \smallsetminus \mathbb{A}$. Then e is transcendental over $\mathbb{K}$. By 4.7.2 Ge consists of all the transcendental elements in $\mathbb{F}$ and so $Ge = \mathbb{F} \smallsetminus \mathbb{A}$. As $\mathbb{E}$ is G-stable, $Ge \subseteq \mathbb{E}$. 4.7.10 implies $\mathbb{F} = \langle \mathbb{F} \smallsetminus \mathbb{A} \rangle = \langle Ge \rangle \leq \mathbb{E}$, a contradiction to $\mathbb{E} \neq \mathbb{F}$.

Hence $\mathbb{E} \leq \mathbb{A}$. By (b)

$$(*) \qquad G^{\mathbb{A}} = \mathrm{Aut}_{\mathbb{K}}(\mathbb{A}).$$

and since $\mathbb{E}$ is G stable we conclude that $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{K}}(\mathbb{A})$-stable. Since $\mathbb{K} \leq \mathbb{A}$ is normal, 4.2.10(d) shows that also $\mathbb{K} \leq \mathbb{E}$ is normal.

(d) Let $b \in \mathbb{F} \smallsetminus \mathbb{A}$. Then by 4.7.10 $b + 1 \in \mathbb{F} \smallsetminus \mathbb{A}$ and so by 4.7.2 there exists $\sigma \in G$ with $\sigma(b) = b + 1 \neq b$. Thus $b \notin \mathrm{Fix}_{\mathbb{F}}(G)$ and so $\mathrm{Fix}_{\mathbb{F}}(G) \leq \mathbb{A}$. Thus

$$(**) \qquad \mathrm{Fix}_{\mathbb{F}}(G) = \mathrm{Fix}_{\mathbb{A}}(G^{\mathbb{A}}) \overset{(*)}{=} \mathrm{Fix}_{\mathbb{A}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{A})) \overset{4.2.26(h)}{=} \mathbb{P}$$

(e) $\mathbb{E}$ is G-closed if and only if

$$(1) \qquad \mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{E}}(\mathbb{F})) = \mathbb{E}$$

and so if and only if $\mathbb{E} \leq \mathbb{F}$ is Galois. Put $\mathbb{B} = \mathbb{A}(\mathbb{E}, \mathbb{F})$. By (**) applied to $\mathbb{E} \leq \mathbb{F}$ in place of $\mathbb{K} \leq \mathbb{F}$, $\mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{E}}(\mathbb{F})) = \mathrm{Fix}_{\mathbb{B}}(\mathrm{Aut}_{\mathbb{E}}(\mathbb{B}))$. So (1) is equivalent to

$$(2) \qquad \mathrm{Fix}_{\mathbb{B}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{B})) = \mathbb{B}.$$

By definition of a Galois extension (2) holds if and only if $\mathbb{E} \leq \mathbb{B}$ is Galois. By (a) applied to $\mathbb{E} \leq \mathbb{F}$, $\mathbb{B}$ is an algebraic closure of $\mathbb{E}$. So by 4.7.7 $\mathbb{E} \leq \mathbb{B}$ is Galois if and only if $\mathbb{E}$ is perfect. So (e) is proved.

(f) Let H be a closed normal subgroup of G with $H \neq \{\mathrm{id}_{\mathbb{F}}\}$. By 4.3.15(e), $\mathcal{F}(H)$ is G-stable. Since $H \neq G$, $\mathcal{F}(H) \neq \mathbb{F}$. By (c), $\mathbb{K} \leq \mathcal{F}(H)$ is normal and so algebraic. Hence $\mathcal{F}(H) \leq \mathbb{A}$ and

$$\mathrm{Aut}_{\mathbb{A}}(\mathbb{F}) = \mathcal{G}(\mathbb{A}) \leq \mathcal{G}(\mathcal{F}(H)) \overset{H\text{-closed}}{=} H.$$

By 4.3.3(h), $\mathcal{G}(\mathbb{A})$ is closed in G. By (a) $\mathbb{K} \leq \mathbb{A}$ is normal and so $\mathbb{A}$ is G-stable. Thus by 4.3.15(d) $\mathcal{G}(\mathbb{A})$ is a normal subgroup of G. Since $\mathbb{A}$ is algebraically closed 4.7.9 shows that $\mathbb{A}$ is perfect and so by (e), $\mathbb{A}$ is closed. Thus $\mathcal{F}(\mathcal{G}(\mathbb{A})) = \mathbb{A} \neq \mathbb{F}$ and so $\mathcal{G}(\mathbb{A}) \neq \{\mathrm{id}_{\mathbb{F}}\}$. Hence $\mathrm{Aut}_{\mathbb{A}}(\mathbb{F}) = \mathcal{G}(\mathbb{A})$ is a non-trivial, closed normal subgroup of G. □

Chapter 5

Multilinear Algebra

Throughout this chapter ring means commutative ring with identity $1 \neq 0$. All modules are assumed to be unitary. We will write (non)-commutative ring for a ring which might not be commutative.

5.1 Multilinear functions and Tensor products

Let $(M_i, i \in I)$ be a family of sets. For $J \subseteq I$ put $M_J = \prod_{j \in J} M_j$ and for $m = (m_i)_{i \in I} \in M_I$ put $m_J = (m_j)_{j \in J} M_J$. If $I = J \cup K$ with $L \cap K = \varnothing$, the map $M_I \to M_J \times M_K, m \to (m_J, m_K)$ is a bijection. We use this canonical bijection to identify M_I with $M_J \times M_K$.

Let W be a set and $f : M_I \to W$ a function. Let $b \in M_K$. Then we obtain a function a function $f_b : M_J \to W, a \to f(a, b)$.

Definition 5.1.1. *Let R a ring, $M_i, i \in I$ a family of R-modules and W an R-module. Let $f : M_I \to W$ be a function. f is R-*multilinear *if for all $i \in I$ and all $b \in M_{I-i}$ the function*

$$f_b : M_i \to W, a \to f(a, b)$$

is R-linear.

Note here that f_b R-linear just means $f(ra, b) = rf(a, b)$ and $f(a + \tilde{a}, b) = f(a, b) + f(\tilde{a}, b)$ for all $r \in R, a \in M_i, b \in M_{I-i}$ and $i \in I$.

The function $f : R^n \to R, \quad (a_1, a_2, \ldots, a_n) \to a_1 a_2 \ldots a_n$ is multilinear. But the function $g : R^n \to R, \quad (a_1, \ldots, a_n) \to a_1$ is not R-linear.

Lemma 5.1.2. *Let $M_i, i \in I$ be a family of R-modules, $f : M_I \to W$ an R-multilinear map, $I = J \uplus K$ and $b \in M_K$. Then $f_b : M_J \to W$ is R-multilinear.*

Proof. Let $j \in J$ and $a \in M_{J-j}$. Then $(a, b) \in M_{I-j}$ and $(f_b)_a = f_{(a,b)}$ is R-linear. So f_b is R-multilinear. □

Lemma 5.1.3. *Let R a ring, $M_i, i \in I$ a finite family of R-modules, W an R-module and $f : M_I \to W$ be a function. Then f is multilinear if and only if*

$$f((\sum_{j\in J_i} r_{ij}m_{ij})_{i\in I}) = \sum_{\alpha\in J_I}(\prod_{i\in I} r_{i\alpha(i)})f((m_{i\alpha(i)})_{i\in I})$$

whenever $(J_i, i \in I)$ is a family of sets, $m_{ij} \in M_i$ and $r_{ij} \in R$ for all $i \in I$ and $j \in J_i$.

Proof. Suppose first that f is multilinear. If $|I| = 1$ we need to show that $f(\sum_{j\in J} r_j m_j) = \sum_{j\in J} r_j f(m_j)$ But this follows easily from the fact that f is linear and induction on J. So suppose that $|I| \geq 2$, let $s \in I$, $K = I - s$. Then by induction

$$\begin{aligned} f((\sum_{j\in J_i} r_{ij}m_{ij}) &\overset{\text{definition of } f_b}{=} f_{\sum_{j\in J_s} r_{sj}m_{sj}}((\sum_{j\in J_i}(r_{ij}m_{ij})_{i\in K} \\ &= \sum_{\alpha\in J_K}(\prod_{i\in K} r_{i\alpha(i)} f_{\sum_{j\in J_s} r_{sj}m_{sj}}(m_{i\alpha(i)})_{i\in K} \\ &= \sum_{\alpha\in J_K}(\prod_{i\in K} r_{i\alpha(i)} f(\sum_{j\in J_s} r_{sj}m_{sj}, (m_{i\alpha(i)})_{i\in K} \\ & \sum_{\alpha\in J_I}\prod_{i\in I} r_{i\alpha(i)} f(m_{i\alpha(i)}) \end{aligned}$$

The other direction is obvious. □

Example: Suppose $f : M_1 \times M_2 \times M_3 \to W$ is multilinear.
Then

$$f(m_{11} + 2m_{12}, 4m_{21}, 3m_{31} + m_{32} =$$

$$= 12f(m_{11}, m_{21}, m_{31}) + 4f(m_{11}, m_{21}, m_{32}) + 24f(m_{12}, m_{21}, m_{31}) + 8f(m_{12}, m_{21}, m_{32})$$

Definition 5.1.4. *Let R be a ring and $M_i, i \in I$ a family of R-modules. A* tensor product *for $(M_i, i \in I)$ over R is a R-multilinear map $f : M_I \to W$ so that for each multilinear map $g : M_I \to \tilde{W}$ there exists a unique R-linear $\breve{g} : W \to \tilde{W}$ with $g = \breve{g} \circ f$.*

Lemma 5.1.5. *Let R be a ring and $(M_i, i \in I)$ a family of R-modules. Then $(M_i, i \in I)$ has a tensor product over R. Moreover, it is unique up to isomorphism, that is if $f_i : M_I \to W_i$, i=1,2, are tensor products, than there exists a R-linear isomorphism $g : W_1 \to W_2$ with $f_2 = g \circ f_1$.*

Proof. Let $F = F_R(M_I)$, the free module on the set M_I. So F has a basis $z(m), m \in M_I$. Let D be the R-submodule if F generated by the all the elements in F of the form

$$z(ra, b) - rz(a, b)$$

and

$$z(a, b) + z(\tilde{a}, b) - z(a + \tilde{a}, b)$$

where $r \in R$, $a \in M_i$, $b \in M_{I-i}$ and $i \in I$.

Let $W = F/D$ and define $f : M_I \to W, m \to z(m) + D$.

To check that f is multilinear we compute

$$f(ra, b) - rf(a, b) = (z(ra, b) + D) - r(z(a, b) + D) = (z(ra, b) - rz(a, b)) + D = D = 0_W$$

and

$$f(a+\tilde{a},b)-f(a,b)-f(\tilde{a},b)=(z(a+\tilde{a},b)+D)-(z(a,b)+D)-z(\tilde{a},b)+D)=(z(a+\tilde{a},b)-z(a,b)-z(\tilde{a},b))+D=D=0_W.$$

So f is R-.multilinear.

To verify that f is a tensor product let $\tilde{f}:M_I\to\tilde{W}$ by R-multilinear. Since F is a free with basis $z(m),m\in M$. There exists a unique R-linear map $\tilde{g}:F\to\tilde{W}$ with $\tilde{g}(z(m))=\tilde{f}(m)$ for all $m\in M_I$. We claim that $D\leq\ker\tilde{g}$. Indeed

$\tilde{g}(z(ra,b)-rz(a,b))=\tilde{g}(z(ra,b)-r\tilde{g}(z(a,b)=\tilde{f}(ra,b)-r\tilde{f}(a,b),$

Here the first equality holds since $\tilde{g}$ is R-linear and the second since $\tilde{f}$ is multilinear.

Similarly $\tilde{g}(z(a+\tilde{a})-z(a,b)-z(\tilde{a},b))=\tilde{g}(z(a+\tilde{a}))-\tilde{g}(z(a,b))-\tilde{g}(z(\tilde{a},b))=\tilde{f}(a+\tilde{a})-\tilde{f}(a,b)-\tilde{f}(\tilde{a},b)=0.$

Hence $\ker\tilde{g}$ contains all the generators of D and since $\ker\tilde{g}$ is an R-submodule of F, $D\leq\ker tildeg$. Thus the map $g:W\to\tilde{W},e+D\to\tilde{g}(e)$ is well defined and R-linear. Note that $g(f(m))=\tilde{g}(f(m))=\tilde{g}(z(m))=\tilde{f}(m)$ and so $\tilde{f}=g\circ f$. To show the uniqueness of g suppose that $h:W\to\tilde{W}$ is R-linear with $\tilde{f}=h\circ f$. Define $\tilde{h}:F\to\tilde{W}$ by $\tilde{h}(e)=h(e+D)$. Then h is R linear and $\tilde{h}(z(m))=h(z(m)+D)=h(f(m))=\tilde{f}(m)=\tilde{g}(z(m))$. Since $z(m)$ is a basis for F this implies $\tilde{h}=\tilde{g}$. Thus $g(e+D)=\tilde{g}(e)=\tilde{h}(e)=h(e+D)$ and $g=h$, as required.

So f is indeed a tensor product.

Now suppose that $f_i:M_I\to W_i$,i=1,2 are tensor products for $(M_i,i\in I$ over R. Let $\{1,2\}=\{i,j\}$. Since f_i is a tensor product and f_j is multilinear, there exists $g_i:W_i\to W_j$ with $f_j=g_if_i$. Then $(g_jg_i)f_i=g_j(g_if_i)=g_jf_j=f_i$. Note that also $\mathrm{id}_{W_i}f_i=f_i$ and so the uniqueness assertion in the definition of the tensor product implies $g_jg_i=\mathrm{id}_{W_i}$. Hence g_1 and g_2 are inverse to each other and g_1 is a R-linear isomorphism. □

Let $(M_i,i\in I)$ be a family of R-modules and $f:M_I\to W$ a tensor product. We denote W by $\bigotimes_R^{i\in I}M_i$ $f((m_i)_{i\in I}$ by $\otimes_{i\in I}m_i$. Also if there is no doubt about the the ring R and the set I in question, we just use the notations $\bigotimes M_i$, $\otimes m_i$ and (m_i)

If $I==\{1,2\ldots,n\}$ we also write $M_1\otimes M_2\otimes\ldots\otimes M_n$ for $\bigotimes M_i$ and $m_1\otimes m_2\otimes\ldots\otimes m_n$ for $\otimes m_i$.

With this notation we see from the proof of 5.1.5 $\bigotimes M_i$ is as an R-module generated by the elements of the form $\otimes m_i$ But these elements are not linear independent. Indeed we have the following linear dependence relations:

$(ra)\otimes b=r(a\otimes b)$ and $(a+\tilde{a})\otimes b=a\otimes b+\tilde{a}\otimes b.$

Here $r\in R,a\in M_i$, $b=\otimes_{j\in J}b_j$ with $b_j\in M_j$ and $i\in I$.

Lemma 5.1.6. *Let I be finite. Then $\bigotimes^I R=R$. More precisely, $f:R^I\to R,(r_i)\to\prod_{i\in I}r_i$ is a tensor product of $(R,i\in I)$.*

Proof. We need to verify that f meets the definition of the tensor product. Let $\tilde{f}:R^I\to\tilde{W}$ be R-multilinear. Define $g:R\to tildeW,r\to r\tilde{f}((1)))$, where (1) denotes the element $r\in R^I$ with $r_i=1$ for all $i\in I$. Then clearly g is R-linear. Moreover,

$$\tilde{f}((r_i))=\tilde{f}((r_i1))=(\prod_{i\in I}r_i)\tilde{f}((1))=g(\prod_{i\in I}r_i)=g(f((r_i))$$

Thus $\tilde{f} = gf$.

Next let $\tilde{g} : R \to \tilde{W}$ be linear with $\tilde{f} = \tilde{g}f$. Then $\tilde{g}(r) = \tilde{g}(r1) = r\tilde{g}(1) = r\tilde{g}(\prod_{i\in I} 1) = rg(f((1)) = r\tilde{f}((1)) = g(r)$ and so g is unique. □

Lemma 5.1.7. *Let $(M_i, i \in I)$ be a family of R-modules. Suppose that I is the disjoint union of subsets $I_j, j \in J$. For $j \in J$ let $f_j : M_{I_j} \to W_j$ be R-multilinear. Also let $g : W_J \to W$ be R-multilinear. Then*

$$g \circ (f_j) : M_I \to W, m \to g((f_j(m_j))$$

is R-multilinear.

Proof. Let $f = g \circ (f_j)$. Let $m \in M_I$ and put $w_j = f_j(m_J)$. Let $w = (w_j) \in W_J$. Then $f(m) = g(w)$.

Let $i \in I$ and pick $j \in J$ with $i \in I_j$. Put $b = (m_k)_{k\in I-i}$ and $v = (w_k)_{k\in J}$. Then $w = (w_j, v)$, $m = (m_i, b)$ and $f_b(m_i) = f(m) = g(w_j, v) = g_v(w_j)$. Let $d = (m_l)_{k\in I_j - i)}$. Then $m_{I_J} = (m_i, d)$. Thus $w_j = f_j(m_{I_j}) = f_j(m_i, d) = (f_j)_d(m_i)$.

Hence $f_b(m_i) = g_v(w_j) = g_v((f_j)_d(m_i))$. So $f_b = g_v \circ (f_j)_d$. Since g is multilinear, g_v is R linear. Since f_j is a multilinear product, $(f_j)_d$ is R-linear. Since the composition of R-linear maps are R-linear, f_b is R-linear. So f is R-multilinear. □

Lemma 5.1.8. *Let $M_i, i \in I$ be a family of R-modules, $f : M_I \to W$ an R-multilinear map, $I = J \uplus K$ and $b \in M_K$.*

(a) There exists a unique R-linear map $\check{f}_b : \otimes^J \to W$ with $\check{f}_b(\otimes^J m_j) = f_b((m_j))$.

(b) The function $f_K : M_K \to \mathrm{Hom}_R(\bigotimes^J M_j, W), b \to \check{f}_b$ is R-multilinear.

(c) There exists a unique R-linear map $\check{f}_K : \bigotimes^K M_k \to \mathrm{Hom}_R(\bigotimes^J M_j, W)$ with $\check{f}_K(\otimes^K m_k)(\otimes^J m_j) = f((m_i))$.

(d) There exists a unique R-bilinear map, $f_{K,J} : \bigotimes^K M_k \times \bigotimes^J M_j \to W$ with $f_{K,J}(\otimes^K m_k, \otimes^J m_j) = f((m_i))$

Proof. (a) Follows from 5.1.2 and the definition of a tensor product.

(b) Let $k \in K$, $a, \tilde{a} \in M_k$, $r \in R$, $b \in M_{K-a}$ and $d \in M_J$. The $(a,b) \in M_K$ and $(a,b,d) \in M_I$. We compute

$$(rf_{(a,b)})(\otimes^J d_j) = rf(a,b,d) = f(ra,b,d) = f_{(ra,b)}(\otimes^J d_j).$$

By the uniqueness assertion in (b), $rf_{(a,b)} = f_{(ra,b)}$. Thus $f_K(ra,b) = rf_K(a,b)$

Similarly

$$(f_{(a,b)} + f_{(\tilde{a},b)})(\otimes^J d_j) = f(a,b,d) + f(\tilde{a},b,d) = f(a+\tilde{a},b,d) = f_{(a+\tilde{a},b)})(\otimes^J d_j)$$

and $f_{(a,b)} + f_{(\tilde{a},b)} = f_{(a+\tilde{a},b)}$. Hence $f_K(a\tilde{a},b) = f_K(a+\tilde{a},b)$ and f_K is R-multilinear.

(c Follows from (b) and the definition of a tensor product.

(d) Define $f_{K,J}(a,b) = \check{f}_K(a)(b)$. Since $\check{f}_K$ and $\check{f}_K(a)$ are R-linear and $f_{K,J}$ is bilinear. Thus (d) follows from (c). □

Lemma 5.1.9. *Let R be a ring and A, B and C R-modules. Then there exists an R-isomorphism*

$$A \otimes B \otimes C \to A \otimes (B \otimes C)$$

which sends $a \otimes b \otimes c \to a \otimes (b \otimes c)$ for all $a \in A, b \in B, c \in C$.

Proof. Define $f : A \times B \times C \to A \otimes (B \otimes C)$, $(a,b,c) \to a \otimes (b \otimes c)$. By 5.1.7, f is multilinear. So there exists an R-linear map $\breve{f} : A \otimes B \otimes C \to A \otimes (B \otimes C)$ with $g(a \otimes b \otimes c) = a \otimes (b \otimes c)$.

By 5.1.8 there exists an R-linear map $g = \otimes_{\{1\},\{2,3\}} \colon A \otimes (B \otimes C) \to A \otimes B \otimes C$ with $g(a \otimes (b \otimes c)) = a \otimes c$.

Note that $(g\breve{f})(a \otimes b \otimes c) = g(a \otimes (b \otimes c)) = a \otimes b \otimes c$. Since $A \otimes B \otimes C$ is generated by the $a \otimes b \otimes c$, we get $g\breve{f} = \mathrm{id}$. Similarly $\breve{f}g = \mathrm{id}$ and so $\breve{f}$ is an R-isomorphism. □

Lemma 5.1.10. *Let I be a finite set and for $i \in I$ let $(M_{ij}, j \in J_i)$ be a family of R-modules. Then there exists an R-isomorphism,*

$$\bigotimes_{i \in I} (\bigoplus_{j \in I_j} M_{ij}) \to \bigoplus_{\alpha \in J_I} (\bigotimes_{i \in I} M_{i\alpha_i}).$$

with

$$\otimes_{i \in I} (m_{ij})_{j \in J_i} \to (\otimes_{i \in I} m_{i\alpha_i})_{\alpha \in J_I}$$

Proof. Let $M_i = \bigoplus_{j \in J_i} M_{ij}$ and let $\pi_{ij} : M_i \to M_{ij}$ the projection map of M_i onto M_{ij}. Note here if $m_i \in M_i$, then $m_i = (m_{ij})_{j \in J_i}$ with $m_{ij} \in M_{ij}$ and $\pi_{ij}(m_i) = m_{ij}$. Let $\alpha \in J_I = \prod_{i \in I} J_i$. Define

$$f_\alpha : M_I \to \bigotimes_{i \in I} M_{i\alpha(i)}, \quad (m_i) \to \otimes_{i \in I} m_{i\alpha_i}.$$

Since $\otimes$ is multilinear and π_{ij} is linear, 5.1.7 implies that f_α is multilinear. Hence there exists a unique R-linear map

$$\breve{f}_\alpha : \bigotimes_{i \in I} M_i \to \bigotimes_{i \in I} M_{i\alpha(i)}$$

with $\breve{f}_\alpha(\otimes m_i) = \otimes m_{i\alpha_i}$. We claim that for a given $m = (m_i)$ there exists only finitely many $\alpha \in I_J$ with $f_\alpha(m) \neq 0$. Indeed there exists a finite subset $K_i \subseteq J_i$ with $m_{ij} = 0$ for all $j \in J_i \setminus K_i$. Thus $\alpha(m) = 0$ for all $\alpha \in J_I \setminus K_I$. Since I and K_i are finite, K_I is finite. Thus

$$\breve{f} = (\breve{f}_\alpha)_{\alpha \in J_I} : \bigotimes_{i \in I} (\bigoplus_{j \in I_j} M_{ij}) \to \bigoplus_{\alpha \in J_I} (\bigotimes_{i \in I} M_{i\alpha_i}).$$

is R-linear with

$$(*) \quad \breve{f}(\otimes_{i \in I} (m_{ij})_{j \in J_i}) = (\otimes_{i \in I} m_{i\alpha_i})_{\alpha \in J_I}$$

To show that $\breve{f}$ is an isomorphism, we define its inverse. For $j \in J_i$ let $\rho_{ij} : M_{ij} \to M_i$ be the canonical embedding. So for $a \in M_{ij}$, $\rho_{ij}(a) = (a_k)_{k \in I_j}$, where $a_k = 0$ of $k \neq j$ and $a_j = a$. Let $\alpha \in J_I$ and define

$$\rho_\alpha : \prod_{i \in I} M_{i\alpha_i} \to \bigotimes_{i \in I} M_i, \quad (m_{i\alpha_i}) \to \otimes_{i \in I} \rho_{i\alpha_i}(m_{i\alpha_i}).$$

Then ρ_α is R-multilinear and we obtain an R linear map

$$\breve{\rho}_\alpha : \bigotimes_{i\in I} M_{i\alpha_i} \to \bigotimes_{i\in I} M_i$$

with

$$\breve{\rho}_\alpha(\otimes_{i\in I} m_{i\alpha_i}) = \otimes_{i\in I} \rho_{i\alpha_i}(m_{i\alpha_i}).$$

Define

$$\breve{\rho} : \bigoplus_{\alpha\in J_I} (\bigotimes_{i\in I} M_{i\alpha_i}) \to \bigotimes_{i\in I} M_i, \quad (d_\alpha) \to \sum_{\alpha\in I_J} \rho_\alpha(d_\alpha).$$

Then $\breve{\rho}$ is R linear. We claim that $\breve{\rho} \circ \breve{f} = \mathrm{id}$ and $\breve{f} \circ \breve{\rho} = \mathrm{id}$.

Let $m = (m_i) = ((m_{ij})) \in M_i$. Then $m_i = \sum_{j\in J_i} \rho_{ij}(m_{ij})$ and by multilinearity of $\otimes$.

$$\otimes_{i\in I} m_i = \sum_{\alpha\in J_I} \otimes_{i\in I} \rho_{i\alpha_i}(m_{i\alpha_i})$$

By (*) and the definition of $\breve{\rho}$.

$$\breve{\rho}(\breve{f}(\otimes_{i\in I} m_i)) = \sum_{\alpha\in I_J} \breve{\rho}\alpha(\otimes_{i\in I} m_{i\alpha_i}) = \sum_{\alpha\in I_J} \otimes_{i\in I} \rho_{i\alpha_i}(m_{ialpha_i}) = \otimes_{i\in I} m_i.$$

Hence $\breve{\rho}\breve{f} = \mathrm{id}$.

Let $d = (d_\alpha) \in \bigoplus_{\alpha\in J_I}(\bigotimes_{i\in I} M_{i\alpha_i})$. To show that $(\breve{f}\breve{\rho})(d) = d$ we may assume that $d_\alpha = 0$ for all $\alpha \neq \beta$ and that $d_\beta = \otimes_{i\in I} m_{i\beta_i}$ with $m_{i\beta_i} \in M_{i\beta_i}$. Put $m_{ij} = 0$ for all $j \neq \beta_i$. Then $m_i := (m_i j) = \rho_{i\beta i}(m_{i\beta_i}$

Then

$$\breve{\rho}(d) = \sum_{\alpha\in J_I} \breve{\rho}_\alpha(d_\alpha) = \breve{\rho}_\beta(\otimes_{i\in I} m_{i\beta_i}) = \otimes_{i\in I} \rho_{i\beta_i}(m_{i\beta_i}) = \otimes_{i\in I} m_i$$

Let $\alpha \in J_I$ with $\alpha \neq 0$. Then $\alpha_i \neq \beta_i$ for some $i \in I$ and so $m_{i\alpha_i} = 0$. Hence

$\breve{f}_\alpha(\breve{\rho}(d)) = 0 = d_\alpha$ if $\alpha \neq \beta$ and $\breve{f}_\alpha(\breve{\rho}(d) = \otimes_{i\in I} m_{i\beta_i} = d_\beta$ if $\beta = \alpha$.

Thus $\breve{f}(\breve{\rho}(d)) = (\breve{f}_\alpha(\breve{\rho}(d)) = (d_\alpha) = d$. Hence $\breve{f}\breve{\rho} = \mathrm{id}$ and $\breve{f}$ is an isomorphism with inverse ρ. □

Corollary 5.1.11. *Let $(M_i, i \in I)$ be a finite family of R-modules. Suppose that M_i is a free R-module with basis $\mathcal{A}_i, i \in I$. Then $\bigotimes_{i\in I} M_i$ is a free R-module with basis*

$$(\otimes_{i\in I} a_i \mid a \in \mathcal{A}_I\}$$

.

Proof. For $j \in \mathcal{A}_i$ let $M_{ij} = R_j$. Then $M_i = \bigoplus_{j\in\mathcal{A}_i} M_{ij}$. For $a \in \mathcal{A}_i$, put $T_a = \bigotimes_{i\in I} M_{ia_i}$. Since each $M_{ij} \cong R$, 5.1.6 implies $T_a \cong R$. More precisely, $\otimes_{i\in I} a_i$ is a basis for T_a. By 5.1.10 $\bigotimes_{i\in I} M_i \cong \bigoplus_{a\in\mathcal{A}_I} T_a$. Hence $(\otimes_{i\in I} a_i \mid a \in \mathcal{A}_I\}$ is indeed a basis for $\bigotimes_{i\in I} M_i$. □

We will denote the basis from the previous theorem by $\bigotimes_{i\in I} \mathcal{A}_i$. If $I = \{1, \dots, n\}$ and $\mathcal{A}_i = \{a_{i1}, a_{i2}, \dots, a_{im_i}\}$ is finite we see that $\bigotimes_{i\in I} M_i$ has the basis

$$a_{1j_1} \otimes a_{2j_2} \otimes \ldots \otimes a_{nj_n}, \quad 1 \leq j_1 \leq m_1, \dots, 1 \leq j_n \leq m_n.$$

Lemma 5.1.12. *(a) Let $(\alpha_i : A_i \to B_i, i \in I)$ a family of R-linear maps. Then there exists a unique R-linear map.*

$$\otimes\alpha_i : \bigotimes A_i \to \bigotimes B_i$$

with

$$(\otimes\alpha_i)(\otimes a_i) = \otimes\alpha_i(a_i)$$

(b) Let $(\alpha_i : A_i \to B_i, i \in I)$ and $(\beta_i : B_i \to C_i, i \in I)$ families of R-linear maps. Then $\otimes(\beta_i \circ \alpha_i) = (\otimes\beta_i) \circ \otimes(\alpha_i)$.

Proof. (a) Define $f : A_I \to \bigotimes B_i, \quad (a_i) \to \otimes\alpha_i(a_i)$. By 5.1.7 f is R-multilinear. So (b) follows from the definition of the tensor product.

(b) Both these maps send $\otimes a_i$ to $\otimes(\beta_i(\alpha_i(a_i)))$. □

5.2 Symmetric and Exterior Powers

Let I be a finite set, R a ring and M an R-module. Let $M_i = M$ for all $i \in M$. Then $M_I = M^I$. Let $\pi \in \mathrm{Sym}(I)$ and $m = (m_i) \in M^I$. Define $m\pi \in M$ by $(m\pi)_i = m_{\pi(i)}$. (So if we view m as a function from $I \to M$, $mpi = m \circ \pi$) For example if $\pi = (1,2,3)$, then $(m_1, m_2, m_3)\pi = (m_2, m_3, m_1)$. Note that for $\pi, \mu \in \mathrm{Sym}(I)$, $m(\pi\mu) = (m\pi)\mu$.

Definition 5.2.1. *Let I be a finite set, R a ring and M an R-modules. Let $f : M^I \to W$ be R-multilinear.*

(a) f is symmetric *if $f(m\pi) = f(m)$ for all $m \in M, \pi \in \mathrm{Sym}(I)$.*

(b) f is skew symmetric *if $f(m\pi) = (\mathrm{sgn}\pi)f(m)$ for all $m \in M, \pi \in \mathrm{Sym}(I)$.*

(c) f is alternating *if $f(m) = 0$ for all $m \in M^I$ with $m_i = m_j$ for some $i \neq j \in I$.*

Lemma 5.2.2. *(a) Let $f : M^I \to W$ be alternating. Then f is skew symmetric.*

(b) Suppose that $f : M^I \to W$ is skew symmetric and that $w \neq -w$ for all $0 \neq w \in W$. Then f is alternating.

(c) Let $f : M^n \to W$ be multilinear with $f(m) = 0$ for all $m \in M^n$ with $m_i = m_{i+1}$ for some $1 \leq i < n$. Then f is alternating.

Proof. (a) Let $\pi \in \mathrm{Sym}(I)$ and $m \in M$ we need to show that $f(\pi m) = \mathrm{sgn} f(\pi m)$. Since π is the product of two cycles we may assume that π itself is a 2-cycle. So $\pi = (i, j)$ for some $i \neq j \in I$. Let $a = m_i, b = m_j$, $d = m_{I \setminus \{i,j\}}$ and $g = f_d$. Then $m = (a, b, d)$, $f(m) = g(a, b)$ and $(\pi f)(m) = f(b, a, d) = g(b, a)$.

Since f and so also g is alternating we compute

$$0 = g(a+b, a+b) = g(a,a) + g(a,b) + g(b,a) + g(b,b) = g(a,b) + g(b,a)$$

Thus $f(\pi m) = g(b,a) = -g(a,b) = (\mathrm{sgn}\pi)f(m)$

(b) Suppose that $m_i = m_j$ for some $i \neq j$ and let $\pi = (i, j)$. Then $m = \pi m$ and so $f(m) = f(\pi m) = (\mathrm{sgn}\pi) f(m) = -f(m)$ Thus by assumption on W, $f(m) = 0$ and f is alternating.

(c) By induction on n. Let $m \in M$ with $m_i = m_j$ for some $1 \leq i < j \leq n$. Let $m = (a, b)$ with $a \in M^{n-1}$, $b \in M$. Let $g = f_b$, that is $g(d) = f(d, b)$ for $d \in M^{n-1}$. By induction g is alternating. So if $j \neq n$, $f(m) = g(a) = 0$. So suppose $j = n$. Let $\pi = (i, n-1)$. By induction and (b), $f(m\pi) = g(a\pi) = -g(a) = -f(m)$. But $(m\pi)_{n-1} = m_i = m_j = m_n = (m\pi)_n$ and so by assumption $f(m\pi) = 0$. Hence also $f(m) = 0$. □

Definition 5.2.3. *Let R be a ring, M an R-module, I a finite set and $f : M^I \to W$ an R-multilinear function.*

(a) f is called an Ith symmetric power *of M over R provided that f is symmetric and for every symmetric function $g : M^I \to \tilde{W}$, there exists a unique R-linear map $\breve{g} : W \to \tilde{W}$ with $g = \breve{g} \circ f$.*

(b) f is called an Ith exterior power *of M over R provided that f is alternating and for every alternating function $g : M^I \to \tilde{W}$, there exists a unique R-linear map $\breve{g} : W \to \tilde{W}$ with $g = \breve{g} \circ f$.*

Lemma 5.2.4. *Let R be a ring, M an R-module and I a finite set. Then an I-th symmetric and an I-th exterior power of M over R exist. Moreover they are unique up to R-isomorphism.*

Proof. Let A be the R-submodule of $\bigotimes^I M$ generated by the elements $\otimes m - \otimes m\pi$, $m \in M_I, \pi \in \mathrm{Sym}(I)$. Let $W = (\bigotimes^I M)/A$ and define $f : M_I \to W$ by $f(m) = \otimes m + A$. We claim that f is an I-th symmetric power for M over R. So let $g : M_I \to \tilde{W}$ be symmetric. Then g is multilinear and so by the definition of a tensor product there exists a unique R-linear map $\grave{g} : \bigotimes^I M \to \tilde{W}$ with $\grave{g}(\otimes m) = g(m)$. Since $g(m) = g(m\pi)$ for all $m \in M, \pi \in \mathrm{Sym}(I)$ we have $\grave{g}(\otimes m) = \grave{g}(\otimes m\pi)$. Thus $\otimes m - \otimes m\pi \in \ker \grave{g}$. Hence also $A \leq \ker \grave{g}$. So there exists a uniquely determined and well defined R-linear map $\breve{g} : W \to \tilde{W}, d + A \to \grave{g}(d)$ for all $d + A \in W$. So f is an I-symmetric power of M over R.

Next let B be the R-submodule of $\bigotimes^I M$ generated by the elements $\otimes m$ where $m \in M$ with $m_i = m_j$ for some $i \neq j \in I$. Let $W = \bigotimes_I M/B$ and define $f : M_I \to W$ by $f(m) = \otimes m + B$. As above it is now a routine exercise to verify that f is an R-exterior power of M over R.

Finally the uniqueness of the symmetric and alternating powers are verified in the usual way. □

We will denote the I-th symmetric power of M over R by $M^I \to S^I M, (m_i) \to \prod_{i \in I} m_i$. The exterior power is denoted by $M^I \to \bigwedge^I M, (m_i) \to \wedge_{i \in I} m_i$.

Lemma 5.2.5. *(a) $S^n R \cong R$ for all $n \geq 1$*

(b) $\bigwedge^1 R \cong R$ and $\bigwedge^n R = 0$ for all $n \geq 2$.

Proof. (a) By 5.1.6 $R^n \to R, (r_i) \to \prod r_i$ is the n-th tensor power of R. Since the map is symmetric and is also the n-th symmetric power.

(b) An alternating map in one variable is just a linear map. So $\bigwedge^R = R$. Now suppose $n \geq 2$, $a, b \in R$, $c \in R^{n-2}$ and $f : R^n \to W$ is alternating. Then $f(a, b, c) = abf(1, 1, c) = 0$. Hence $\Lambda^n R = 0$. □

Lemma 5.2.6. *Let $(M_i, i \in I)$ be an R modules, I a finite set and suppose that I is the disjoint unions of the subsets $I_k \in K$ and M_k is an R-module with $M_i = M_k$ for all $i \in I_k$. Let $g : M_I \to W$ be multilinear. Then*

(a) *Suppose that for all $k \in K$ and $b \in I \setminus I_k$, $g_b : M_k^{I_k} \to W$ is alternating. Then there exists a unique R-linear map*

$$\breve{g} : \bigotimes_{k\in K} (\bigwedge^{I_k} M_k) \to W$$

with

$$\breve{g}(\otimes_{j\in J}(\wedge_{i\in I_k} m_i) = g((m_i))$$

for all $(m_i) \in M^I$.

(b) *Suppose that for all $k \in K$ and $b \in I \setminus I_k$, $g_b : M_k^{I_k} \to W$ is symmetric Then there exists a unique R-linear map*

$$\breve{g} : \bigotimes_{k\in K} (S^{I_k} M) \to W$$

with

$$\breve{g}(\otimes_{j\in J}(\wedge_{i\in I_k} m_i) = g((m_i))$$

for all $(m_i) \in M^I$.

Proof. This is easily proved using the methods in 5.1.2 and 5.1.9 □

Lemma 5.2.7. *Let R be a ring, I a finite set and $(M_j, j \in J)$ a family of R-modules. Let $\Delta = \{d \in \mathbb{N}^J \mid \sum_{j\in J} d_j = |I|\}$. For $j \in J$ let $\{I_d^j \mid j \in J\}$ be a partition of I with $|I_d^j| = d_j$ for all $j \in J$. For $d \in \Delta$ put $A(d) = \{\alpha \in J^n \mid |\alpha^{-1}(j)| = d_j\}$. For $\alpha \in A(d)$ and $j \in J$ put $I_\alpha^j = \alpha^{-1}(j) = \{i \in I \mid \alpha_i = j\}$. Let $\pi_\alpha \in \mathrm{Sym}(I)$ with $\pi_\alpha(I_d^j) = I_\alpha^j$. Then*

(a) *The function*

$$f : (\bigoplus_{j\in J} M_j)^I \to \bigoplus_{d\in\Delta}(\bigotimes_{j\in J} S^{I_d^j} M_j)$$

$$((m_{ij})_{j\in J})_{i\in I}) \to (\sum_{\alpha\in A(d)} \bigotimes_{j\in J}(\prod_{i\in I_d^j} m_{\pi_\alpha(i)j})\ )_{d\in\Delta}$$

is an I-th symmetric power of $\bigoplus_{j\in J} M_j$ over R.

(b) *The function*

$$f : (\bigoplus_{j\in J} M_j)^I \to \bigoplus_{d\in\Delta}(\bigotimes_{j\in J} \bigwedge^{I_d^j} M_j)$$

$$((m_{ij})_{j\in J})_{i\in I}) \to (\sum_{\alpha\in A(d)} \mathrm{sgn}_{\pi_\alpha} \bigotimes_{j\in J}(\bigwedge_{i\in I_d^j} m_{\pi_\alpha(i)j})\ )_{d\in\Delta}$$

is an I-th exterior power of $\bigoplus_{j\in J} M_j$ over R.

Proof. (b) View each $\alpha = (\alpha_i)_{i \in I} \in J^n$ as the function $I \to J, i \to \alpha_i$. Since $\{I_d^j \mid j \in J$ of I is a partition of I, each I_d^j is a subset of I and each $i \in I$ is contained I_d^j for a unique $j \in J$. Define $\alpha_d \in J^I$ by $(\alpha_d)_i = j$ where $i \in I_d^j$.

Let $\alpha \in J^I$. Note that $\{I_\alpha^j \mid j \in J\}$ is a partition of I. Define $d = d_\alpha \in \Delta$ by $(d_\alpha)_j = |I_\alpha^j|$. So d is unique in Δ with $\alpha \in A(d)$. Note that $I_{\alpha_d}^j = I_d^j$. We will now verify that there exists a $\pi_\alpha \in \mathrm{Sym}(I)$ with $\pi_\alpha(I_d^j) = I_\alpha^j$. Since $|I_\alpha^j| = |I_d^j|$, there exists a bijection $\pi_\alpha^j : I_d^j \to I_\alpha^j$.

Define $\pi_\alpha \in \mathrm{Sym}(I)$ by $\pi_\alpha(i) = \pi_\alpha^j(i)$, where $i \in I_d^j$. Since $\pi_\alpha^j(i) \in I_{\alpha^j}$, $\alpha(\pi_\alpha^j(i)) = j$. But $j = \alpha_d(i)$ and so $\alpha \circ \pi_\alpha = \alpha_d$.

Conversely if $\pi \in \mathrm{Sym}(I)$ with $\alpha \circ \pi = \alpha_d$ then $\pi^j : I_d^j \to I_\alpha^j, i \to \pi(i)$ is a well defined bijection.

Define

$$f_d^j : M^n \to \bigwedge^{d_j} M_j, \quad m \to \wedge_{i \in I_d^j} m_{ij}$$

and

$$f_d : M^n \to \bigotimes_{j \in J} (\bigwedge^{d_j} M_j), \quad m \to \otimes_{j \in J} f_d^j(m))$$

We will now show $\mathrm{sgn}\pi_\alpha f_d \circ \pi_a lpha$ does not depend on the particular choice of π_α. For this let $\pi \in \mathrm{Sym}(n)$ with $\alpha_d = \alpha \circ \pi$. Put $\sigma = \pi - 1\pi_\alpha$ and $\sigma^j = (\pi^j) - 1\pi_\alpha^j$. So Then $\sigma^j \in \mathrm{Sym}(I_d^j)$ and and

$$(f_d^j \circ \pi_\alpha(m) = f_d^j(m\pi_\alpha) = \wedge_{i \in I_d^j}(m\pi_\alpha)_{ij} = \wedge_{i \in I_d^j}(m_{\pi_\alpha^j(i)j} =$$

$$= \wedge_{i \in I_d^j} m_{\pi^j(\sigma^j(i))j} = (\mathrm{sgn}\sigma^j)(\wedge_{i \in I_d^j} m_{\pi^j(i)j}) = (\mathrm{sgn}\sigma^j)(f_d^j \circ \pi)(m)$$

Thus $f_d^j \circ \pi_\alpha = (\mathrm{sgn}\sigma^j) f_d^j \circ \pi$ Taking the tensor product over all $j \in J$ and using $\mathrm{sgn}\sigma = \prod_{j \in J} \mathrm{sgn}\sigma^j$ we get $f_d \circ \pi_\alpha = \mathrm{sgn}\sigma f_d \circ \pi$. But $\mathrm{sgn}\pi = \mathrm{sgn}\pi_\alpha \mathrm{sgn} sigma$ and so

$$\mathrm{sgn}_{\pi_\alpha} f_d \circ \pi_\alpha \mathrm{sgn}\pi f_d \circ \pi$$

So we can define $f_\alpha = \mathrm{sgn}_\pi f_d \circ \pi$, where $\pi \in \mathrm{Sym}(n)$ with $\alpha_d = \alpha\pi$.

Let $\mu \in \mathrm{Sym}(n)$ and $j \in J$. Then $(\alpha\mu)(i) = j$ if and only if $\alpha(\mu(i)) = j$. Thus $\mu(I_{\alpha\mu}^j) = I_\alpha^j$. Hence $d_{\alpha\mu} = d_\alpha = d$. Put $\rho = \pi_{\alpha\mu}$ Then

$$\alpha_d = (\alpha\mu) \circ \rho = \alpha \circ (\mu \circ \rho$$

So by definition of f_α

$f_\alpha(m) = (\mathrm{sgn}(\mu \circ \rho))(f_d \circ (\mu \circ \rho) = (\mathrm{sgn}\mu)(\mathrm{sgn}\rho)(f_d \circ \rho)(m\mu) = \mathrm{sgn}\mu f_{\alpha\mu}(m\mu)$. So we proved:

(**) $f_{\alpha\mu}(m\mu) = (\mathrm{sgn}\mu) f_\alpha(m)$

For $d \in \Delta$ define $\bar{f}_d = \sum_{\alpha \in A(d)} f_\alpha$ We will show that $\bar{f}_d$ is alternating. By 5.1.7, $f_d^a lpha$ is multilinear. Hence also $\bar{f}_d$ is multilinear.

Now suppose that $m_k = m_l$ for some $k \neq l \in I$. Put $\mu = (k, l) \in \mathrm{Sym}(I)$.

Let $\alpha \in A(d)$. Suppose that $\alpha = \alpha\mu$, that is $\alpha_k = \alpha_l$. Let $j = \alpha(i)$. Then $k, l \in I^j_\alpha)$. Since $m_l = m_k$, $m_{lj} = m_{ij}$ Thus $\wedge_{i \in I^j_\alpha} m_{ij} = 0$, $f^j_\alpha(m) = 0$ and so also $f_\alpha(m) = 0$.

Suppose next that $\alpha \neq \alpha\mu$. Since $m_k = m_l$, $m = m\mu$. So by (**)

$$f_{\alpha\mu}(m) = f_{\alpha\mu}(m\mu) = \mathrm{sgn}\mu f_\alpha(m) = -f_\alpha(m)$$

Hence $f_{\alpha\mu}(m) + f_\alpha(m) = 0$. It follows that $\bar{f}_d(m) = \sum_{\alpha \in A(d)} f_\alpha(m) = 0$ and $\bar{f}_d$ is alternating.

Now define

$$f = (\bar{f}_d) : M^n \to \bigoplus_{d \in \Delta} (\bigotimes_{j \in J} \bigwedge^{d_j} M_j), \quad m \to (\bar{f}_d(m))_{d \in \Delta}.$$

To complete the proof of (b) it remains to verify that f is an I-th exterior power of M. Since each f_d is alternating, f is alternating. Let $g : M^n \to W$ be alternating.

By 5.2.6 there exists a unique R-linear map

$$\breve{g}_d : \bigotimes_{j \in J} (\bigwedge^{I^j_d} M_j) \to W$$

with

$$\breve{g}_d(\otimes j \in J \wedge_{i \in I^j_d} m_i = g(m)$$

where $m \in M^I$ with $m_i \in M_j$ for all $i \in I^j_d$.

Define

$$\breve{g} : \bigoplus_{d \in \Delta} (\bigotimes_{j \in J} \bigwedge^{d_j} M_j) \to W, \quad (u_d)_{d \in \Delta} \to \sum_{d \in \Delta} \breve{g}_d(u_d)$$

Let $m \in M^I$. Since g is multilinear,

$$g(m) = \sum_{\alpha \in J^I} w_\alpha$$

where $w_\alpha = g(m_{i\alpha(i)})$.

Let $\pi = \pi_\alpha$. Since g is alternating and $\alpha_d = \alpha\pi$,

$$w_\alpha = \mathrm{sgn}\pi g(m_{\pi i, \alpha_d(i)})$$

Note that $\otimes j \in J \wedge_{i \in I^j_d} m_i \wedge_{i \in I^j_d} m_{\pi i \alpha_d(i)} = f_d(m\pi))$ and so by definition of $\breve{g}_d$ and the previous equation

$$w_\alpha = \mathrm{sgn}\pi \breve{g}_d(f_d(m\pi)) = \breve{g}_d(f_\alpha(m))$$

Thus

$$g(m) = \sum_{\alpha \in J^I} w_\alpha) = \sum_{d \in \Delta} \sum_{\alpha \in A(d)} \breve{g}_d(f_\alpha(m)) ==$$

$$= \sum_{d\in\Delta} \breve{g}_d(\sum_{\alpha \in A(d)} f_\alpha(m)) = \sum_{d \in \Delta} \breve{g}_d \bar{f}_d(m)) = \breve{g}((\bar{f}_d(m)_{d\in\Delta}) = \breve{g}(f(m))$$

Thus $g = \breve{g} \circ f$. So f is indeed an exterior power and (b) is proved.

(a) To prove (a) we change the proof for (b) as follows: Replace $\bigwedge$ by S. Replace $\wedge$ by $\cdot$. Replace every sgn*lambda* by 1. Finally the following argument needs to be added:

Let $\mu \in \mathrm{Sym}(I)$. Then using (**) and $A(d) = \{\alpha\mu \mid \alpha \in A(d)$ we get

$$\bar{f}_d(m) = \sum_{\alpha\in A_d} f_\alpha(m) = \sum_{\alpha \in A(d)} f_{\alpha\mu}(m\mu) = \sum_{\alpha \in A_d} f_\alpha(m\mu) = \bar{f}_d(m\mu).$$

Thus $\bar{f}_d$ is symmetric. □

A remark on the preceding theorem. The proof contains an explicit isomorphism. But this isomorphism depends on on the choice of the partitions I_d^k. And the computation of the isomorphism depends on the choice of the π_α. Here is a systematic way to make these choices. Assume $I = \{1, \ldots, n\}$ and choose some total ordering on J. Let $d \in \Delta$ and let $J_d = \{j \in J \mid d_j \neq 0$. Note that $|J_d| \leq |I|$ and so J_d is finite. Hence $J_d = \{j_1, \ldots j_u$ with $j_1 < j_2 < \ldots < j_u$. To simplify notation we write k for j_k. Choose $I_d^1 = \{1, 2, \ldots, d_1$, $I_d^2 = \{d_1 + 1, d_1 + 2, \ldots, d_1 + d_2\}$ and so on. Now let $\alpha \in A(d)$. So $I_d^j = \{s + 1, s + 2, \ldots s + d_j$, where $s = \sum_{k<j} d_k$Define π_α as follows. Send 1 to the smallest i with $\alpha(i) = 1$, 2 to the second smallest element with $\alpha(i) = 1$, d_1 to the largest element with $\alpha(i) = 2$, $d_1 + 1$ to the smallest element with $\alpha(i) = 2$ and so on.

Finally we identify $\bigwedge^{I_d^j} M_j$ with $\bigwedge^{d_j} M_j$ by identifying $\wedge_{i \in I_{dj}} v_i \in \bigwedge^{I_d^j} M_j$ with $\wedge_{t=1}^{d_j} v_{s+t} \in \bigwedge^{d_j} M_j$, where $s = \sum_{k<j} d_k$.

Let $m = (m_i) \in M^I$ such that for all $i \in I$ there exists a unique $j \in J$ with $m_{ij} \neq 0$. So $m_i = m_{ij}$ for a unique $j \in J$. Denote this j by $\alpha(i)$. Then $\alpha \in J^I$. Note that $\bar{f}_d(m) = 0$ for all $d \neq d_\alpha$. So suppose that $\alpha \in A(d)$. Let $I_\alpha^j = \{i_1^j, i_2^j, \ldots i_{d_j}^j\}$ with $i_1^j < i_2^j < \ldots < i_{d_j}$. Then since $\wedge$ is skew symmetric there exists $\epsilon \in \{1, -1\}$ with

$$\wedge m = m_{1,\alpha(1)} \wedge m_{2,\alpha(2)} \wedge \ldots \wedge m_{n,\alpha(n)} =$$

$$= \epsilon m_{i_1^1,1} \wedge m_{i_2^1,1} \wedge \ldots \wedge m_{i_{d_1},1} \wedge m_{i_2^2,2} \ldots \wedge m_{i_{d_2},2} \wedge \ldots \wedge m_{i_1^u,u} \wedge \ldots \wedge m_{i_{d_u}^u,u}$$

Then $\epsilon = \mathrm{sgn}\pi_\alpha$ and $\bar{f}_d(m)$ is

$$\epsilon(m_{i_1^1,1} \wedge m_{i_2^1,1} \wedge \ldots \wedge m_{i_{d_1},1}) \otimes (m_{i_2^2,2} \ldots \wedge m_{i_{d_2},2}) \otimes \ldots \otimes (m_{i_1^u,u} \wedge \ldots \wedge m_{i_{d_u}^u,u})$$

For example suppose that $|I| = 3$ and $|J| = 2$. We want to compute $f(m_{11} + m_{12}, m_{21} + m_{22}, m_{31} + m_{32})$. Since f is multilinear we need to compute $f(m_{1\alpha(1)}, m_{2\alpha(2)}, m_{3\alpha(3)}$ where $\alpha(i) \in J = \{1, 2\}$.

If $\alpha = (1, 1, 1)$ then $d_\alpha = (3, 0)$ and

$$\bar{f}_{(3,0)}(m_{11}, m_{21}, m_{31}) = m_{11} \wedge m_{21} \wedge m_{31}$$

If $\alpha = (1,1,2)$ then $d_\alpha = (2,1)$ and

$$\bar{f}_{(2,1)}(m_{11}, m_{21}, m_{32}) = (m_{11} \wedge m_{21}) \otimes m_{32}$$

If $\alpha = (1,2,1)$ then $d_\alpha = (2,1)$ and

$$\bar{f}_{(2,1)}(m_{11}, m_{22}, m_{31}) = -(m_{11} \wedge m_{31}) \otimes m_{22}$$

If $\alpha = (1,2,2)$ then $d_\alpha = (1,2)$ and

$$\bar{f}_{(1,2)}(m_{11}, m_{22}, m_{32}) = m_{11} \otimes (m_{22} \wedge m_{32})$$

If $\alpha = (2,1,1)$ then $d_\alpha = (2,1)$ and

$$\bar{f}_{(2,1)}(m_{11}, m_{21}, m_{32}) = (m_{21} \wedge m_{31}) \otimes m_{12}$$

If $\alpha = (2,1,2)$ then $d_\alpha = (1,2)$ and

$$\bar{f}_{(1,2)}(m_{12}, m_{21}, m_{32}) = -m_{21} \wedge (m_{12} \otimes m_{32})$$

If $\alpha = (2,2,1)$ then $d_\alpha = (1,2)$ and

$$\bar{f}_{(1,2)}(m_{12}, m_{22}, m_{31}) = m_{31} \otimes (m_{12} \wedge m_{22})$$

If $\alpha = (2,2,2)$ then $d_\alpha = (0,3)$ and

$$\bar{f}_{(0,3)}(m_{12}, m_{22}, m_{32}) = m_{12} \wedge m_{22} \wedge m_{32}.$$

Thus the four coordinates of $f(m)$ are:
$d = (3,0)$:

$$m_{11} \wedge m_{21} \wedge m_{31}$$

$d = (2,1)$:

$$(m_{11} \wedge m_{21}) \otimes m_{32} - (m_{11} \wedge m_{31}) \otimes m_{22} + (m_{21} \wedge m_{31}) \otimes m_{12}$$

$d = (1,2)$:

$$m_{11} \otimes (m_{22} \wedge m_{32}) - m_{21} \wedge (m_{12} \otimes m_{32}) + m_{31} \otimes (m_{12} \wedge m_{22})$$

$d = (0,3)$:

$$m_{12} \wedge m_{22} \wedge m_{32}$$

Lemma 5.2.8. *Let R be a ring, n a positive integer and M a free R-modules with basis $\mathcal{B}$. Let " $\leq$ " be a total ordering on $\mathcal{B}$.*

(a) $(b_1 b_2 \ldots b_n \mid b_1 \leq b_2 \leq \ldots b_n \in \mathcal{B})$ *is a basis for* $S^n M$.

(b) $(b_1 \wedge b_2 \wedge \ldots \wedge b_n \mid b_1 < b_2 < \ldots b_n \in \mathcal{B})$ *is a basis for* $S^n M)$.

Proof. For $b \in \mathcal{B}$ put $M_b = Rb$. Then $M_b \cong R$ and $M = \bigoplus_{b\in\mathcal{B}} M_b$. We will apply 5.2.7 with $I = \{1,\dots,n\}$ and $J = \mathcal{B}$. Let Δ be as in the statement of that theorem. Let $d \in \Delta$.

(a) By 5.2.5, $S^t M_b \cong R$ with basis b^t. By 5.1.6

$$\bigotimes_{b\in\mathcal{B}} (S^{d_b} M_b) \cong R$$

and has $\otimes_{b\in\mathcal{B}} b^{d_b}$ has a basis. (a) now follows from 5.2.7(a)

(b) By 5.2.5 $\bigwedge^t M_b = 0$ for all $t \geq 2$. So

$$\bigotimes_{b\in\mathcal{B}} (\bigwedge^{d_b} M_b) \cong R = 0$$

if $d_b \geq 2$ for some $b \in \mathcal{B}$ and

$$\bigotimes_{b\in\mathcal{B}} (\bigwedge^{d_b} M_b) \cong R$$

if $d_b \leq 1$ for all $b \in \mathcal{B}$. Moreover, it has basis $\otimes_{b\in\mathcal{B}, d_b=1} b$. (b) now follows from 5.2.7(b). □

Example: Suppose M has basis $\{a, b, c, d\}$. Then $S^3 M$ has basis

$$d^3, cd^2, c^2d, c^3, bd^2, bcd, bc^2, b^2d, b^2c, b^3, ad^2, acd, ac^2, abd, abc, ab^2, a^2d, a^2c, a^2b, a^3$$

and $\bigwedge^3 M$ has basis

$$b \wedge c \wedge d, a \wedge c \wedge d, a \wedge b \wedge d, a \wedge b \wedge c$$

Corollary 5.2.9. *Let R be a ring and n, m positive integer. Then*

(a) $S^m R^n \cong R^{\binom{n+m+1}{m}}$

(b) $\bigwedge^m R^n \cong R^{\binom{n}{m}}$.

Proof. This follows from 5.2.8 □

Lemma 5.2.10. *Let R be a ring and M an free R-module with finite basis $\mathcal{A}$ and $\mathcal{B}$. Then $|\mathcal{A}| = |\mathcal{B}|$.*

Proof. Let $n = |\mathcal{A}|$. Then $M \cong R^n$. So by 5.2.9(b), n is the smallest non-negative integer with $\bigwedge^{n+1} M = 0$. So n is uniquely determined by M and $n = |\mathcal{B}|$. □

Definition 5.2.11. *Let R be a ring and M and free R-module with a finite basis $\mathcal{B}|$. Then $|\mathcal{B}|$ is called the rank of M.*

5.3 Determinants and the Cayley-Hamilton Theorem

Lemma 5.3.1. *Let I be finite set and R a ring.*

(a) Let $\alpha : A \to B$ be R-linear. Then there exists a unique R-linear map

$$\wedge^I \alpha : \bigwedge^I A \to \bigwedge^I B$$

with

$$\wedge^I \alpha(\wedge a_i) = \wedge \alpha(a_i).$$

(b) Let $\alpha : A \to B$ and $\beta : B \to C$ be R-linear. Then

$$\wedge^I(\beta \circ \alpha) = \wedge^I \beta \circ \wedge^I \alpha.$$

Proof. (a) Define $g : A^I \to \bigwedge^I B, (a_i) \to \wedge \alpha(a_i)$. If $a_i = a_j$ for some $i \neq j$ then also $\alpha(a_i) = \alpha(b_i)$ and so $g(a) = 0$. Thus g is alternating and (a) follows from the definition of an exterior power.

(b) Both these maps send $\wedge a_i$ to $\wedge \beta(\alpha(a_i))$. □

Theorem 5.3.2. *Let R be a ring and n a positive integer.*

(a) Let R be a ring, $0 \neq M$ a free R-module of finite rank n, and $\alpha \in \mathrm{End}_R(V)$. Then there exists a unique $r \in R$ with $\wedge^n \alpha = r\mathrm{id}_{\wedge^n M}$. We denote this r by $\det \alpha$.

(b)

$$\det : \mathrm{End}_R(V) \to R, \alpha \to \det \alpha$$

is a multiplicative homomorphism.

(c) There exists a unique function $\det : \mathcal{M}_R(n) \to R$ (called determinant) with the following two properties:

(a) When viewed as a function in the n columns, $\det$ is alternating.

(b) Let I_n be the $n \times n$ idendity matrix. Then $\det I_n = 1$.

(d) Let $A = (a_{ij}) \in \mathcal{M}_R(n)$. Then

$$\det A = \sum_{\pi \in \mathrm{Sym}(n)} \mathrm{sgn}\pi \prod_{i=1}^{n} a_{i\pi i}$$

(e) Let $A = (a_{ij}) \in \mathcal{M}_R(n)$ and $a_j = (a_{ij})$ the j-th column of A. Then $\wedge a_j = \det A \wedge e_j$, where $e_j = (\delta_{ij}) \in R^n$.

(f) Let R be a ring, $0 \neq M$ a free R-module of finite rank n, $\alpha \in \mathrm{End}_R(V)$. and $\mathcal{B}$ a basis for M. Let $A = \mathcal{M}^{\mathcal{B}}(\alpha)$ be the matrix for α with respect to $\mathcal{B}$. Then

$$\det \alpha = \det A$$

(g) *Let $A \in \mathcal{M}_R(n)$. Then*

$$\det A = \det A^T$$

where $a^T_{ij} = a_{ji}$.

Proof. (a) By 5.2.9, $\bigwedge^I M \cong R$. Thus by 3.6.15, $\mathrm{End}_R(\bigwedge^I M) = R_{\mathrm{id}}$. So (a) holds.

(b) follows from 5.3.1.

(c) Let $e_i = (\delta_{ij}) \in R^n$. Then by 5.2.8, $e := \wedge_{i=1}^n e_i$ is a basis for $\bigwedge^n R^n$. Define $\tau : \bigwedge^n R^n \to R, re \to r$. Let $A \in \mathcal{M}_R(n)$ a view A as $(a_i)_{1 \le i \le n}$ with $a_i \in R^n$. Define $\det A = \tau(\wedge_{i \in I} a_i$. Since $I_n = (e_i)$, $\det I_n = 1$. So det fulfills **(Det Alt)** and **Det I**. Suppose now $f : (R^n)^n \to R$ is alternating with $f((e_i)) = 1$. Then by definition of an I-th exterior power there exists an R-linear map $\breve{f} : \bigwedge^n R^n \to R$ with $f = \breve{f} \circ \wedge$. Then $\breve{f}(e) = \breve{e}(\wedge e_i) = f((e_i) = 1$ and so $\breve{f} = \tau$ and $f = \det$. Thus (c) holds.

(d) We will apply 5.2.7 with $I = J = \{1, \ldots, n\}$ and $M_j = Re_j$. So $\bigoplus_{j \in J} = R^n$. Let $\delta \in \Delta$. If $d_j \geq 2$ for some $j \in J$ then $\bigwedge^{I^j_d} M_j = 0$. If $d_j \leq 1$ for all j, then $\sum_{j \in J} d_j = n = |I|$ forces $d_j = 1$ for all $j \in J$. Let $d \in \Delta$ with $d_j = 1$ for all $j \in J$. Also $R_{e_j} \to R, re_j \to R$ is an 1-st exterior power. Let $\alpha \in J^I$. Then $\alpha \in A(d)$ if and only if $|\alpha^{-1}(j)| = 1$ for all $j \in J$. This is the case if and only of $\alpha \in \mathrm{Sym}(n)$. Also $\pi_\alpha = \alpha$. Hence 5.2.7 implies that

$$f : (R^n)^n \to R \quad (m_{ij}) \to \sum_{\alpha \in \mathrm{Sym}(n)} \prod_{i=1}^n m_{i\pi i}$$

is an n-th exterior power of R^n. Note that $f((e_i)) = 1$. So this this choice of $\bigwedge^n R^n$ we have $e = 1$, $\tau = \mathrm{id}_R$ and $\det = f$. so (d) holds.

(e) was proved in (c).

(f) For $A \in \mathcal{M}_{\mathcal{B}}(R)$ let $\alpha = \alpha_A$ be the corresponding elements of $\mathrm{End}_R(M)$. So $\alpha(b) = \sum_{d \in \mathcal{B}} a_{db} d$. Let $a_b = (a_{db}$, the b-th column of A. Suppose that $a_b = a_c$ with $b \neq c$. Then $\alpha(b) = \alpha(c)$ and so $(\wedge\alpha)(\wedge b) = \wedge\alpha(b) = 0$. Hence $\det \alpha = 0$. Also $\det I_n = \det \mathrm{id} = 1$ and so $A \to \det(\alpha_A)$ fulfilled **(Det Alt)** and **(Det I)**. Thus the uniqueness of $\det A$ implies $\det A = \det \alpha$.

(g) Using (d) we compute

$$\begin{aligned}\det A^T &= \sum_{\pi \in \mathrm{Sym}(n)} \mathrm{sgn}\pi \prod_{i \in I} a^T_{i\pi(i)} = \sum_{\pi \in \mathrm{Sym}(n)} \mathrm{sgn}\pi \prod_{i \in I} a_{\pi(i)i} = \\ &= \sum_{\pi \in \mathrm{Sym}(n)} \mathrm{sgn}\pi \prod_{i \in I} a_{i\pi^{-1}(i)} = \sum_{\pi \in \mathrm{Sym}(n)} \mathrm{sgn}\pi \prod_{i \in I} a_{i\pi(i)} = \det A\end{aligned}$$

□

Definition 5.3.3. *Let R be a ring and $s : A \to B \to C$ R-bilinear.*

(a) *An s-basis for is a triple $((a_d \mid d \in D), (b_d \mid d \in D), c)$ such that D is a set, $(a_d \mid d \in D)$ is a basis for A, $(b_d, d \in D)$ is a basis for B and $\{c\}$ is a basis for C with $s(a_d, b_e) = \delta_{de} c$ for all $d, e \in D$.*

(b) *We say that is s is a* pairing *if there exists an s-basis. s is a finite pairing if s is pairing and* $\mathrm{rank} A = \mathrm{rank} B$ *is finite.*

Note that if $s : A \to B \to C$ is a pairing, then A, B and C are free R-modules and $C \cong R$ as an R-module. Also s is non-degenerate, that is $s(a,b) = 0$ for all $b \in B$ implies $a = 0$, and $s(a,b) = 0$ for all $a \in A$ implies $b = 0$.

The converse is only true in some special circumstances. For example if R is a field, $s : A \to B \to C$ is bilinear, $\dim_R C = 1$ and $\dim_R A$ is finite, then it is not to difficult to see that s is a pairing.

But if $\dim_R A$ is not finite this is no longer true in general. For example let $B = A^* = \mathrm{Hom}_R(A,R)$ and $s(a,b) = b(a)$. Then $\dim_R B > \dim_R A$ and so s is not a pairing.

For another example define $s : \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}(a,b) \to \mathbb{Z}, (a,b) \to 2ab$. The s is not a pairing. Indeed suppose $(\{a\},\{b\},c)$ is an s basis. Then $c = s(a,b) = 2ab$, a contradiction to $\mathbb{Z} = \mathbb{Z}c$.

Lemma 5.3.4. *Let R be a ring, I, J, K finite sets with $K = I \uplus J$ and let $s : A \times B \to R$ be R-bilinear. Let $\Delta = \{E \subseteq K \mid |E| = |J|\}$ and for $E \in \Delta$ choose $\pi_E \in \mathrm{Sym}(K)$ with $\pi_E(J) = E$.*

(a) There exists a unique R-bilinear map

$$s_K^J : \bigwedge^K A \times \bigwedge^J B \to \bigwedge^I A$$

with

$$s_K^J(\wedge a_k, \wedge b_j) = \sum_{E\in\Delta} \det(s(a_{\pi_E(j)}, b_{j'})_{j,j'\in J}) \bigwedge_{i\in I} a_{\pi_E(i)}$$

(b) s_K^J is independent form the choice of the π_E.

(c) Let $\alpha \in \mathrm{End}_R(A)$ and $\beta \in \mathrm{End}_R(B$ with $s(\alpha(a), b) = s(a, \beta(b))$ for all $a \in A, b \in B$. Then

$$(\wedge^I \alpha)\,(s_K^J(\,u\,,\,(\wedge^J\beta)(v)\,)\,) = s_K^J(\,(\wedge^K\alpha)(u)\,,\,v\,)$$

for all $u \in \wedge^K A$ andv $\in \wedge^J B$.

(d) Suppose there exists a basis $\mathcal{E} = (e_d, d \in D)$ for A and a basis $\mathcal{F} = (f_d, d \in D)$ for B such that $s(e_d, f_{d'}) = \delta_{dd'}$. Let $\alpha \in D^K$ and $\beta \in D^J$ be one to one. Then

$$s_K^J((\bigwedge_{k\in K} e_{\alpha(k)}, \bigwedge_{j\in J} f_{\beta(k)}) = \begin{cases} \pm \bigwedge_{k\in K\smallsetminus\alpha^{-1}(\beta(J))} e_{\alpha(k)} & \text{if } \beta(J) \subseteq \alpha(K) \\ = 0 & \text{if } \beta(J) \nsubseteq \alpha(K) \end{cases}.$$

Proof. (a) and (b) We first show that

$$f_E(a,b) := \mathrm{sgn}\pi_E \det(s(a_{\pi_E(j)}, b_{j'})_{j,j'\in J} \bigwedge_{i\in I} a_{\pi_E(i)}$$

is independent from the choice of π_E. Indeed let $\pi \in \mathrm{Sym}(K)$ with $\pi(J) = E$. Let $\sigma = \pi^{-1}\pi_E$. Let $\sigma_J \in \mathrm{Sym}(J)$ be defined by $\sigma_J(j) = \sigma(j)$. Similarly define σ_I. Then

$$\det(s(a_{\pi_E}(j), b_{j'})) = \det(s(a_{(\pi\sigma_J(j)}, b_{j'}) = \mathrm{sgn}\sigma_J \det(s(a_{\pi i}, b_{j'})$$

and

$$\bigwedge_{i\in I} a_{\pi_E(i)} = \bigwedge_{i\in I} a_{\pi\sigma_I(i)} = \mathrm{sgn}\sigma_I \bigwedge_{i\in I} a_{\pi(i)}.$$

Using that $\mathrm{sgn}\pi = \mathrm{sgn}\sigma\mathrm{sgn}\pi_E = \mathrm{sgn}\sigma_I\mathrm{sgn}\sigma_j\mathrm{sgn}\pi_E$ and multiplying the last two equations together we obtain the claimed independence from the choice of π_E.

Define

$$f : A^K \times B^J \to \bigwedge^J A, \quad (a,b) \to \sum_{E\in\Delta} f_E(a,b)$$

In view of 5.2.6 it remains to show that f_b and f_a are alternating for all $a \in A^K$ and $b \in B^J$. That f_a is alternating is obvious. So suppose $b \in B^J$ and $a \in A^K$ with $a_k = a_l$ for distinct $k,l \in K$. Let $E \in \Delta$ and put $\pi = \pi_E$. If k and l are both in $\pi(J)$ then $\det(s(a_{\pi j}, b_{j'})) = 0$. If k,l are both in I then $\bigwedge_{i\in I} a_{\pi(i)} = 0$. So in both these cases $f_E(a,b) = 0$. Suppose now that $k \in \pi(I)$ and $l \in \pi(J)$. Let $\sigma = (k,l) \in \mathrm{Sym}(K)$ and $E' = \sigma(E) \neq E$. We may choose $\pi_{E'} = \sigma\pi$. $a_k = a_l$ now implies $f_{E'}(a,b) = \mathrm{sgn}\sigma f_E(a,b)$ and so $f_{E'}(a,b) + f_E(a,b) = 0$. If follows that $f_b(a) = f(a,b) = 0$ and f_b is alternating.

(c) Let $a \in A^K$, $b^\in B^J$. Note that $\beta \circ b = (\beta(b_j))$. Let $E \in \Delta$. Then

$$(\bigwedge^I \alpha)(f_E(a,\beta\circ b)) = (\bigwedge^I \alpha)(\mathrm{sgn}\pi_E \det(s(a_{\pi_E(j)},\beta(b_{j'}))\bigwedge_{i\in I} a_{\pi_E(i)}) =$$

$$= \mathrm{sgn}\pi_E \det(s(\alpha(a_{\pi_E(j)}, b_{j'})\bigwedge_{i\in I}\alpha(a_{\pi_E(i)})) = f_E(\alpha\circ a, b)$$

Thus (c) holds.

(d) Suppose $E \in \Delta$ and $f_E(a,b) \neq 0$ where $a = (e_{\alpha(k)})$ and $b = (f_{\beta(j)})$. Let $A = s(e_\alpha(\pi_E(j)), f_{\beta(j'})$. Then $\det A \neq 0$. Let $t \in E$. Then $t = \pi_E(j)$ for some $\in J$ and so $(s(e_\alpha(t), t, \alpha f_{\beta(j')})_{j'\in J}$ is a row of A. This row cannot be zero and $s(e_\alpha(t), t, \alpha f_{\beta(t'}) \neq 0$ for some $t' \in J$. But then $\alpha(t) = \beta(t')$. It follows that $\beta(J) \subseteq \alpha(I)$ and $E = \alpha^{-1}\beta(I)$. Also $\det A = \pm 1$ and so (ca) holds. □

Proposition 5.3.5. *Let R be a ring and M an R-module.*

(a) Let I, J and K finite sets with $K = I \uplus J$ Then there exists a unique bilinear map

$$\wedge : \bigwedge^I M \times \bigwedge^J M \to \bigwedge^K M, (a,b) \to a \wedge b$$

with

$$(\wedge_{i\in I} m_i) \wedge (\wedge_{j\in J} m_j) = \wedge_{k\in K} m_i$$

for all $(m_i) \in M^{k+l}$.

(b) Define

$$\bigwedge M = \bigoplus_{i=0}^{\infty} \bigwedge^i M$$

and

$$\wedge : \bigwedge M \times \bigwedge M \to \bigwedge M, \quad (a_i)_{i=o}^{\infty} \wedge (b_j)_{j=0}^{\infty} = (\sum_{i=0}^{k} a_i \wedge b_{k-i})_{k=0}^{\infty}.$$

Then $(\bigwedge M, +, \wedge)$ *is a (non)-commutative ring with* $R = \bigwedge^0 M \leq Z(\bigwedge M)$.

Proof. (a) Define $f : M^I \times M^J \to \bigwedge^K M, ((a_i),(a_j)) \to \wedge_{k\in K} a_k$. Clearly $f_{(a_i)}$ and $f_{(a_j)}$ is alternating and so (a) follows from 5.2.6.

(b) First of all $(\bigwedge M, +)$ is an abelian group. By (a) $\wedge$ is bilinear. So the distributive laws hold. Let l, m, n be non-negative integers and $m_k \in M$ for $1 \leq k \leq l + m + n$. Then

$$(\bigwedge_{i=1}^{l} m_i \wedge \bigwedge_{i=l+1}^{l+m} m_i) \wedge \bigwedge_{i=l+m+1}^{l+m+n} m_i = \bigwedge_{i=1}^{l+m+m} m_i = \bigwedge_{i=1}^{l} m_i \wedge (\bigwedge_{i=l+1}^{l+m} m_i \wedge \bigwedge_{i=l+m+1}^{l+m+n} m_i)$$

and so $\wedge$ is associative.

So $(\bigwedge M, +, \wedge)$ is indeed a (non)-commutative ring. That $R \leq Z(\bigwedge M)$ follows from the fact that $\wedge$ is R-linear. □

Lemma 5.3.6. *Let R be a ring and $s : A \times B \to C$ a finite pairing.*

(a) The functions

$$s_A : A \to \mathrm{Hom}_R(B, C), a \to s_a$$

and

$$s_B : B \to \mathrm{Hom}_R(A, C), b \to s_b$$

are R-linear isomorphism.

(b) Let $f \in \mathrm{End}_R(B)$. Then there exists a unique $f^s \in \mathrm{End}_R(A)$ with $s(f^s(a), b) = s(a, f(b))$ for all $a \in A$, $b \in B$.

(c) Suppose $(a_d, d \in D)$, $(b_d, d \in D)$ and (c) are s-basis for (A, B, C). Let $M_D(f^s) = M_D(f)^T$

Proof. Let $((a_d \mid, d \in D), (b_d \mid d \in D), c)$ be an s basis. (a) For $e \in D$ define $\phi_e \in \mathrm{Hom}_R(B, C)$ by $\phi_e(\sum_{r_d b_d} = r_e c$. Then $(\phi_d, d \in D)$ is a basis for $\mathrm{Hom}_R(B, C)$. Since $s(a_e, b_d) = \delta_{ed} c$. $s_A(e) = \phi_e$. Hence (a) holds.

(b) Define $\tilde{f} \in \mathrm{End}_R(\mathrm{Hom}_R(B, C)$ by $\tilde{f}(\phi) = \phi \circ f$. Let $g \in \mathrm{End}_R(A), a \in A$ and $b \in B$. Then

$$s(a, f(b)) = s_A(a)(f(b)) = ((\tilde{f})(s_A))(a)(b)$$

and

$$s(g(a), b) = s_A(g(a))(b)$$

Hence $s(a, f(b) = s(g(a), b)$ for all $a \in A$, $b \in B$ if and only if $\tilde{f} \circ s_A = s_A \circ g$. By (a), s_A has an inverse so $f^s = s_A^{-1} \tilde{f} s_A$ is the unique element fulfilling (c).

(c) Let $g \in \mathrm{End}_R(B)$. Put $U = M_f(D)$ and $V = M_g(D)$. So $g(a_d) = \sum_{h\in D} v_{hd} a_h$ and $f(b_d) = \sum_{h\in D} u_{hd} b_h$. Thus

$$s(a_e, f(b_d)) = \sum_{h\in D} u_{hd} s(a_e, b_h) = u_{ed} c$$

and

$$s(g(a_e), b_d) = sum_{h\in D} v_{he} s(a_h, b_d) = v_{de} c$$

Hence $s(a, f(b)) = s(g(a), f)$ for all $a \in A$, $b \in B$ if and only if $v_{de} = u_{ed}$ for all $d, e \in D$. So (c) holds (and we have a second proof for (b)). □

Recall that for an R-module M, M^* denote the dual module, so $M^* = \mathrm{Hom}_R(M, R)$.

Lemma 5.3.7. *Let R be a ring, M a free module of finite rank over R and I a finite set*

(a) There exists a unique R-bilinear function $s^I : \bigwedge^I M^* \times \bigwedge^I M \to R$ with $s^I(\bigwedge \phi_i, \bigwedge m_i) = \det(\phi_i(m_j))_{i,j\in I}$.

(b) s_I is a finite pairing.

(c) $\bigwedge^I M^* \cong (\bigwedge^I M)^*$ as R-modules.

Proof. Define $s : M^* \times M \to R, (\phi, m) \to \phi(m)$. (a) follows from 5.3.4(a) applied with $A = M^*, B = M, K = I, J = I$ and "$I = \varnothing$". And (b) follows from part (d) of the same lemma. Finally (c) is a consequence of (b) and 5.3.6(a). □

Proposition 5.3.8. *Let R be a ring and M a R-module of finite rank. Let $f \in \mathrm{End}_R(M)$. Then there exists $f^{\mathrm{ad}} \in \mathrm{End}_R(M)$ with $f \circ f^{\mathrm{ad}} = f^{\mathrm{ad}} \circ f = \det f \mathrm{id}_M$.*

Proof. Consider $t : M \times \bigwedge M^{n-1} \to \bigwedge M^n, (m, b) \to m \wedge b$. We claim that t is a finite pairing. For this let $(a_i, 1 \le i \le n)$ be a basis for M. Put $b_i = a_1 \wedge a_2 \wedge a_{i-1} \wedge a_{i+1} \wedge a_n$. Let $c = a_1 \wedge \dots a_n$. By 5.2.8, $(b_i, 1 \le i \le n)$ is a basis for $\bigwedge^{n-1} M$ and $\{c\}$ is a basis for $\bigwedge^n M$. Also $a_i \wedge b_j = 0$ for $i \neq j$ and $a_i \wedge b_i = (-1)^{i_1} c$. $((a_i), ((-1)^{i-1} b_i), c)$ is a t basis. Let $f^a d = (bigwedge^{n-1} f)^t$ be given by 5.3.6(b). So $f^{\mathrm{ad}} \in \mathrm{End}_R(M)$ is uniquely determined by

$$f^a d(m) \wedge b = m \wedge (\overset{n-1}{\bigwedge} f)(b)$$

for all $m \in M, b \in \bigwedge^{n-1} M$.

In particular,

$$(f^{\mathrm{ad}}(f(m) \wedge b) = f(m) \wedge (\overset{n-1}{\bigwedge} f)(b) = (\overset{n}{\bigwedge} f)(m \wedge b) = (\det f)(m \wedge b) = m \wedge (\det f) b$$

Note that also $(\det f) m \wedge b = m \wedge (\det f) b$ and so by 5.3.6

$$f^{\mathrm{ad}} \circ f = ((\det f) \mathrm{id}_{\bigwedge^{n-1} M})^t = (\det f) \mathrm{id}_M$$

To show that also $f \circ f^{\mathrm{ad}} = \mathrm{id}_M$ we use the dual M^* of M. Recall that $f^* \in \mathrm{End}_R(M^*)$ is define by $f^*(\phi) = \phi \circ f$. It might be interesting to note that $f^* = f^s$, where s is the pairing $s : M^* \to M, (\phi, m) \to \phi(m)$.

Applying the above results to f in place of f^* we have

$$f^{*\mathrm{ad}} \circ f^{*} = (\det f^{*})\mathrm{id}_{M^{*}}$$

By 5.3.2(g) we have $\det f{\ast} = \det f$. So dualizing the previous statement we get

$$f \circ (f^{*\mathrm{ad}*} = \det f \mathrm{id}_M$$

So the proposition will be proved once we show that $f^{*\mathrm{ad}*} = f^{\mathrm{ad}}$ or $f^{*\mathrm{ad}} = f^{\mathrm{ad}^*}$.

To do this we will compute that matrix of f^{ad} with respect to the basis (a_i). Let D be the matrix of f with respect to (a_i) and E the matrix of $\bigwedge^{n-1} f$ with respect to $((-1)^{i-1}b_i)$. We compute

$$(\bigwedge^{n-1} f)(b_i) = \wedge_{h\neq i} f(a_h) = \wedge_{h\neq i}(\sum_{k=1}^{n} d_{hk}a_k$$

Let D_{ij} be the matrix $(d_{kl})_{k\neq i, l\neq j}$. Then the coefficient of b_j in $\wedge_{h\neq i}(\sum_{k=1}^{n} d_{hk}a_k$ is readily seen to be $\det D_{ij}$.

It follows that

$$E_{ij} = (-1)^{i-1}-1^{j-1} \det D_{ij} = (-1)^{i+j} \det D_{ij}$$

Let (ϕ_i) be the basis of M^* dual to (a_i). So $\phi_i(a_j) = \delta_{ij}$. Then the matrix for f^* with respect to (ϕ_i) is D^T. Note that $(D^T)_{ij} = (D_{ji})^T$ and so the (i,j) coefficient of the matrix of $f^{*\mathrm{ad}}$ is

$$(-1)^{i+j}\det(D^T)_{ij} = (-1)^{i+j}\det(D_{ji})^T = (-1)^{i+j}\det D_{ji}$$

Thus $f^{*\mathrm{ad}}$ has the matrix E^T with respect to (ϕ_i). So does $(f^{\mathrm{ad}*}$. Hence $f^{*\mathrm{ad}} = f^{\mathrm{ad}*}$ and the proposition is proved. □

Lemma 5.3.9. *Let R and S be rings with $R \leq S$. Let M be an R module. Then there exists bilinear function*

$$\cdot : S \times S \otimes_R M \to S \otimes M, (s, \tilde{m}) \to s\tilde{m}$$

with

$$s(t \otimes m = st \otimes m$$

for all $s, t \in S$ and $m \in M$. Moreover, $(S \otimes_R M, c \cdot 0$ is an S-module.

Proof. Let $s \in S$. By 5.1.12 there exists a unique $s\mathrm{id}_S \otimes id_M \in \mathrm{End}_R(S \otimes_R M)$ which sends $t \otimes m$ to $st \otimes m$. We will write $s \otimes 1$ for $s\mathrm{id}_S \otimes \mathrm{id}_M$. It is readily verified that $s \to s \otimes 1$ is a ring homomorphism. So the lemma is proved. □

Lemma 5.3.10. *Let R and S be rings with $R \leq S$.Let M be a free R-module with basis $\mathcal{B}$.*

(a) $S \otimes_R M$ is a free S-module with basis $1 \otimes \mathcal{A} := \{1 \otimes b \mid b \in \mathcal{B}$.

(b) Let $\alpha \in \mathrm{End}_R(M)$, A the matrix of α with respect to $\mathcal{B}$ and $s \in S$. Then sA is the matrix of $s \otimes \alpha$ with respect to $1 \otimes \mathcal{B}$.

Proof. (a) Note that $M = \bigoplus_{b\in\mathcal{B}} Rb$ and $Rb \cong R$. By 5.1.10 $S \otimes_R M \cong \bigoplus_{b\in\mathcal{B}} S \otimes_R Rb$. Also by 5.1.6 $S \otimes_R b \cong S$.

(b) Let $d \in \mathcal{B}$ Then

$$(s \otimes \alpha)(1 \otimes d) = s \otimes \alpha(d) = s \otimes (\sum_{e\in\mathcal{B}} b_{ed} e) = \sum_{e\in\mathcal{B}} (sb_{ed}(1 \otimes e)$$

So (b) holds. □

Definition 5.3.11. *Let R be a ring, M a free R-module of finite rank and $\alpha \in \mathrm{End}_R(M)$.*

(a) Let S be a ring with R as a subring. Let $s \in S$. Then $s \otimes \alpha$ denotes the unique R-endomorphism of $S \otimes_R M$ with

$$(s \otimes 1)(t \otimes m) = (st \otimes \alpha(m)$$

for all $t \in S, m \in M$.

(b) Consider $x \otimes 1 - 1 \otimes \alpha \in \mathrm{End}_{R[x]}(R[x] \otimes_R M)$. Then

$$\chi_\alpha = \det(x \otimes 1 - 1 \otimes \alpha) \in R[x]$$

is called the characteristic polynomial *of α.*

(c) Let n be positive integer and $A \in \mathcal{M}_R(n)$. Consider the matrix $xI_n - A \in \mathcal{M}_{R[x]}(n)$. Then $\chi_A = \det(xI_n - A)$ is called the characteristic polynomial *of A.*

Lemma 5.3.12. *Let R be a ring, M an R-module with finite basis I, $n = |I|$, $\alpha \in \mathrm{End}_R(M)$ and A the matrix of α with respect to A.*

(a) $\chi_\alpha = \chi_A$.

(b) For $J \subset I$ let $A_J = (a_{ij})i, j \in J$. The coefficient of x^m in χ_A is

$$(-1)^{n-m} \sum_{J\subset I, |J|=n-m} \det A_J$$

(c) χ_α is monic of degree n.

Proof. (a) By 5.3.10(b) the matrix for $x \otimes 1 - 1 \otimes \alpha$ with respect to $xI_n - A$. Thus (a) follows from 5.3.2(f)

(b) Let $D = xI_n - A$. Let a_i be the i column of A_i. Let $e_i = (\delta_{ij})$. The $D = (xe_i - a_i)$. For $J \subset I$ let A_J^* be the matrix with whose k-column is a_k if $k \in J$ and e_k if $k \notin J$. Then since det is multilinear

$$\det D = \sum_{J\subseteq I} x^{|I|-|J|}(-1)^{|J|} \det A^* J$$

.

Let $T(J)$ be the matrix with

$$t(J)_{ij} = \begin{cases} a_{ij} & \text{if } i, j \in J \\ 1 & \text{if } i = j \notin J \\ 0 & \text{otherwise} \end{cases}$$

Then it is easy to see that $\det A^*(J) = \det T(J) = \det A(J)$ and (b) follows.
(c) Follows from (b) □

Theorem 5.3.13. *Let R be a ring, M be a free R-module of finite rank. Let $\alpha \in \mathrm{End}_R(M)$. Then*

$$\chi_\alpha(\alpha) = 0.$$

Proof. Define

$$\phi : R[x] \times M \to M, \quad (f,m) \to f(\alpha)(m).$$

Since ϕ is bilinear there exists a unique R-linear map

$$\Phi : R[x] \otimes_R M \to M \text{ with } \Phi(f \otimes m) = f(\alpha)(m).$$

Let $\beta = x \otimes 1 - 1 \otimes \alpha \in \mathrm{End}_{R[x]}(R[x] \otimes_R M)$.
Let $f \in R[x]$ and $m \in M$. Then

$$\beta(f \otimes m) = xf \otimes m - f \otimes \alpha(m) = fx \otimes m - f \otimes \alpha(m)$$

and so

$$\Phi(\beta(f \otimes m)) = (f(\alpha)\alpha)(m) - (f(\alpha)(\alpha(m)) = 0$$

Hence $\Phi\beta = 0$.
By 5.3.8 there exists $\beta^{\mathrm{ad}} \in \mathrm{End}_{R[x]}(R[x] \otimes_R M)$ with $\beta \circ \beta^{\mathrm{ad}} = \det\beta \otimes 1$.
It follows that

$$0 = (\Phi \circ \beta) \circ \beta^{\mathrm{ad}} = \phi \circ (\beta \circ \beta^{\mathrm{ad}}) = \Phi \circ (\det\beta \otimes 1)$$

So

$$0 = \phi((\det\beta \otimes 1))(1 \otimes m) = \phi(\det\beta \otimes m) = (\det\beta)(\alpha)(m)$$

By definition $\chi_\alpha = \det\beta$ and so the Cayley Hamilton Theorem is proved. □

Theorem 5.3.14. *Let M be a finitely generated R-module and $\alpha \in \mathrm{End}_R(M)$. Then there exists a monic polynomial $f \in R[x]$ with $f(A) = 0$.*

Proof. Let I be a finite subset of M with $M = RI$. Let $F = F_R(I)$ be the free R-module on I. So F has a basis $(a_i, i \in I)$. Let π be the unique R-linear map from F to M with $a_i \to i$ for all $i \in I$. Since $M = RI$, $M = \pi(F)$. By 3.7.3 there exists $\beta \in \mathrm{End}_R(F)$ with

$$\pi \circ \beta = \alpha \circ \pi$$

We claim that (*) $\pi \circ f(\beta) = f(\alpha) \circ \pi$ for all $f \in R[x]$

For this let $S = \{f \in R[x] \mid \pi \circ f(\beta) = f(\alpha) \circ \pi\}$. Let $f, g \in S$. Then

$$\pi \circ (fg)(\alpha) = \pi \circ (f(\alpha \circ g(\alpha)) = (\pi \circ f(\alpha) \circ g(\alpha) = (f(\alpha) \circ \pi) \circ g(\alpha) =$$
$$= f(\alpha) \circ (\pi \circ g(\alpha)) = f(\alpha) \circ (g(\alpha) \circ \pi) = (f(\alpha) \circ g(\alpha)) \circ \pi) = (fg)(\alpha) \circ \pi$$

Since π is $\mathbb{Z}$-linear, also $f - g \in S$. Thus S is a subring of $R[x]$. Since R and x are in S, $S = R[x]$ and (*) is proved. Let $f = \chi_\beta$. The f is monic and by 5.3.13 $f(\beta) = 0$. By (*)

$$f(\alpha) \circ \pi = \pi \circ f(\beta) = 0$$

Since π is onto this implies $f(\alpha) = 0$. □

Chapter 6

Hilbert's Nullstellensatz

Throughout this chapter ring means commutative ring with identity and R is a ring. All R-modules are assumed to be unitary.

6.1 Multilinear Maps

Definition 6.1.1. *Let $(V_i, i \in I)$ a family of R-modules, an R module and $f : \bigtimes_{i\in I} M_i \to M$ a function. Let $I = J \cup K$ with $J \cap K = \varnothing$,*

(a) $V_J := \bigtimes_{j\in J} V_j$.

(b) *If $u = (u_j)_{j\in J} V_J$ and $v = (v_k)_{k\in K} \in V_K$, then we identify $(u, v) \in V_J \times V_K$ with the tuple $w = (w_i)_{i\in I}$ where $w_i = u_i$ if $i \in J$ and $w_i = v_i$ if $i \in K$. We also write $f(u, v)$ for $f((u, v))$.*

(c) *For $u \in V_J$ define $f_u : V_K \to W, v \to f(u, v)$. Sometimes we will write f_u^J for f_u.*

(d) *f is called R-multilinear if for all $i \in I$ and all $u \in V_{I\setminus i,}$, $f_u : V_i \to W$ is R-linear.*

(e) *An R-multilinear map is called bilinear of $|I| = 2$ and trilinear if $|I| = 3$.*

(f) $W^I = \bigtimes_{i\in I} W$.

Example 6.1.2. (a) If $|I| = 1$ a R-multilinear map is R-linear map.

(b) $R^n \times R^n \to R, \left((r_i)_{i=1}^n, (s_i)_{i=1}^n\right) \to \sum_{i=1}^n r_i s_i$ is R-bilinear.

(c) Let V be an R-module. Note that $\mathrm{End}_R(V)$ is an R module via $(r\phi)(v) = r\phi(m)$. Then $\mathrm{End}_R(V) \times V \to V, (\phi, v) \to \phi(v)$ is R-bilinear.

Definition 6.1.3. *Let V and W be R-modules and I a set. Put $V_i = V$ for all $i \in I$ and so $V_J = V^J$ for all $J \subseteq I$. An R-multilinear function $f : V^I \to V$ is called*

(a) symmetric *if $f_u(v, w) = f_u(v, v)$,*

(b) skew-symmetric *if* $f_u(v,w) = -f_u(w,v)$*;*

(c) alternating *if* $f_u(v,v) = 0$.

for all $i \neq j \in I$*,* $u \in V^{I\smallsetminus\{i,j\}}$ *and* $v,w \in V$.

Lemma 6.1.4. *(a) Every alternating map is skew-symmetric.*

(b) If $f : M^I \to N$ *is skew symmetric and* $2n \neq 0_N$ *for all* $n \in N^\sharp$*, then* f *is alternating.*

Proof. Let $i \neq j \in I$, $u \in M^{I\smallsetminus\{i,j\}}$, $v,w \in M$ and put $g = f_u$.

(a) $0 = g(v+w,v+w) = g(v,v) + g(v,w) + g(w,v) + g(w,w) = g(v,w) + g(w,v)$.

(b) From $g(v,w) = -g(w,v)$ applied with $v = w$ we get $g(v,v) = -g(v,v)$. So $2g(u,u) = 0$ and $g(u,u) = 0$ □

Lemma 6.1.5. *Let* I *be a set,* $(I_j)_{j\in J}$ *a partition of* I*,* $(V_i)_{i\in I}$ *and* $(W_j, j \in J)$ *families of* R*-modules and* Z *an* R*-module. Let* $f : W_J \to Z$ *be* R*-multilinear and for each* $j \in J$ *let* $g_j : V_{I_j} \to W_j$ *be* R*-multilinear. Then*

$$V_I \to Z, (v_i)_{i\in I} \to f\left(\left(g_j\big((v_i)_{i\in I_j}\big)\right)_{j\in J}\right)$$

is R*-multilinear.*

Proof. Readily verified. □

Lemma 6.1.6. *Let* I *be finite set,* $(V_i, i \in I)$ *be family of* R*-modules and* W *an* R*-module. Suppose that for each* $i \in I$*,* V_i *is a free* R*-module with basis* $\mathcal{B}_i \subseteq V_i$*. Put* $\mathcal{B}_i = \times_{i\in I} \mathcal{B}_i \subseteq V_I$ *and let* $g : \mathcal{B}_I \to W$ *be a function. Then there exists a unique* R*-multilinear map* $f : V_I \to W$ *with* $f|_{\mathcal{B}_I} = g$.

Proof. Suppose first that $f : V_I \to W$ is R-multilinear with $f|_{\mathcal{B}_I} = g$. Let $v = (v_i)_{i\in I} \in V_I$. Then since $\mathcal{B}_i$ is a basis for V_i there exists uniquely determined $r_{ib_i} \in R, b_i \in \mathcal{B}_i$ with

$$v_i = \sum_{b_i\in\mathcal{B}_i} r_{ib_i} b_i$$

Since f is R-multilinear we conclude that

$$(*) \qquad \begin{aligned} f(v) &= f\left(\left(\textstyle\sum_{b_i\in\mathcal{B}_i} r_{ib_i} b_i\right)_{i\in I}\right) \\ &= \textstyle\sum_{(b_i)_{i\in I}\in\mathcal{B}_i} \left(\prod_{i\in I} r_{ib_i}\right) f\big((b_i)_{i\in I}\big) \\ &= \textstyle\sum_{(b_i)_{i\in I}\in\mathcal{B}_i} \left(\prod_{i\in I} r_{ib_i}\right) g\big((b_i)_{i\in I}\big) \end{aligned}$$

So f is uniquely determined. Conversely it is readily verified that (*) defines an R-multilinear map. If $v \in \mathcal{B}_I$, then $r_{ib_i} = \delta_{v_i b_i}$ and so $\prod_{i\in I} r_{ib_i} = \prod_{i\in I} \delta_{v_i b_i}$, which is 0 unless $v_i = b_i$ for all $i \in I$, in which case it is 1. So $f(v) = g(v)$ for $v \in \mathcal{B}_I$. □

Proposition 6.1.7. *Let $n \in \mathbb{Z}^+$, $\mathrm{M}_n(R)$ the ring of $n \times n$-matrices with coefficients in R and $A \in M_n(R)$. We define the* determinant $\det(A)$ *of A inductively on as follows: If $n = 1$ and $A = (a)$, define* $\det(A) = a$. *Suppose next $n > 1$ and that* $\det(B)$ *has been defined for all $(n-1) \times (n-1)$-matrices. For $1 \leq i, j \leq n$ let A_{ij} be the $n \times n$ matrix defined obtained from A by deleting row i and column j. Define*

$$\det_j(A) := \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}$$

Then $\det_j(A) = \det_l(A)$ *for all* $1 \leq j, l \leq n$ *and we define* $\det(A) = \det_j(A)$. *View* $\det$ *function in the n-columns :*

$$\det : (R^n)^n \to R, ((a_{ij})_{i=1}^n)_{j=1}^n \to \det\big((a_{ij})\big)$$

Then $\det$ *is alternating and R-linear. Also* $\det(I_n) = 1$,

Proof. We will first show that $\det_j(A) = \det_l(A)$. Without loss $j < k$. We have

$$\begin{aligned} \det_j(A) &= \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) \\ &= \sum_{i=1}^{n} \sum_{k=1, k \neq i} (-1)^{i+j} (-1)^{\epsilon} a_{ij} a_{kl} \det((A_{ij})_{kl}) \end{aligned}$$

where $(A_{ij})_{kl})$ is the matrix obtained by deleting row i and k and columns j and l from A and ϵ is as follows:

Observe that column l of A is column $l-1$ of A_{ij}. If $k < i$, then row k of A is row k of A_{ij}. If $k > i$, then row k of A is row $k-1$ of A_{ij}. Hence

$$\epsilon = \begin{cases} k + l - 1 & \text{if } k < i \\ k + l - 2 & \text{if } k > i \end{cases}$$

Similarly

$$\begin{aligned} \det_l(A) &= \sum_{k=1}^{n} (-1)^{k+l} a_{kl} \det(A_{kl}) \\ &= \sum_{k=1}^{n} \sum_{i=1, i \neq k} (-1)^{k+l} (-1)^{\eta} a_{kl} a_{ij} \det(A_{kl})_{ij}) \end{aligned}$$

where $(A_{kl})_{il})$ is the matrix obtained by deleting row k and i and columns l and j from A and η is as follows:

Observe that column j of A is column j of A_{kl}. If $k < i$, then row i of A is row $i-1$ of A_{kl}. If $k > i$, then row i of A is row i of A_{kl}. Hence

$$\eta = \begin{cases} i + j - 1 & \text{if } k < i \\ i + j & \text{if } k > i \end{cases}$$

If $i < k$ we conclude

$$(-1)^{i+j}(-1)^{k+l+\epsilon} = (-1)^{i+j+k+l-1} = (-1)^{k+l}(-1)^{\eta}$$

and if $k > i$ then

$$(-1)^{i+j}(-1)^{k+l+\epsilon} = (-1)^{i+j+k+l-2} = (-1)^{i+j+k+l} = (-1)^{k+l}(-1)^{\eta}$$

Thus show that $\det_j(A) = \det_l(A)$ and so we can define $\det(A) = \det_j(A)$ for any $1 \leq j \leq n$. Clearly $\det_j$ is R-linear as a function in column j of A (with the remaining columns fixed). Since $\det = \det_j$ we conclude that det is R-multilinear as a functions of its columns.

To show that det is alternating suppose that column r and column s of A are equal for some $1 \leq r < s$ of A. Suppose $n \geq 3$. Then we may choose $j \neq r$ and $j \neq s$. Then for each i, A_{ij} has two equal columns. Thus by induction $\det(A_{ij}) = 0_R$ for all i and so $\det(A) = \det_j(A) = 0_R$.

So suppose $n = 2$. Then $A = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$ and so $\det A = ab - ba = 0_R$. Thus det is alternating.

Suppose $A = I_n$. Then for $i \neq j$, A_{ij} has a zero column and so $\det(A_{ij} = 0_R$. For $i = j$, $A_{ii} = I_{n-1}$ and so by induction $\det A_{ii} = 1_R$. So $\det I_n = 1_R$. □

Lemma 6.1.8. *Let $n \in \mathbb{N}$ and $A = (a_{ij}) \in \mathrm{M}_n(R)$. Define the $A^{\mathrm{ad}} = (b_{ij}) \in \mathrm{M}_n(R)$ by $b_{ij} = (-1)^{ij}\det(A_{ji})$. Then*

$$\mathbb{A}^{\mathrm{ad}}A = \det(A)I_n$$

A^{ad} is called the adjoint *of A.*

Proof. Fix $1 \leq i, j \leq n$ and let $D = (d_{rs})$ be $n \times n$ obtained from A by replacing column i of A by column j if A. So

$$d_{rs} = \begin{cases} a_{rs} & \text{if } s \neq i \\ a_{rj} & \text{if } s = i \end{cases}$$

Note that $A_{ki} = D_{ki}$. The (i, j)-coefficient of $A^{\mathrm{ad}}A$ is

$$\begin{aligned} \textstyle\sum_{k=1}^{n} b_{ik}a_{kj} &= \textstyle\sum_{k=1}^{n} a_{kj}(-1)^{i+k}\det(A_{ki}) \\ &= \textstyle\sum_{k=1}^{n} d_{ki}(-1)^{i+k}\det(D_{ki}) \end{aligned}$$

The definition of $\det = \det_i$ shows that this is equal to $\det D$. If $i = j$, then $D = A$ and so $\det D = \det A$. If $i \neq j$, then the i and j columns of D are equal and so $\det A = 0_R$. Thus $A^{\mathrm{ad}}A = \det(A)I_n$. □

Proposition 6.1.9. *Let V and W be R-modules and I a finite set. Suppose V is free of finite rank and $\mathcal{B}$ is a finite R-basis for V. Choose a total order on I and a total order on $\mathcal{B}$. Let*

$$\mathcal{B}^I_< = \{(b_i)_{i\in I} \mid b_i < b_j \textit{ for all } i < j \in I\}$$

Let $g : \mathcal{B}^I_< \to W$ be any function. Then there exists unique alternating R-multilinear function with $f : V^I \to W$ with $f|_{\mathcal{B}^I_<} = g$.

Proof. Let $f : V^I \to I$ be a alternating R-multilinear function with $f|_{\mathcal{B}^I_<} = g$. To show that f is unique it suffices to show that $f(b)$ is uniquely determined for all $b = (b_i)_{i\in I} \in \mathcal{B}^I$, (see 6.1.6). If $b_i = b_j$ for some $i \neq j \in I$, then since f is alternating $f(b) = 0_R$. So suppose that $b_i \neq b_j \in i$. Then there exists a unique $\pi \in \mathrm{Sym}(I)$ such that $b \circ \pi \in \mathcal{B}^I_<$ (note here that $b \circ \pi = (b_{\pi(i)})_{i\in I}$). Observe that there exist 2-cycles $\pi_j = (a_j, b_j) \in \mathrm{Sym}(I), 1 \leq j \leq k$ such that $\pi = \pi_1\pi_2\ldots\pi_k$. By 6.1.4(a), $f(c \circ \mu) = -f(c)$ for all $c \in V^I$ and any two cycle $\mu \in \mathrm{Sym}(I)$. $f(b) = (-1)^k f(b \circ \pi) = (-1)^k g(b \circ \pi)$ and so also $f(b)$ is uniquely determined.

To show the existence of f we assume without loss that $I = \{1, 2, \ldots, n\}$ with the usual ordering. Let $v = (v_i)_{i\in I} \in V^I$. Then $v_i = \sum_{b\in\mathcal{B}} a_{ib} b$ for some unique $a_{ib} \in R, i \in I, b \in \mathcal{B}$. Let $A = (a_{ib}) \in M_{I\times\mathcal{B}}(R)$. For $b = (b_i)_{i\in I} \in \mathcal{B}^I_<$ let A_b be the $n \times n$ submatrix $(a_{ib_j})_{1\leq i,j\leq n}$ of A. Define

$$f(v) := \sum_{b\in\mathcal{B}^I_<} \det(A_b) g(b)$$

Since det is an alternating it is easy to see that f is alternating and R-multilinear. Suppose $v \in \mathcal{B}^I_<$ and $b \in \mathcal{B}^I_<$. Then $r_{ib_j} = \delta_{d_i b_j}$ Thus A_b has a zero column unless each b_j is equal to some d_i. Since both b and d are increasing, this shows that $\det(A_b) = 0_R$ for all $b \neq v$. For $b = v$, $A_b = I_n$ and so $\det(A_v) = 1$. So $f(v) = g(v)$ and $f|_{\mathcal{B}^I_<} = g$. □

Lemma 6.1.10. *Let V and W be R-modules and I a set.*

(a) Let $\mathrm{L}_I(V, W)$ is the set of R-multilinear map from $V^I \to W$. Then $\mathrm{L}_I(V, W)$ is an R-module via:

$$(f + g)(v) = f(v) + g(v) \textit{ and } (rf)(v) = rf(v)$$

for all $f, g \in \mathrm{L}_I(V, W)$, $r \in R$ and $v \in V^I$.

(b) V^I is an R and an $\mathrm{End}_R(V)$-module via $u + v = (u_i + v_i)_{i\in I}$, $rv = (ru_i)_{i\in I}$ and $sv = (s(v_i))_{i\in I}$ for all $u = (u_i)_{I\in I}, v = (v_i)_{i\in I} \in V^I$, $r \in R$ and $s \in \mathrm{End}_R(V)$.

(c) The monoid ($\mathrm{End}_R(V), \circ)$ is acting on $\mathrm{L}_I(V, W)$ on the right via

$$(fs)(v) = f(sv)$$

for all $f \in \mathrm{L}_I(V, W)$, $s \in \mathrm{End}_R(V)$ and $v \in V^I$.

(d) $\mathrm{L}_I(V, W)$ is a $\mathrm{End}_R(W)$-module via

$$(tf)(v) = t(f(v))$$

for all $f \in \mathrm{L}_I(V, W)$, $t \in \mathrm{End}_R(W)$ and $v \in V^I$.

(e) Let $\bigwedge_I(V, W)$ be the the set of alternating R-multilinear map from $V^I \to W$. Then $\bigwedge_I(V, W)$ is an $\mathrm{End}_R(V)$-invariant R-submodule of $\mathrm{L}_I(V, W)$.

Proof. Readily verified. □

Corollary 6.1.11. *Let V and W be free R-modules with basis $\mathcal{B}$ and $\mathcal{D}$ and I a set. Suppose I and $\mathcal{B}$ are finite and choose a total orderings on I and a total ordering on $\mathcal{B}$. For $b \in \mathcal{B}^I_<$ and $d \in \mathcal{D}$ let $f^{bd} : V^I \to W$ be the unique alternating R-multilinear map with*

$$f^{bd}(c) = \begin{cases} d & \text{if } b = c \\ 0_W & \text{if } b \neq c \end{cases}$$

Then $\bigwedge_I(V, W)$ is a free R-module with basis $(f^{bd})_{(b,d)\in\mathcal{B}^I_<\times\mathcal{D}}$.

Proof. Let $f \in \bigwedge_I(V, W)$ and let $a_{bd} \in R$ for $b \in \mathcal{B}^I_<$ and $d \in \mathcal{D}$, almost all 0. Then

$$\begin{array}{rcll} f & = & \sum_{(b,d)\in\mathcal{B}^I_<\times\mathcal{D}} a_{bd} f^{bd} & \\ \iff f(c) & = & \sum_{(b,d)\in\mathcal{B}^I_<\times\mathcal{D}} a_{bd} f^{bd}(c) & \text{for all } c \in \mathcal{B}^I_< \\ \iff f(c) & = & \sum_{d\in\mathcal{D}} a_{cd} d & \text{for all } c \in \mathcal{B}^I_< \end{array}$$

Since $\mathcal{D}$ is a R-basis for $\mathcal{B}$ we see that there exists uniquely determined a_{cd} fulfilling the last of these equations. □

Definition 6.1.12. *Let V and W be R-modules, $n \in \mathbb{N}$ and I a set. Then $\bigwedge_I(V) = \bigwedge_I(V, R)$, $\bigwedge_n(V, W) = \bigwedge_{\{1,2,\ldots,n\}}(V, W)$ and $\bigwedge_n(V) = \bigwedge_{\{1,2,\ldots,n\}}(V)$.*

Lemma 6.1.13. *Let V be a free R-module of finite rank n. Let $\alpha \in \mathrm{End}_R(V)$.*

(a) There exists a unique $r_\alpha \in R$ with

$$f\alpha = rf \text{ for all } f \in \textstyle\bigwedge_n(V)$$

(b) The map $\det : \mathrm{End}_R(V) \to R, \alpha \to r_\alpha$ is a multiplicative homomorphism, that is $\det(\alpha\beta) = \det(\alpha)\det(\beta)$ for all $\alpha, \beta \in \mathrm{End}_R(V)$.

(c) If A is the matrix of α with respect to some R-basis of V, then $\det(\alpha) = \det(A)$.

Proof. (a) Let $\mathcal{B} = \{b_1, b_2, \ldots b_n\}$ be basis for V. Order $\mathcal{B}$ by $b_1 < b_2 \ldots b_n$ and put $b = (b_1, b_2, \ldots b_n)$. Put $I = \{1, 2, 3 \ldots, n\}$ order in the usual way. Then clearly $\mathcal{B}^I_< = \{b\}$ and 1 is an R-basis for R. Thus by 6.1.11 f^{b1} is an R-basis for $\bigwedge_n(V)$. Hence

$$f^{b1}\alpha = r_\alpha f^{bl}$$

for a unique $r_\alpha \in R$. Also each $f \in \bigwedge_n(V)$ is of the form $f = rf^{b1}$ for some $r \in R$. Since α acts R-linearly on $\bigwedge_n(V)$ we conclude that (a) holds.

(b) Let $\alpha, \beta \in End_R(V)$ and $f \in \bigwedge_n(V)$. Then

$$f(\alpha\beta) = (f\alpha)\beta = (r_\alpha f)\beta = r_beta(r_\alpha f) = (r_\beta r_\alpha)f = (r_\alpha r_\beta)f$$

Hence $r_{\alpha\beta} = r_\alpha r_\beta$ and (b) holds.

(c) We will compute $\det(\alpha)$. We have

$$\det(\alpha) = r_\alpha = r_\alpha 1_R = r_\alpha f^{b1}(b) = (r_\alpha f^{b1})(b) = (f^{b1}\alpha)(b) = f^{b1}(\alpha(b)) = f^{b1}\big((\alpha(b_j)_{j\in I}\big)$$

Let $A = (a_{ij})$ be the matrix for α with respect to $\mathcal{B}$. Then $\alpha(b_j) = \sum_{i\in I} a_{ij}b_i$. So

$$\det(\alpha) = f^{b1}\left(\Big(\sum_{i\in I} a_{ij}b_i\Big)_{j\in J}\right)$$

Since f^{bl} is alternating we see the function $\tau : \mathrm{M}_I(R) \to R, A \to \det(\alpha)$ is alternating and R-multilinear in the columns of A. Also if $A = \mathrm{id}_n$, then $\alpha = id_V$, $\det(\mathrm{id}_V) = 1_R$ and so $\tau(I_n) = 1_R$. 6.1.9 shows that τ is uniquely determined and so $\tau = \det$, that is $\det(\alpha) = \det(A)$. □

Lemma 6.1.14. *Let V be an R-module and I a finite set. Then V^I is an $\mathrm{M}_I(R)$-module via*

$$Av = \Big(\sum_{i\in I} a_{ij}v_j\Big)_{i\in I}$$

for all $A = (a_{ij})_{(i,j)\in I\times I} \in \mathrm{M}_I(R)$ and $v = (v_j)_{j\in I} \in V^I$.

Proof. Let $A = (a_{ij})$, $B = (b_{jk})$ and $C := AB$. Then $C = (c_{ik})$ with $c_{ik} = \sum_{j\in I} a_{ij}b_{jk}$. Let $v = (v_k)_{k\in I} \in V^I$. Then

$$\begin{array}{rcl}
A(Bv) & = & A\Big(\sum_{k\in I} b_{jk}v_k\Big)_{j\in I} \\
& = & \Big(\sum_{j\in I} a_{ij}\big(\sum_{k\in I} b_{jk}v_k\big)\Big)_{i\in I} \\
& = & \Big(\sum_{k\in I}\big(\sum_{j\in I} a_{ij}b_{jk}\big)v_k\Big)_{i\in I} \\
& = & \Big(\sum_{k\in I} c_{ik}v_k\Big)_{i\in I} \\
& = & Cv = (AB)v
\end{array}$$

□

Definition 6.1.15. *Let $n \in \mathbb{N}$ and $A \in \mathrm{M}_n(R)$. Note that $xI_n - A \in \mathrm{M}_n(R[x])$ and $R[x]$ is a commutative ring. So we can define*

$$\chi_A := \det(xI_n - A) \in R[x]$$

χ_A is called the characteristic polynomial of A.

Theorem 6.1.16 (Cayley Hamilton)**.** *Let $n \in \mathbb{N}$ and $A \in \mathrm{M}_n(R)$. Then $\chi_A(A) = O_n$, where $O_n = 0_{\mathrm{M}_n(R)}$ is the $n \times n$-zero matrix over R.*

Proof. By **??** the maps $R[x] \to \mathrm{M}_n(R), f \to f(A)$ is a ring homomorphism. Note that (for example by 6.1.14) R^n is an $\mathrm{M}_n(R)$ module via $Bv = (\sum_{j=1}^n b_{ij}v_j)_{i=1}^n$ for all $B = (b_{ij}) \in \mathrm{M}_n(R)$ and all $v = (v_j)_{j=1}^n \in R^n$. Thus $V := R^n$ is also an $R[x]$ module via $fv = f(A)v$ for all $f \in R[x]$ and $v \in V$. Note that $xv = Av$ for all $v \in R^n$. Since V is an $R[x]$-module we conclude from 6.1.14 that V^n is a $\mathrm{M}_n([R[x])$-module. Put $e_k = (\delta_{kj})_{j=1}^n \in V$. Then

$$xe_k = Ae_k = \left(\sum_{j=1}^n a_{ij}\delta_{kj}\right)_{i=1}^n = (a_{ik})_{i=1}^n = \sum_{i=1}^n a_{ik}e_i$$

Let $D = xI_n - A^{\mathrm{T}} \in \mathrm{M}_n(R[x])$ and $e = (e_j)_{j=1}^n \in V^n$. Then $D = (d_{ij})$ with $d_{ij} = \delta_{ij}x - a_{ji}$. Hence

$$De = \left(\sum_{j=1}^n d_{ij}e_j\right)_{i=1}^n = \left(\sum_{j=1}^n(\delta_{ij}x - a_{ji})e_j\right)_{i=1}^n = \left(xe_i - \sum_{j=1}^n a_{ji}e_j\right)_{i=1}^n = (xe_i - xe_i)_{i=1}^n = 0_{V^n}$$

Hence also $D^{\mathrm{ad}}(De) = 0_{V^n}$ and so $(D^{\mathrm{ad}}D)e = 0_{V^n}$. By 6.1.8 $D^{\mathrm{ad}}D = \det(D)I_n$ we have $(D^{\mathrm{ad}}D)e = (\det(D)e_i))_{i=1}^n$. Hence $\det(D)e_i = 0_V$ for all $1 \leq i \leq n$. By Homework 6#10, $\det(D) = \det(D^{\mathrm{tr}}) = \chi_A$ and so $\chi_A e_i = 0$ for all $v \in V$. But $\chi_A e_i = \chi_A(A)e_i$ and so the i-column of $\chi_A(A)$ is zero. Thus $\chi_A(A) = 0_n$. □

Lemma 6.1.17. *Let V and W be $R[x]$-modules and $\pi : W \to W$ a function. Then π is $R[x]$-linear if and only if π is R-linear and $\pi(xv) = x\pi(v)$ for all $v \in V$.*

Proof. The forward direction is obvious. So suppose π is R-linear and $\pi(xv) = x\pi(v)$ for all $v \in V$. Let $S = \{f \in R[x] \mid \pi(fv) = f\pi(v) \text{ for all } v \in V\}$. We will show that S is a subring of $R[x]$. Indeed let $f, g \in S$ and $v \in V$. Then

$$\pi((f+g)v(= \pi(fv + gv) = \pi(fv) + \pi(gv) = f\pi(v) = g\pi(v) = (f+g)\pi(v)$$

and

$$\pi((fg)(v) = \pi(f(gv)) = f\pi(gv)f(g\pi(v)) = (fg)\pi(v))$$

So $f + g, fg \in V$. Similarly 0_R and $-f \in S$. So S is a subring of $R[x]$. Since π is R-linear, $R \subseteq S$ and by assumption $x \in S$. Thus $S = R[x]$ and π is $R[x]$-linear. □

Theorem 6.1.18. *Let M be a finitely generated R-module and $\alpha \in \mathrm{End}_R(M)$. Then there exists a monic polynomial $f \in R[x]$ with $f(\alpha) = 0_{\mathrm{End}_R(M)}$.*

Proof. Let I be a finite subset of M with $M = \langle I\rangle_R = RI$. Then for each $j \in I$ there exist $a_{ij} \in R$, $i \in I$ with $\alpha(j) = \sum_{i\in I} a_{ij}i$. (Note here that the a_{ij} are not necessarily unique.) View R^I as an $R[x]$-module via $fv = f(A)v$ and view M as an $R[x]$ module via $fm = f(\alpha)(m)$. Define $\pi : R^I \to M, (r_i)_{i\in I} \to \sum_{i\in I} r_i i$. Then π is onto and R-linear. Let $e_i = (\delta_{ij})_{j\in I}$. By definition of π and A

$$x\pi(e_j) = xj = \alpha(j)\sum_{i=1}^n a_{ij}i$$

and

$$\pi(xe_j) = \pi(Ae_j) = \pi((a_{ij})_{i\in I}) = \sum_{i\in I} a_{ij}i$$

Thus $x\pi(e_j) = \pi(xe_j)$.. Since x acts R-linearly on R^I and M this implies $x\pi(v) = pi(xv)$ for all $v \in R^n$. Thus by 6.1.17, π is $R[x]$ linear. Put $f = \chi_A$. Then f is monic, $f \in R[x]$, $f(A) = 0$ and so for all $v \in R^n$,

$$f(\alpha)(\pi(v)) = f\pi(v) = \pi(f(v)) = \pi(f(A)v) = \pi(0v) = \pi(0) = 0.$$

Since π is onto we conclude that $f(\alpha) = 0$. □

6.2 Ring Extensions

Definition 6.2.1. *Let R and S be rings with $R \leq S$ and $1_S = 1_R$. Then S is called a* ring extension *of R. Such a ring extension is denoted by $R \leq S$.*

Definition 6.2.2. *Let $R \leq S$ be a ring extension.*

(a) Let $s \in S$. s is called integral *over R if $f(s) = 0$ for some monic polynomial $f \in R[x]$.*

(b) $R \leq S$ is called integral *if all $s \in S$ are integral over R.*

(c) $R \leq S$ is called finite if S is finitely generated as an R-module (by left multiplication)

Example 6.2.3. (1) Suppose $R \leq S$ is a ring extension with R a field and S an integral domain. Let $s \in S$. Then s is integral over R if and only if s is algebraic over R. $R \leq S$ is integral if and only if its algebraic. Note that then by 4.1.14 S is a field. $R \leq S$ is a finite ring extension if and only if its a finite field extension.

(2) Let $R = \mathbb{Z}$ and $S = \mathbb{C}$. Then $\sqrt{2}$ is integral over $\mathbb{Z}$. $\frac{1}{2}$ is not integral over $\mathbb{Z}$. Indeed suppose that $\frac{1}{2}$ is integral over $\mathbb{Z}$. Then there exists $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ with

$$a_0 + a_1\frac{1}{2} + a_2\frac{1}{4} + \ldots a_{n-1}\frac{1}{2}^n + \frac{1}{2^n} = 0$$

Multiplication with 2^n shows that

$$1 = -(a_0 2^n + a_1 2^{n-1} + \ldots + a_{n-1}2)$$

since the left hand side of this equation is even, we derived a contradiction.

Theorem 6.2.4. *Let $R \leq S$ be a ring extension and $s \in S$. Then the following statements are equivalent:*

(a) s is integral over R.

(b) $R \leq R[s]$ is finite.

(c) There exists a subring T of S containing $R[s]$ such that $R \leq T$ is finite.

(d) There exists a faithful $R[s]$- module M, which is finitely generated as an R-module.

Proof. (a) $\Longrightarrow$ (b): Suppose $f(s) = 0$ for a monic $f \in R[x]$. Let $J = \{g \in R[x] \mid g(s) = 0\}$. Then $R[s] \cong R[x]/J$ and $R[x]f \leq J$.

We claim that $R[x]/R[x]f$ is finitely generated as an R-module. Indeed let $g \in R[x]$. Since f is monic we can apply the division algorithm and so $g = qf + r$, where $q, r \in R[x]$ with $\deg q < \deg f$. Let $n = \deg f$. We conclude that $g + R[x]$ is in the R span of $(x^i + R[x]f)_{i=0}^{n-1}$.

This proves the claim. Since $R[x]/J$ is isomorphic to a quotient of $R[x]/R[x]f$, also $R[X]/J$ and $R[s]$ are finitely generated as an R-module.

(b) $\Longrightarrow$ (c): Just choose $T = R[s]$.

(c) $\Longrightarrow$ (d): Put $B = T$. Since $1 \in T$, $aT \neq 0$ for all $0 \neq a \in R[s]$. Thus T is a faithful $R[s]$ module.

(d) $\Longrightarrow$ (a): By 6.1.18 there exists a monic $f \in R[x]$ with $f(s)M = 0$. Since M is faithful for $R[s]$, $f(s) = 0$. □

Corollary 6.2.5. *Let $R \leq S$ be a finite ring extension. Then $R \leq S$ is integral.*

Proof. This follows immediately from 6.2.4(c) applied with $T = S$. □

Lemma 6.2.6. *Let $R \leq E$ and $E \leq S$ be finite ring extensions. Then $R \leq S$ is a finite ring extension.*

Proof. Let I be a finite subset of E with $RI = E$ and J a finite subset of S with $S = EJ$. Then by 4.1.5(aa) $S = R\{ij \mid i \in I, J\}$. So also $R \leq S$ is finite □

Proposition 6.2.7. *Let $R \leq S$ be a ring extension and $I \subseteq S$ such that each $b \in I$ is integral over R.*

(a) If I is finite, $R \leq R[I]$ is finite and integral.

(b) $R \leq R[I]$ is integral.

(c) The set $Int(R, S)$ of the elements in S which are integral over R is a subring S. Moreover, $R \leq Int(R, S)$ is integral.

Proof. (a) By induction on $|I|$. If $|I| = 0$ there is nothing to prove. So suppose there exists $i \in I$ and let $J = I \setminus \{i\}$. Put $E = R[J]$. By induction $R \leq E$ is finite. Since i is integral over R, f is integral over E. Thus by 6.2.4(b), $E \leq E[i]$ is finite. Note that $E[i] = R[J][i] = R[I]$ and so (a) follows from 6.2.6.

(b) By 4.1.4(b) $R[I] = \bigcup\{R[J] \mid J \subseteq I, |J| < \infty\}$. By (a) each of the extensions $R \leq R[J]$ are integral. So(b) holds.

(c) Follows from (b) applied to $I = \mathrm{Int}(T, S)$. □

Definition 6.2.8. *Let $R \leq S$ be a ring extension and let $Int(R,S)$ the set of elements in S which are integral over R. Then $Int(R,S)$ is ca called to* integral closure *of R in S. If $R = Int(R,S)$, then R is called T*integrally closed *in S.*

If R is an integral domain and R is integrally closed in $\mathbb{F}_R$ (the field of fraction of R), then R is called integrally closed.

Example 6.2.9. Let $A = \text{Int}(\mathbb{Z},\mathbb{C})$. Then A is the set of complex numbers which are the roots of an integral monic polynomial. So A is the set of algebraic integers (see Homework 2#6). We now know from 6.2.7 that A is a subring of $\mathbb{C}$, which generalized Homework 2#6(c). By Homework 2#6(b), $A \cap \mathbb{Q} = \mathbb{Z}$. Thus $\text{Int}(\mathbb{Z},\mathbb{Q}) = \mathbb{Z}$ and so $\mathbb{Z}$ is integrally closed. But $\mathbb{Z}$ is not integrally closed in $\mathbb{C}$ since $\sqrt{2} \in A$.

Lemma 6.2.10. *Let $R \leq E$ and $E \leq S$ be integral ring extensions. Then $R \leq S$ is integral.*

Proof. Let $s \in S$ and let $f \in E[x]$ be the monic with $f(s) = 0$. Let I be the set of non-zero coefficients f. Then I is a finite subset of E and so by 6.2.7(a), $R \leq R[I]$ is finite. Since $f \in R[I][x]$, 6.2.4 implies that $R[I] \leq R[I][s]$ is finite. So by 6.2.6, $R \leq R[I][s]$ is finite. So by 6.2.4, s is integral over R. □

6.3 Ideals in Integral Extensions

Definition 6.3.1. *Let R be ring and I an ideal in R. Then*

$$\text{rad}\, I = \text{rad}_R I = \{r \in R \mid r^n \in I \textit{ for some } n \in \mathbb{Z}^+\}.$$

$\text{rad}_R I$ *is called the* radical *of I in R . If $I = \text{rad}_R I$, I is called a radical ideal in R.*

Lemma 6.3.2. *Let R be a ring and P an ideal in R.*

(a) rad$P$ *is an ideal in R and $P \leq \text{rad}P$.*

(b) rad$P$ *is a radical ideal.*

(c) All primes ideals in R are radical ideals.

Proof. (a) Note that $r \in \text{rad}P$ if and only if $r + P$ is nilpotent in R/P. By Homework 6#5 in MTH 818, the nilpotent elements of R/P form an ideal in R/P. So (a) holds.

(b) Homework 6#5 in MTH 818 $R/\text{rad}\, R\big/\text{rad}\, R/P$ has no non-zero nilpotent elements.

(c) If P is a prime ideal, then R/P has no zero divisors and so also no non-zero nilpotent elements. □

Lemma 6.3.3. *Let $R \leq S$ be an integral ring extension.*

(a) Let P be an ideal in R and $p \in P$.

(a) $Sp \cap R \subseteq \text{rad}_R P$.

(b) If P is a prime ideal or a radical ideal in R, then $Sp \cap R \subseteq P$.

(b) Suppose S is an integral domain

(a) Let $0 \neq b \in S$, then $Sb \cap R \neq 0$.

(b) Let Q be a non-zero ideal in S, then $Q \cap R \neq 0$.

Proof. (a) Let $s \in S$ such that $r := sp \in R$. Since $R \leq S$ is integral there exists $r_0, r_1 \ldots r_{n-1} \in R$ with

$$s^n = r_{n-1}s^{n-1} + \ldots + r_1 s + r_0$$

Multiplying this equation with p^n we obtain:

$$(sp)^n = (r_{n-1}p)(sp)^{n-1} + \ldots + r_1 p^{n-1}(sp) + r_0 p^n$$

Hence

$$r^n = (r_{n-1}p)r^{n-1} + \ldots + (r_1 p^{n-1})r + r_0 p^n$$

As P is an ideal and $r_i r^i \in R$ we have $r_i r^i p^{n-i} \in P$ for all $0 \leq i < n$. So the right side of the last equation lies in P. Thus $r^n \in P$ and $r \in \text{rad}P$.

(a:b) In both cases 6.3.2 implies that $P = \text{rad}_R P$. So (a:b) follows from(a:a).

(b:a) Let $f \in R[x]$ be a monic polynomial of minimal degree with $f(b) = 0$. Let $f = xg + r$ where $r \in R$ and $g \in R[x]$ is monic of degree one less than f. Then

$$0 = f(b) = bg(b) + r$$

and so $r = -g(b)b$

If $r = 0$, we get $g(b)b = 0$. Since $b \neq 0$ and S is an integral domain, $g(b) = 0$. But this contradicts the minimal choice of $\deg f$.

Hence $0 \neq r = -g(b)b \in R \cap Sb$.

(b:b) Let $0 \neq b \in Q$. Then by (b:a) $\{0\} \neq R \cap Sb \subseteq R \cap Q$. □

Theorem 6.3.4. *Let $R \leq S$ be an integral extension and P a prime ideal in R. Put*

$$\mathcal{M} := \{I \mid I \textit{ is an ideal in } R, R \cap I \subseteq P\}$$

Order $\mathcal{M}$ by inclusion. Let $Q \in \mathcal{M}$.

(a) Q is contained in a maximal member of $\mathcal{M}$

(b) The following are equivalent:

(a) Q is maximal in $\mathcal{M}$.

(b) Q is a prime ideal and $R \cap Q = P$.

Proof. Put $\mathcal{M}_Q := \{I \in \mathcal{M} \mid Q \leq I\}$. Then a maximal element of $\mathcal{M}_Q$ is also a maximal element of $\mathcal{M}$.

(a) Since $Q \in \mathcal{M}_Q$, $\mathcal{M}_Q \neq \varnothing$. So by Zorn's Lemma A.3.8 it remains to show that every non-empty chain $\mathcal{D}$ in $\mathcal{M}_Q$ has an upper bound in $\mathcal{M}_Q$. Put $D = \bigcup \mathcal{D}$. By 2.5.21(a) D is an ideal in S. Let $E \in \mathcal{D}$. Then $Q \leq E \leq D$. Moreover,

$$R \cap D = \bigcup_{E \in \mathcal{D}} R \cap E \subseteq P$$

Thus $D \in \mathcal{M}_Q$ and D is an upper bound for $\mathcal{D}$.

(b) For $E \subseteq S$ put $\overline{E} = E + Q/Q \subseteq S/Q$. Since S is integral over R, $\overline{S}$ is integral over $\overline{R}$. (Indeed let $\overline{s} \in \overline{S}$. Then $\overline{s} = s + Q$ for some $s \in S$ and there exists a monic polynomial $f \in R[x]$ with $f(s) = 0$. The $\overline{f}$ is a monic polynomial in $\overline{S}[x]$ and $\overline{f}(\overline{s}) = 0$.

$$\begin{array}{rcccccc} \overline{R}/\overline{P} & = & R + Q/Q\big/P + Q/Q & \cong & R + Q/P + Q & = & R + (P + Q)/P + Q \\ & \cong & R/R \cap (P + Q) & = & R/P + (R \cap Q) & = & R/P \end{array}$$

Since P is a prime ideal in R we conclude that $\overline{P}$ is a prime ideal in $\overline{R}$. Let I be an ideal in S with $Q \leq I$. We have

$$\begin{array}{rc} & \overline{R} \cap \overline{I} \leq \overline{P} \\ \Longleftrightarrow & ((R + Q)/Q) \cap I/Q \leq P + Q/Q \\ \Longleftrightarrow & (R + Q) \cap I \leq P + Q \\ \Longleftrightarrow & Q + (R \cap I) \leq P + Q \end{array}$$

If $R \cap I \leq P$ we have $Q + (R \cap I) \leq P + Q$. If $Q + (R \cap I) \leq P + Q$, then $R \cap I \leq (P + Q) \cap R = P + (Q \cap R) \leq P$. So

$$\overline{R} \cap \overline{I} \leq \overline{P} \Longleftrightarrow R \cap I \leq I$$

Therefore $\{\overline{I} \mid I \in \mathcal{M}_Q\} = \{J \leq \overline{S} \mid J \text{ is an ideal in } \overline{S}, \overline{R} \cap J \subseteq \overline{P}\}$.

If follows that (b) holds if and only if (b) holds for $(\overline{S}, \overline{R}, \mathrm{P}, \overline{Q}$ in place of (S, R, P, Q). Since $\overline{Q} = 0$ we thus may assume that $Q = 0$.

(b:a) $\Longrightarrow$ (b:b): Suppose that Q is not a prime ideal. As $Q = 0$, this means S is not an integral domain. Hence there exists $b_1, b_2 \in S^\sharp$ with $b_1 b_2 = 0$. Since $Q = 0$ is maximal in $\mathcal{M}$, $Sb_i \notin \mathcal{M}$ and so $R \cap Sb_i \nleq P$. Hence there exist $s_i \in S$ with $0 \neq r_i := s_i b_i \in R \setminus P$. But then $r_1 r_2 = (s_1 b_1)(s_2 b_2) = (s_1 s_2)(b_1 b_2) = 0 \in P$. But this contradicts the fact that P is a prime ideal in R.

So Q is a prime ideal. Suppose that $P \neq R \cap Q$, that is $P \neq 0$. Let $0 \neq p \in P$. Then by 6.3.3(a) , $Sp \cap R \leq P$. Hence $Sp \in \mathcal{M}$, contradiction the maximality of $Q = 0$. So (b:a) implies (b:b).

(b:b) $\Longrightarrow$ (b:a): Suppose now that Q is a prime ideal and $P = R \cap Q$. Since $Q = 0$ this means that S is an integral domain and $P = 0$. Let I be any non-zero ideal in S. Then by 6.3.3(b:b) $R \cap I \neq 0$ and so $R \cap I \nleq P$ and $I \notin \mathcal{M}$. Thus $\mathcal{M} = \{0\}$ and Q is maximal. □

Corollary 6.3.5. *Let $R \leq S$ be an integral extension.*

(a) Let P be a prime ideal in R and Q an ideal in S with $R \cap Q \leq P$. Then there exists a prime ideal M in S with $R \cap M = P$ and $Q \leq M$.

(b) Let P be a prime ideal in R. Then there exists a prime ideal M in S with $R \cap M = P$.

(c) Let Q_1 and Q_2 be prime ideals in S with $R \cap Q_1 = R \cap Q_2$ and $Q_1 \leq Q_2$. Then $Q_1 = Q_2$.

(d) Let Q be a maximal ideal in S. Then $Q \cap R$ is a maximal ideal in R.

(e) Let P be a maximal ideal in S. Then there exists a maximal ideal M of S with $R \cap M = P$.

Proof. (a) We apply 6.3.4. Let $\mathcal{M}$ be defined as there. By part (a) there exists a maximal element M of $\mathcal{M}$ containing Q. By part (b) M is a prime ideal and $R \cap M = P$.

(b) follows from (a) applied with $Q = 0$.

(c) By 6.3.4, applied with $P = R \cap Q_1$ and $Q = Q_1$ we get that Q_1 is maximal in $\mathcal{M}$. As $Q_2 \in \mathcal{M}$ and $Q_1 \leq Q_2$, $Q_1 = Q_2$.

(d) Since $1 \notin Q$, $R \cap Q \neq R$. So by 2.4.18, $Q \cap R$ is contained in a maximal ideal P of R. By (a) there exists an ideal M in S with $P = R \cap M$ and $Q \leq M$. Since Q is maximal, $M = Q$. Thus $R \cap Q = R \cap M = P$ and so $R \cap Q$ is a maximal ideal in R.

(e) By 2.4.19, P is a prime ideal in R. So by (b) there exists an ideal Q of S with $R \cap Q = P$. Let M be a maximal ideal in S with $Q \leq M$. Then $P = R \cap Q \leq R \cap M < R$ and since P is a maximal ideal in R, $P = R \cap M$. □

6.4 Noether's Normalization Lemma

Definition 6.4.1. *Let $\mathbb{K}$ be a field. A $\mathbb{K}$-algebra is a ring R with $\mathbb{K}$ as a subring. A $\mathbb{K}$-algebra R is called finitely generated if $R = \mathbb{K}[I]$ for some finite subset I of K*

Theorem 6.4.2. *Let $\mathbb{K}$ be a field and R a $\mathbb{K}$-algebra. Suppose that there exists a finite subset I of R such that $\mathbb{K}[I] \leq R$ is integral. Then there exists a finite subset J of R such that J is algebraically independent over $\mathbb{K}$ and $\mathbb{K}[J] \leq R$ is integral.*

Proof. Choose a finite subset I of R of minimal size such that$\mathbb{K}[I] \leq R$ is integral. Suppose that $u =: (i)_{i \in i}$ is not algebraic independent over $\mathbb{K}$ and pick $0 \neq f \in \mathbb{K}[x_i, i \in I]$ with $f(u) = 0$. Put $J = \bigoplus_{j \in J} \mathbb{N}$. Then $f = \sum_{\alpha \in J} k_\alpha x^\alpha$, where $k_\alpha \in \mathbb{K}$, almost all 0. Put $J^* = \{\alpha \in \mathbb{I} \mid k_\alpha \neq 0\}$. Then

$$(1) \qquad \sum_{\beta \in J^*} k_\beta u^\beta = 0$$

where $u^\beta = \prod_{i \in I} i^{\beta_i}$. Since J^* is finite, we can pick $c \in \mathbb{Z}^+$ with $\alpha_i < c$ for all $\alpha \in \mathbb{J}^*$ and $i \in I$. Fix $l \in I$ and let $(t_i) \in \mathbb{N}^I$ be a 1-1 function with $t_l = 0$. Define

$$\rho : \mathbb{J}^* \to \mathbb{Z}^+, \quad \alpha \to \sum_{i \in I} c^{t_i} \alpha_i$$

We claim that ρ is one to one. Indeed suppose that $\rho(\alpha) = \rho(\beta)$ for $\alpha \neq \beta \in \mathbb{J}^*$. Let $I^* = \{i \in I \mid \alpha_i \neq \beta_i$ and $k \in I^*$ with t_k is minimal.

$$0 = \rho(\alpha) - \rho(\beta) = c^{t_k}\left(\alpha_k - \beta_k + \sum_{i \in I^* \setminus \{k\}} c^{t_i - t_k}(\alpha_i - \beta_i)\right)$$

Since t is 1-1, $t_k < t_j$ for all $i \in I^* \setminus \{k\}$. So we conclude that c divides $\alpha_k - \beta_k$, a contradiction to $c > \alpha_j$ and $c > \beta_j$.

Since ρ is 1-1, we can choose $\alpha \in J^*$ with $\rho(\alpha) < \rho(\beta)$ for all $\beta \in J^* \setminus \{\alpha\}$.

For $i \in I$ define $v_i = i - l^{c^{t_i}}$. Put $S := \mathbb{K}[v_i, i \in I]$. Note that $v_l = l - l^{c^{t_l}} = l - l^{c^0} = l - l^1 = 0$. So

$$S = \mathbb{K}[V_i, \in I \setminus \{l\}] \tag{2}$$

We will show that l is integral over S. Let $\beta \in J^*$. Since $i = l^{c^{t_i}} + v_i$ we have

$$u^\beta = \prod_{i \in I} i^{\beta_i} = \prod_{i \in I} (l^{c^{t_i}} + v_i)^{\beta_i}.$$

Thus $u^\beta = g_\beta(l)$ where $g_\beta \in S[x]$ is a monic of degree $\rho(\beta)$. Put

$$g := \sum_{\beta \in J^*} k_\beta g_\beta \in S[x].$$

Then maximality of $\rho(\alpha)$ shows that g has degree $\rho(\alpha)$ and leading coefficient k_α. Moreover,

$$g(l) = \sum_{\beta \in J^*} k_\beta g_\beta(l) = \sum_{\beta \in J^*} k_\beta u^\beta = 0.$$

Thus $k_\alpha{-}1g$ is a monic polynomial over S with l as a root and so l is integral over S. Note that $i = v_i + l^{c^t_i} \in S[l]$ and thus $\mathbb{K}[I] \leq S[l] \leq \mathbb{K}[I]$. So $\mathbb{K}[I] = S[l]$ and $S \leq \mathbb{K}[l]$ is integral. Since also $\mathbb{K}[I] \leq R$ is integral we conclude from 6.2.10 that $S \leq R$ is integral. But this contradicts (2) and the minimal choice of $|J|$. □

Proposition 6.4.3. *Let $R \leq S$ be an integral extension and suppose that that R and S are integral domains. Then S is a field if and only if R is a field.*

Proof. Suppose first that R is a field. Then $R \leq S$ is algebraic and so by 4.1.14(c) , S is a field.

Suppose next that S is a field and let $r \in R^\sharp$. Since S is a field, $1 \in S r \cap R$. Hence by 6.3.3(a:b) applied with $P = Rr$, $1^n \in Rr$ for some $n \in \mathbb{Z}^+$. Thus $1 = tr$ for some $t \in T$. Hence r is invertible in R, and R is a field. □

Proposition 6.4.4. *(a) Let $\mathbb{K} \leq \mathbb{F}$ be a field extensions such that $\mathbb{F}$ is finitely generated over $\mathbb{K}$ as a ring. Then $\mathbb{K} \leq \mathbb{F}$ is finite. In particular, if $\mathbb{K}$ is algebraically closed then $\mathbb{F} = \mathbb{K}$.*

(b) Let $\mathbb{K}$ be an algebraically closed field, A a finitely generated $\mathbb{K}$-algebra and M a maximal ideal in A. Then $A = \mathbb{K} + M$.

Proof. (a) By 6.4.2 there exists a finite subset J of $\mathbb{K}$ such that $\mathbb{K}[J] \leq \mathbb{F}$ is integral and J is algebraically independent over $\mathbb{K}$. By 6.4.3, $\mathbb{K}[J]$ is a field. Since the units in $\mathbb{K}[J]$ are $\mathbb{K}$ we get $J = \varnothing$. Hence $\mathbb{K} \leq \mathbb{F}$ is integral and so algebraic. Thus by 4.1.14 $\mathbb{K} \leq \mathbb{F}$ is finite.

(b) Note that $\overline{A} := A/M$ is a field. Also $\overline{\mathbb{K}} = (\mathbb{K} + M)/M$ is a subfield of $\overline{A}$ isomorphic to $\mathbb{K}$ and $\overline{A}$ is a finitely generated $\overline{\mathbb{K}}$ algebra. So by (a) $\overline{A} = \overline{\mathbb{K}}$ and thus $A = \mathbb{K} + M$. □

6.5 Affine Varieties

Hypothesis 6.5.1. *Throughout this section $\mathbb{K} \leq \mathbb{F}$ is field extension with $\mathbb{F}$ algebraically closed. D is a finite set, $A = \mathbb{K}[x_d, d \in D]$ and $B = \mathbb{F}[x_d, d \in D]$, with A viewed as a subset of B.*

Definition 6.5.2. *Let $S \subseteq A$ and $U \subseteq \mathbb{F}^D$.*

(a) $V(S) = V_{\mathbb{F}^D}(S) = \{v \in \mathbb{F}^D \mid f(v) = 0$ *for all* $f \in S\}$.

$V(S)$ *is called an* affine variety *in* $\mathbb{F}^D$ *defined over* $\mathbb{K}$, *or a* $\mathbb{K}$*-variety in* $\mathbb{F}^D$.

(b) $U \subseteq \mathbb{F}^D$ *define* $J(U) := J_A(U) = \{f \in A \mid f(u) = 0$ *for all* $u \in U\}$.

(c) U *is called* closed *if* $U = V(J(U))$ *and* S *is called closed if* $S = J(V(S))$.

Lemma 6.5.3. *Let $U \subseteq \tilde{U} \subseteq \mathbb{F}^D$ and $S \subseteq \tilde{S} \subseteq A$.*

(a) $J(U)$ *is an ideal in* R.

(b) $J(\tilde{U}) \subseteq J(U)$.

(c) $V(\tilde{S}) \subseteq V(S)$.

(d) $U \subseteq V(J(U))$.

(e) $S \subseteq J(V(S))$.

(f) The following are equivalent:

- *(a)* U *is* $\mathbb{K}$*-variety in* $\mathbb{F}^D$.
- *(b)* $U = V(S)$ *for some* $S \subseteq A$.
- *(c)* U *is closed.*
- *(d)* $U = V(I))$ *for some ideal* I *of* A.

(g) S *is closed if and only if* $S = J(U)$ *for some* $U \subseteq F^D$.

(h) $V(S) = V(AS)$.

Proof. (a) Clearly $0 \in J(U)$. Let $f, g \in J(U)$, $h \in A$ and $u \in U$. Then $(f - g)(u) = f(g) - g(u) = 0$ and $(hf)(u) = h(u)f(u) = 0$. So $f - g \in J(U)$ and $hf \in J(U)$.

(b) and and (c) are obvious.

(d) Let $u \in U$. Then for all $f \in J(U)$, $f(u) = 0$. So (d) holds.

(e) Similar to (d).

(f) Suppose U is $\mathbb{K}$-variety in $\mathbb{F}^D$, then by definition $U = V(S)$ for some $S \subseteq A$. So (f:a) implies (f:b)

Suppose $U = V(S)$ for some $S \subseteq A$. Then by (d) $S \subseteq J(U)$ and so by (b) $V(J(U)) \subseteq J(S) = U$. By (d), $U \leq (J(U))$ and hence $U = V(J(U))$. So (f:b) implies (f:c)

Suppose U is closed. Then $U = U(J(U))$. By (a) $J(U)$ is an ideal in A and so (f:c) implies (f:d).

Clearly (f:d) implies (f:a). So (f) holds.

(g) If S is closed then $S = J(U)$ for $U = J(S)$. The other direction is similar to the implication (f:b) $\Longrightarrow$ (f:c).

(h) Since $S \subseteq AS$, $V_(AS) \leq V(S)$. By (e) $S \subseteq J(V(S))$ and by (a), $J(V(S))$ is an ideal. Thus $AS \subseteq J(V(S))$ and so $V(S) \subseteq V(AS)$. □

Example 6.5.4. (1) Suppose that $|D| = 1$ and so $A = \mathbb{K}[x]$ and $\mathbb{F}^D = \mathbb{F}$. Let U be a affine $\mathbb{K}$-variety in $\mathbb{F}$. Then by 6.5.3(f), $U = V(I)$ for some ideal I in $\mathbb{K}[x]$. By 2.6.6, $\mathbb{K}[x]$ is a PID and so there exists $f \in \mathbb{K}[x]$ with $I = \mathbb{K}[x]f$. Thus by 6.5.3(h), $U = V(I) = V(f)$. So U is the set of roots of f in $\mathbb{F}$. So either $f = 0$ and $U = \mathbb{F}$ or U is finite.

Now let U be any finite subsets of $\mathbb{K}$ and put $f = \prod_{u \in U} x - u$. Then $V(f) = U$ and so any finite subsets of $\mathbb{K}$ are is an affine $\mathbb{K}$-variety in $\mathbb{F}$.

If $\mathbb{K} = \mathbb{F}$ we see the affine $\mathbb{F}$-varieties in $\mathbb{F}$ are $\mathbb{F}$ itself and the finite subsets of $\mathbb{F}$.

(2) Let $\mathbb{K} = \mathbb{R}$, $\mathbb{F} = \mathbb{C}$ and $D = \{1, 2\}$. Then $A = \mathbb{K}[x_1, x_2]$. Let $f = x_1^2 + x_2^1 - 1$. Then $V(f) = \{(a, b) \in \mathbb{C}^2 \mid a^2 + b^2 = 1\}$.

(3) Let $n \in \mathbb{Z}^+$ and $D = \{(i, j) \mid 1 \leq i, j \leq n\}$. Then $\mathbb{F}^D = M_n(\mathbb{F})$ is the set of $n \times n$-matrices with coefficients in $\mathbb{F}$. Write x_{ij} for $x_{(i,j)} \in A$ and consider the matrix $X := (x_{ij}) \in M_n(A)$. Put $f = \det(X) \in A$. Let $u = (u_{ij}) \in \mathbb{F}^D = M_n(\mathbb{F})$. Then $f(u) = \det u$. Thus

$$V(f - 1) = \{u \in M_n(\mathbb{F}) \mid \det(u) = 1\} = \mathrm{SL}_n(\mathbb{K})$$

Lemma 6.5.5. *Let $u \in \mathbb{F}^D$.*

(a) $J(u)$ is the kernel of the evaluation map: $\Phi : A \to \mathbb{F}, f \to f(u)$.

(b) If $\mathbb{K} \leq \mathbb{F}$ is algebraic, $J(u)$ is a maximal ideal in A.

Proof. (a) is obvious. (b) Note that $\mathbb{K} \leq \Phi(\mathbb{K}) \leq \mathbb{F}$. Therefore $\Phi(\mathbb{K})$ is an integral domain which is algebraic over $\mathbb{K}$. So by 4.1.14 $\Phi(\mathbb{K})$ is an field. By (a) and the first isomorphism theorem for rings, $A/J(u)$ is a field and so by 2.4.22 $J(u)$ is a maximal ideal in A. □

Lemma 6.5.6. *Let M be a maximal ideal in B.*

(a) There exists $u = (u_d)_{d \in D} \in \mathbb{F}^D$ with $M = J_B(u)$.

(b) M is the ideal in B generated by $\{x_d - u_d \mid d \in D\}$.

(c) $V(M) = \{u\}$.

Proof. (a) and (b) By 6.4.4, $B = \mathbb{F} + M$. Hence for each $d \in D$ there exists $u_d \in \mathbb{F}$ with $x_d - u_d \in M$. Put $u = (u_d)_{d \in D}$ and let I be the ideal generated by $\{x_d - u_d \mid d \in D)$. Then $x_d \in \mathbb{F} + I$ and so $\mathbb{F} + I$ is a subring of B containing $\mathbb{F}$ and all x_d. Hence $B = \mathbb{F} + I$ and B/I is a field. So I is a maximal ideal. Since $I \leq M$ we get $I = M$ and since $I \leq J_B(u)$, $I = J_B(u)$. So $M = I = J_B(u)$.

(c) Let $a \in V(M)$. Since $x_d - u_d \in M$, $0 = (x_d - u_d)(a) = a_d - u_d$. Hence $a_d = u_d$ and $a = d$. □

Proposition 6.5.7. *Let I be an ideal in A with $I \neq A$. Then $V(I) \neq \varnothing$*

Proof. By 2.4.18 I is contained in a maximal ideal P of A. Let $\mathbb{A}$ be the set of elements in $\mathbb{F}$ algebraic over $\mathbb{K}$. Then

$$V_{\mathbb{A}^D}(P) \subseteq V(P) \subseteq V(I),$$

and so we may assume that $\mathbb{F} = \mathbb{A}$ and I is maximal in A. Then $\mathbb{K} \leq \mathbb{F}$ is algebraic and so each $b \in \mathbb{F} \subseteq B$ is integral over $\mathbb{K}$ and so also over A. Since $B = A[\mathbb{F}]$ we conclude from 6.2.7 that $A \leq B$ is integral. Hence by 6.3.5, there exists a maximal ideal M of B with $I = A \cap M$. By 6.5.6, $V(M) \neq \varnothing$. Since $V(M) \subseteq V(I)$ the proposition is proved. □

Theorem 6.5.8 (Hilberts' Nullstellensatz). *Let I be an ideal in A. Then $J(V(I)) = \text{rad}I$. In other words, I is closed if and only if I is a radical ideal.*

Proof. Let $f \in \text{rad}I$ and $u \in V(I)$. Then $f^n \in I$ for some $n \in \mathbb{Z}$. Thus $(f(u))^n = f^n(u) = 0$ and since $\mathbb{F}$ is an integral domain, $f(u) = 0$. Thus $f \in J(V(I))$ and $\text{rad}I \subseteq J(V(I))$.

Next let $0 \neq f \in J(V(I))$. We need to show that $f \in \text{rad}I$. Put $E = D \cup \{f\}$ and put $y = x_f$. Then $\mathbb{K}[x_e, e \in E] = A[y]$. Let L be the ideal in $A[y]$ generated by I and $yf - 1$.

Suppose for a contradiction that $V_{\mathbb{F}^E}(L) = \varnothing$ and pick $c \in V_{\mathbb{F}^E}(L)$. Then $c = (a, b)$ with $a \in \mathbb{F}^D$ and $b \in \mathbb{F}$. Let $g \in I$. Then $g \in L$ and $0 = g(a, b) = g(a)$. Thus $a \in V(I)$. Since $f \in J(V(I))$ we get $f(a) = 0$. Hence $0 = (yf - 1)(a, b) = bf(a) - 1 = -1 \neq 0$, a contradiction.

Thus $V_{\mathbb{F}^E}(L) = \varnothing$. 6.5.7 implies $L = A[y]$. So there exist $g_s(y) \in A[y], 0 \leq s \leq m$ and $f_s \in I, 1 \leq s \leq m$, with

$$(*) \qquad 1 = g_0(y)(yf - 1) + \sum_{s=1}^{m} g_i(y) f_i.$$

Let $\mathbb{F}_A = \mathbb{K}(x_d, d \in D)$ be the field of fractions of A. Let $\phi : A[y] \to \mathbb{F}_A$ be the unique ring homomorphism with $\phi(a) = a$ for all $a \in A$ and $\phi(y) = f^{-1}$. (see **??**. Applying ϕ to (*) we obtain:

$$(**) \qquad 1 = g_0(f^{-1})(f^{-1}f - 1) + \sum_{s=1}^{m} g_i(f^{-1}) f_i = \sum_{s=1}^{m} g_i(f^{-1}) f_i.$$

Let $k \in \mathbb{Z}^+$ with $k \geq \deg_y g_i(y)$ for all $1 \leq i \leq m$. Then $g_i(f^{-1})f^k \in A$ for all i and thus $g_i(f^{-1})f^k f_i \in AI = I$. So multiplying equation (**) with f^k we get $f^k \in I$ and $f \in \operatorname{rad} I$. □

Corollary 6.5.9. *Then map $U \to J(U)$ is a inclusion reversing bijection with inverse $I \to V(I)$ between the affine $\mathbb{K}$-varieties in $\mathbb{F}^D$ and the radical ideals in A.*

Proof. Let U be an affine $\mathbb{K}$-variety in $\mathbb{F}^D$. Then by definition, $U = V(S)$ for some ideal S if A. So by 6.5.3(f)(g), U and $I := J(U)$ are closed. Thus $V(J(U)) = U$ and by Hilbert's Nullstellensatz, $I = J(V(I)) = \operatorname{rad} I$. So I is a radical ideal.

Suppose next that I is a radical ideal in A. Then by definition $V(I)$ is a affine $\mathbb{K}$-variety in $\mathbb{F}^D$ and by Hilbert's Nullstellensatz, $I = \operatorname{rad} I = J(V(I))$.

Finally by 6.5.3(b), $U \to J(U)$ is inclusion reversing. □

We would like to show that every affine variety is of the form $V(S)$ for a finite subset S of A. For this we need a little excursion:

Definition 6.5.10. *A ring R is called* Noetherian *if every ideal in R is finitely generated as an ideal.*

Theorem 6.5.11 (Hilbert's Basis Theorem)**.** *Let R be a Noetherian ring. Then also $R[x_d, d \in D]$ is Noetherian.*

Proof. By induction on $|D|$ it suffices to show that $R[x]$ is Noetherian.

Let J be an ideal in $R[x]$. For $n \in \mathbb{N}$ let J_n be the set of all $r \in R$ such that $r = 0$ or $r = \operatorname{lead}(f)$ for some $f \in J$ with $\deg f = n$. Observe that J_n is an ideal in R. Since $\operatorname{lead}(xf) = \operatorname{lead}(f)$, $J_n \subseteq J_{n+1}$. Let $0 \leq n \leq t$. By 2.5.23 $\{J_n \mid n \in \mathbb{N}\}$ has a maximal element say J_t, for some $t \in \mathbb{N}$. Then $J_m = J_t$ for all $m \geq t$. By assumption each J_n is finitely generated and so we can choose $r_{nj}, 1 \leq j \leq k_n$ with

$$(*) \qquad J_n = \sum_{j=1}^{k_n} R r_{nj}.$$

For $0 \leq n \leq t$ and $1 \leq j \leq k_n$ pick $f_{nj} \in J$ with

$$(**) \qquad \operatorname{lead}(f_{nj}) = r_{nj}.$$

Let I be the ideal in $R[x]$ generated by the $f_{nj}, 0 \leq n \leq t$ and $1 \leq j \leq k_n$. Note that $I \subseteq J$. For $m > t$ put $k_n := k_t$, $r_{mj} := r_{nj}$ and $f_{mj} := x^{m-t}$. Since $J_m = J_t$ we conclude that (*) and (**) holds for all $n \in \mathbb{N}$. Moreover $f_{nj} \in I$ for all n, j.

We will now show that $J = I$. So let $f \in J$. If $f = 0$, $f \in I$. So suppose $f \neq 0$ and let $n = \deg f$ and $s = \operatorname{lead}(f)$. By (*),

$$s = \sum_{j=1}^{k_n} s_j r_{nj},$$

for some $s_k \in R, 1 \leq j \leq k_n$. Put

$$g := \sum_{j=1}^{k_n} s_j f_{nj}.$$

Then $\mathrm{lead}(g) = s$, $g \in I$ and $\deg g = n$. Thus $f - g \in J$ and $\deg(f-g) < n$. By induction on $\deg f$, $f - g \in I$ and so $f = (f-g) + g \in I$. This shows that $I = J$ and so J is a finitely generated ideal in $R[x]$. □

Corollary 6.5.12. *(a) A is a Noetherian ring.*

(b) Let U be an affine $\mathbb{K}$-variety. Then $U = V(S)$ for some finite subset S of A.

(c) Let $\mathcal{V}$ be a non-empty set of $\mathbb{K}$ varieties in $\mathbb{F}^D$. Then $\mathcal{V}$ has a minimal element.

Proof. (a) Clearly $\mathbb{K}$ is Noetherian, so (a) follows Hilbert's Basis Theorem.

(b) By (a) $J(U)$ is finitely generated as an ideal. So $J(U) = AS$ for some finite subset S of A. Thus by 6.5.3

$$U = V(J(U)) = V(AS) = V(S).$$

(c) Let $\mathcal{I} = \{J(U) \mid U \in \mathcal{V}\}$. Then by (a) and 2.5.23 $\mathcal{I}$ has a maximal element say $J(U_0)$ for some $U_0 \in \mathcal{V}$. Let U be in $\mathcal{V}$ with $U \subseteq U_0$. Then $J(U_0) \subseteq J(U)$ and by maximality of $J(U_0)$, $J(U_0) = J(U)$. Thus

$$U = V(J(U)) = V(J(U_0)) = U_0$$

and so U_0 is a minimal element of $\mathcal{U}$. □

Lemma 6.5.13. *Let S and T be ideals in A. Then*

$$V(S) \cup V(T) = V(S \cap T) == V(ST)$$

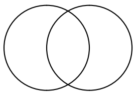
Proof. Clearly $V(S) \cap V(T) \subseteq V(S \cap T)$. Since S and T are ideals, $ST \subseteq S\alpha' T$ and so $V(S \cap T) \subseteq V(ST)$. So it remains to show that $V(ST) \subseteq V(S) \cup V(T)$. Let $u \in F^{\mathrm{D}}$ with $v \notin V(S) \cup V(T)$. Then there exists $s \in S$ and $t \in T$ with $s(u) \neq 0 \neq t(u)$. Then $(st)(u) = s(u)t(u) \neq 0$ and since $st \in ST$, $u \notin V(ST)$. So $V(ST) \subseteq V(S) \cup V(T)$. □

Definition 6.5.14. *An affine $\mathbb{K}$-variety U in $\mathbb{F}^D$ is called $\mathbb{K}$-irreducible provided that:*
Whenever U_1 and U_2 are $\mathbb{K}$-varieties in $\mathbb{F}^D$ with $U = U_1 \cup U_2$, then $U = U_1$ or $U = U_2$

Example 6.5.15. (1) Let $\mathbb{F} = \mathbb{C}$ and $U = V(x^2 - 2y^2)$. If $\mathbb{K} = \mathbb{R}$, then $(x^2 - 2y^2) = (x + \sqrt{2}y)(x - sqrt2y)$ and so by 6.5.13 $U = V(x + \sqrt{2}y) \cup V(x - sqrt2y)$ and so U is not an irreducible $\mathbb{R}$-variety.

But it can be shown that U is an irreducible $\mathbb{Q}$-variety.

(2) Let $\mathbb{F} = \mathbb{C}$ and $\mathbb{K} = \mathbb{Q}$. Let $U = V(x^2 + y^2 - 4)((x-1)^2 + y^2 - 4))$:



Then U is the union of two irreducible subvarieties namely the circles $V(x^2 + y^2 - 4)$ and $V(x-1)^2 + y^2 - 4)$. But U cannot be written has the disjoint union of two subvarieties.

Lemma 6.5.16. *Let U be a affine $\mathbb{K}$-variety in $\mathbb{F}^D$. Then U is $\mathbb{K}$- irreducible if and only if $J(U)$ is a prime ideal in A.*

Proof. Suppose first that $J(U)$ is a prime ideal in A and let U_1, U_2 be affine $\mathbb{K}$-varieties with $U = U_1 \cup U_2$. Then $U = U_1 \cup U_2 \subseteq V(J(U_1)J(U_2))$ and so $J(U_1)J(U_2) \subseteq J(U)$. Since $J(U)$ is a prime ideal we conclude $J(U_i) \subseteq J(U)$ for some $i \in \{1,2\}$. Hence $U \subseteq V(J(U_i)) = U_i \subseteq U$ and so $U = U_i$.

Suppose next that U is irreducible and let J_1 and J_2 be ideal in A with $J_1 J_2 \subseteq J(U)$. We need to show that $J_k \subseteq J(U)$ for some i. Replacing J_i be $J_i + J(U)$ we may assume that $J(U) \subseteq J_i$ for $i = 1$ and 2. Then $V(J_i) \subseteq U_i$. By 6.5.13

$$V(J_1) \cup V(J_2) = V(J_1 \cap J_2) = V(J_1 J_2)$$

Since $J_1 J_2 \leq J(U) \leq J_1 \cap J_2$ we have

$$V(J_1 \cap J_2) \subseteq U = J(V(U)) \subseteq V(J_1 J_2)$$

Thus $U = V(J_1) \cup V(J_2)$ and since U is irreducible, $V(J_k) = U$ for some k. Thus $J_k \leq J(U)$ and $J(U)$ is a prime ideal in A. □

Chapter 7

Simple Rings and Simple Modules

7.1 Jacobson's Density Theorem

Definition 7.1.1. *Let R be a ring and M an R-module. M is called minimal if M has no proper R-submodule. M is called* simple R-module *M is minimal and $RM \neq 0$.*

Example 7.1.2. 1. Let I is be left ideal in R, then R/I is simple if and only if I is a maximal left ideal in R and $R^2 \nsubseteq I$.

2. Let D be a division ring and V is an D-module. We will show that V is a simple $\mathrm{End}_D(V)$ module. For this we first show that for each $u, v \in V$ with $u \neq 0_V$ there exists $\alpha \in \mathrm{End}_D(V)$ with $\alpha(u) = v$. For this let $\mathcal{B}$ be a basis for V with $u \in \mathcal{B}$. Then there exists a unique D-linear map $V \to W$ with $\alpha(w) = v$ for all $w \in \mathcal{B}$. In particular, $\alpha(u) = v$.

   Now let U be any non-zero $\mathrm{End}_D(V)$-submodule of B. Let $u \in U^\sharp$ and $v \in V$. Then by the above there exists $\alpha \in \mathrm{End}_D(V)$ with $\alpha(u) = v$. Thus $v \in U$ and $U = V$.

Lemma 7.1.3 (Schur's Lemma)**.** *Let M, N be simple R-modules and $f \in \mathrm{Hom}_R(M, N)$. If $f \neq 0$, then f is R-isomorphism. In particular,* $\mathrm{End}_R(M)$ *is a division ring.*

Proof. Since $f \neq 0$, $\ker f \neq M$. Also $\ker f$ is an R-submodule and so $\ker f = 0$ and f is 1-1. Similarly, $\mathrm{Im} f \neq 0$, $\mathrm{Im} f = N$ and so f is onto. So f is a bijection and has an inverse f^{-1}. An easy computation shows that $f^{-1} \in \mathrm{Hom}_R(N, M))$. Choosing $N = M$ we see that $\mathrm{End}_R(M)$ is a division ring. □

Definition 7.1.4. *Let R be a ring and M be an R-module.*

(a) Let $N \subseteq M$. N is called R-closed *in M if $N = \mathrm{Ann}_M(\mathrm{Ann}_R(N)$.*

(b) Let $I \subseteq R$. I is called M-closed *in R if $I = \mathrm{Ann}_R(\mathrm{Ann}_M(I)$.*

Lemma 7.1.5. *Let R be a ring and M an R module. Let $U \subseteq \tilde{U} \subseteq M$ and $S \subseteq \tilde{S} \subseteq R$.*

(a) $U \subseteq \mathrm{Ann}_R(S)$ if and only if $S \subseteq \mathrm{Ann}_M(R)$.

(b) $\mathrm{Ann}_R(\tilde{U}) \subseteq \mathrm{Ann}_R(U)$.

(c) $\mathrm{Ann}_M(\tilde{S}) \subseteq \mathrm{Ann}_M(S)$.

(d) $U \subseteq \mathrm{Ann}_M(\mathrm{Ann}_R(U))$.

(e) $S \subseteq \mathrm{Ann}_R(\mathrm{Ann}_M(S))$.

(f) *U is R-closed in M if and only if $U = \mathrm{Ann}_M(S)$ for some $S \subseteq M$.*

(g) *S is M-closed in R if and only if $S = \mathrm{Ann}_R(U)$ for some $U \subseteq M$.*

(h) *$I \to \mathrm{Ann}_M(I)$ is an inclusion reversing bijection between the M-closed subsets of R and R-closed subsets of M with inverse $W \to \mathrm{Ann}_R(W)$.*

Proof. This follows from A.1.13 applied to the relation $\{(r,m) \in R \times M \mid rm = 0\}$. □

Lemma 7.1.6. *Let R be a ring and M an R-module.*

(a) *Let W be an R-closed subset of M (that is $W = \mathrm{Ann}_M(I)$ for some $I \subseteq R$). Then W is an $\mathrm{End}_R(M)$-submodule of M.*

(b) *Let I be an M-closed subset of R (that is $R = \mathrm{Ann}_R(W)$ for some $W \subseteq M$). Then I is left ideal in R,*

(c) *Let I be an R-closed subsets of R. Then W is an R-submodule of M if and only of $\mathrm{Ann}_R(W)$ is an ideal in R.*

(d) *Let I be an M-closed subset of R. Then I is an ideal in R if and only if $\mathrm{Ann}_M(I)$ is an R-submodule of M.*

(e) *$I \to \mathrm{Ann}_M(I)$ is an inclusion reversing bijection between the M-closed ideals of R and R-closed R-submodules of M with inverse $W \to \mathrm{Ann}_R(W)$.*

Proof. (a) Let $m \in \mathrm{Ann}_M(I)$, $i \in I$ and $\phi \in \mathrm{End}_R(M)$. Then

$$i(\phi m) = \phi(im) = \phi 0 = 0$$

and so $\phi m \in \mathrm{Ann}_M(I)$.

(b) By 3.1.24(c), $\mathrm{Ann}_R(W)$ is a left ideal in R.

(c) If I is ideal in R, the 3.1.24(d) shows that $W := \mathrm{Ann}_M(I)$ is an R-submodule of M. If W is an R-submodule of M, then by 3.1.24(e), $\mathrm{Ann}_R(W)$ is an ideal in R. Since I is closed $I = \mathrm{Ann}_R(W)$ and so I is an ideal in R.

(d) Put $I = \mathrm{Ann}_R(W)$. Since W is R-closed, $W = \mathrm{Ann}_R(I)$ and (d) follows from (c).

(e) follows from (c) and 7.1.5(h). □

Lemma 7.1.7. . *Let M be a simple R-module, V a R-closed subset of M and $w \in M \setminus V$. Put $I = \mathrm{Ann}_R(V)$. Then $M = Iw$ and the map $\beta : I/\mathrm{Ann}_I(w) \to M, i + \mathrm{Ann}_I(w) \to iw$ is a well defined R-isomorphism.*

Proof. Since V is closed, $V = \mathrm{Ann}_R(V)$ and so $Iw \neq 0$. By 3.1.24 I is a left ideal in R. Define

$$\phi : I \to M, i \to iw$$

Then ϕ is R-linear, $\mathrm{Im}\,\phi = Iw$ and $\ker\phi = \mathrm{Ann}_I(w)$. Thus by Isomorphism Theorem of modules,

$$\beta : I/\mathrm{Ann}_I(w) \to Im, i + \mathrm{Ann}_I(w) \to iw.$$

is a well-defined R-isomorphism. In particular, Iw is an R-submodule of M. Since $Iw \neq o$ and e M is simple, $M = Iw$ and the lemma is proved. □

Lemma 7.1.8. *Let M be simple R-module and $\mathbb{D} = \mathrm{End}_R(M)$. Let $V \leq W$ be $\mathbb{D}$-submodules of M with $\dim_{\mathbb{D}}(W/V)$ finite. If V is closed in M with respect to R, then also W is closed in M with respect to R. In particular, all finite-dimensional $\mathbb{D}$ subspaces of M are closed.*

Proof. By induction on $\dim_{\mathbb{D}} W/V$ we may assume that $\dim_{\mathbb{D}} W/V = 1$. Let $w \in W \setminus V$. Then $W = V + \mathbb{D}w$. Put $I = \mathrm{Ann}_R(V)$ and $J = \mathrm{Ann}_I(w)$. We will show that $W = \mathrm{Ann}_R(J)$. So let $m \in \mathrm{Ann}_M(J)$. Then $J \subseteq \mathrm{Ann}_I(m)$ and hence the map $\alpha : I/J \to M, i + J \to im$ is well defined and R-linear. By 7.1.7 the map $\beta : I/J \to M, i + J \to iw$ is an R-isomorphism. Put $\delta = \alpha\beta^{-1}$. Then $\delta : M \to M$ is R-linear and $\delta(iw) = im$ for all $i \in I$. Hence $\delta \in \mathbb{D}$ and

$$i(m - \delta(w)) = im - i\delta(w)) = im - \delta(iw) = im - im = 0$$

] for all $i \in I$. Since V is closed, $V = \mathrm{Ann}_M(I)$ and so $\delta(w) - m \in V$. Thus $m \in \delta(w) + V \leq W$ and $\mathrm{Ann}_M(J) \subseteq W$

Since $\mathrm{Ann}_M(J)$ is a D-submodule of M containing V and w, $W = V + \mathbb{D}w \leq \mathrm{Ann}_M(J)$. Hence $W = \mathrm{Ann}_W(J)$ and so by 7.1.5(f), W is R-closed in M.

Since M is a simple R-module, $RM \neq 0$ and so $\mathrm{Ann}_M(R) \neq M$. Since M is simple this implies $\mathrm{Ann}_M(R) = 0$. So 0 is a R-closed in M. Hence the first statement of the lemma implies the second. □

Definition 7.1.9. *Let M be an R-module and $\mathbb{D} \leq \mathrm{End}_R(M)$ a division ring. Then we say that R acts densely on M with respect to $\mathbb{D}$ if for each finite $\mathbb{D}$-linearly independent family $(m_i)_{i=1}^n$ in M and each family $(w_i)_{i=1}^n$ in M there exists $r \in R$ with*

$$rm_i = w_i$$

for all $1 \leq i \leq n$.

Theorem 7.1.10 (Jacobson's Density Theorem)**.** *Let R be a ring and M a simple R-module. Put $\mathbb{D} := \mathrm{End}_R(M)$, then R acts densely on M with respect to $\mathbb{D}$.*

Proof. Let $(m_i)_{i=1}^n$ be finite $\mathbb{D}$-linear independent family in M and and $(w_i)_{i=1}^n$ a family of M. By induction on n we will show that there exists $r \in R$ with $rm_i = w_i$ for all $1 \le i \le n$. For $n = 0$, there is nothing to prove. By induction there exists $s \in R$ with $sm_i = w_i$ for all $1 \le i < n$. Put $V = \langle m_i \mid 1 \le i < n \rangle_{\mathbb{D}}$. Then by 7.1.8 V is R-closed and so by 7.1.7 there exists $t \in \mathrm{Ann}_R(V)$ with $tm_n = w_n - sm_n$. Put $r = s + t$. For $1 \le i < n$, $tm_i = 0 =$ and so $rm_i = sm_i = w_i$. Also $rm_i = sm_i + tm_i = sm_n + (w_n - sm_n) = w_n$ and the theorem is proved. □

Definition 7.1.11. *Let R be a ring and M an R-module.*

(a) Let $W \subseteq M$. Then $\mathrm{N}_R(W) = \{r \in R \mid rW \subseteq W\}$.

(b) $R|_M$ is the image of R in $\mathrm{End}(M)$ under $*_R : R \to \mathrm{End}(M), r \to (m \to rm)$.

Corollary 7.1.12. *Let M be a simple R-module, $\mathbb{D} = \mathrm{End}_R(M)$ and W a finite dimensional $\mathbb{D}$-submodule of M. . Then $\mathrm{N}_R(W)$ is a subring of W, W is an $\mathrm{N}_R(W)$-submodule of M, $\mathrm{Ann}_R(W)$ is an ideal in $\mathrm{N}_R(W)$ and then*

$$\mathrm{N}_R(W)/\mathrm{Ann}_R(W) \cong \mathrm{N}_R(W)^{*W} = \mathrm{End}_{\mathrm{D}}(W).$$

Proof. Let $r, s \in \mathrm{N}_R(W)$ and $w \in W$. Then $(r + s)w = rw + sw \in W$ and $(rs)w = r(sw) \in W$. Thus $\mathrm{N}_R(W)$ is a subring of R. Consider

$$\Phi : \mathrm{N}_R(W) \to \mathrm{End}_{\mathbb{D}}(W), r \to (m \to rm)$$

Then $\ker\Phi = \mathrm{Ann}_R(W)$ and $\mathrm{Im}\,\Phi = \mathrm{N}_R(W)^{*W} = \mathbb{E}$. So the first isomorphism theorem for rings shows that $\mathrm{Ann}_R(W)$ is an ideal in $\mathrm{N}_R(W)$ and $\mathrm{N}_R(W)/\mathrm{Ann}_R(W) \cong \mathrm{N}_R(W)^{*W}$.

Let $\phi \in \mathrm{End}_{\mathrm{D}}(W)$ and choose a basis $(m_i)_{i=1}^n$ for W over $\mathbb{D}$. By 7.1.10 there exists $r \in R$ with $rv_i = \phi v_i$ for all $1 \le i \le n$. Then $rW \le W$ and so $r \in \mathrm{N}_R(W)$. Since both $\Phi(r)$ and ϕ are in $\mathrm{End}_{\mathrm{D}}(W)$ and map $m_i \to \phi m_i$, $\Phi(r) = \phi$. Thus Φ is onto and $\mathrm{N}_R(W)^{*W} = \mathrm{End}_{\mathrm{D}}(W)$. □

Corollary 7.1.13. *Let R be ring, M be a simple R-module and put $\mathbb{D} = \mathrm{End}_R(M)^{\mathrm{op}}$. Suppose that M is a finite dimensional $\mathbb{D}$-module. Then*

$$R/\mathrm{Ann}_R(M) \cong R|_M = \mathrm{End}_{\mathbb{D}}(M)$$

Proof. Note that $\mathrm{N}_R(M) = R$. So 7.1.13 follows from 7.1.12 applied with $W = M$. □

7.2 Semisimple Modules

Definition 7.2.1. *Let R be a ring and M an R-module. M is called a* semisimple *R-module if M is the (internal) direct sum of simple R-submodules.*[1]

[1] Note that this holds if and only if M is isomorphic to the external direct sum of simple R-modules

Lemma 7.2.2. *Let R be ring, M an R-module, N an R-submodule of M, $\mathcal{S}$ a set of simple R-submodules of M and $\mathcal{I} \subseteq \mathcal{S}$. Suppose that*

$$N \cap \sum \mathcal{I} = 0, \qquad \sum \mathcal{I} = \bigoplus \mathcal{I}, \qquad \textit{and} \qquad M = N + \sum \mathcal{S}$$

Then there exists $\mathcal{M} \subseteq \mathcal{S}$ with $\mathcal{I} \subseteq \mathcal{M}$ such that

$$M = N \oplus \bigoplus \mathcal{M}$$

Proof. Let $\mathfrak{M}$ be set of all sets $\mathcal{T}$ such that

$$\mathcal{I} \subseteq \mathcal{T} \subseteq \mathcal{S}, \quad N \cap \sum \mathcal{T} = 0 \quad \text{and } \sum \mathcal{T} = \bigoplus \mathcal{T}.$$

Since $\mathcal{I} \in \mathfrak{M}$, $\mathfrak{M} \neq \varnothing$. Order $\mathfrak{M}$ by inclusion and let $(\mathcal{D}_i)_{i \in I}$ be a chain in $\mathfrak{M}$. Let $\mathcal{D} = \bigcup_{i \in I} \mathcal{D}_i$. We will show that $\mathcal{D} \in \mathfrak{M}$ (and so $\mathcal{D}$ is an upper bound for $(\mathcal{D}_i)_{i \in I}$). If $i \in I$, then $\mathcal{D}_i \in \mathfrak{M}$ and so $\mathcal{I} \subseteq \mathcal{D}_i \subseteq \mathcal{S}$. Hence also $\mathcal{I} \subseteq \mathcal{D} \subseteq \mathcal{S}$.

Note that $(\sum \mathcal{D}_i)_{i \in I}$ is chain of submodules of M and so $\sum \mathcal{D} = \bigcup_{i \in I} \sum \mathcal{D}_i$. By definition of $\mathfrak{M}$, $N \cap \sum \mathcal{D}_i = 0$ for all $i \in I$ and so also $N \cap \sum \mathcal{D} = 0$.

Let $S \in \mathcal{D}$ and put $J = \{i \in I \mid S \in \mathcal{D}_i\}$. For $i \in I$ define $\mathcal{D}'_i = \mathcal{D}_i \setminus \{S\}$. Also let $\mathcal{D}' = \mathcal{D} \setminus \{S\}$. Since $(\mathcal{D}_i)_{i \in I}$ is a chain,

$$\mathcal{D} = \bigcup_{j \in J} \mathcal{D}_j \qquad \text{and so} \quad \mathcal{D}' = \bigcup_{j \in J} \mathcal{D}'_j$$

Note that $(\sum \mathcal{D}'_j)_{j \in J}$ is a chain of R-submodules of M and so $\sum \mathcal{D}' = \bigcup_{j \in J} \sum \mathcal{D}'_j$.

By definition of $\mathfrak{M}$, $\sum \mathcal{D}_j = \bigoplus \mathcal{D}_j$ and so $S \cap \sum \mathcal{D}'_j = 0$ for all $j \in J$. It follows that $S \cap \sum \mathcal{D}' = 0$. Thus the definition of an internal direct sum implies $\sum \mathcal{D} = \bigoplus \mathcal{D}$. Hence $\mathcal{D} \in \mathfrak{M}$.

We proved that every chain in $\mathfrak{M}$ has an upper bound. So we can apply Zorn's lemma to obtain a maximal element $\mathcal{M}$ in $\mathfrak{M}$. Put $W = \sum \mathcal{M}$.

Suppose for a contradiction that that $M \neq N + W$. By assumption $M = N + \sum \mathcal{S}$ and so there exists $S \in \mathcal{S}$ with $S \nleq N + W$. Then $S \neq (N + W) \cap S$ and since S is a simple R-module, $(N + W) \cap S = 0$. So

$$(N + W) \cap (S + W) = W + ((N + W) \cap S) = W \quad \text{and so} \qquad N \cap (S + W) \leq N \cap W = 0.$$

Also $W \cap S = 0$ implies that

$$\sum \big(\mathcal{M} \cup \{S\}\big) = W + S = W \oplus S = (\bigoplus \mathcal{M}) \oplus S = \bigoplus \big(\mathcal{M} \cup \{S\}\big).$$

Thus $\mathcal{M} \cup \{S\} \in \mathfrak{M}$. Since $S \nleq N + W$, $S \notin \mathcal{M}$ and we obtain a a contradiction to the maximality of $\mathcal{M}$.

Thus

$$M = N + W = N \oplus W = N \oplus \sum \mathcal{M} = N \oplus \bigoplus \mathcal{M}$$

and the lemma is proved. □

Lemma 7.2.3. *Let $\mathcal{S}$ a set of simple R-submodules of the R-module M. Also let N be a R-submodule of M and suppose that $M = \sum \mathcal{S}$.*

(a) There exists a subset $\mathcal{M}$ of $\mathcal{S}$ with $M = N \oplus \bigoplus \mathcal{M}$.

(b) $M = \bigoplus \mathcal{T}$ for some $\mathcal{T} \subseteq \mathcal{S}$.

(c) $M/N \cong \bigoplus \mathcal{T}$ for some subset $\mathcal{T}$ of $\mathcal{S}$.

(d) M/N is semisimple.

(e) $N \cong \bigoplus \mathcal{T}$ for some subset $\mathcal{T}$ of $\mathcal{S}$.

(f) N is semisimple.

(g) If N is a simple R-module, then $N \cong S$ for some $S \in \mathcal{S}$.

(h) Suppose N is a maximal N-submodule of M, then $M/N \cong S$ for some $S \in \mathcal{S}$.

(i) M is semisimple R-module.

Proof. (a): This follow from 7.2.2 applied with $\mathcal{I} = \emptyset$.

(b) follows from (a) applied with $N = 0$.

(c) follows from (a).

(d) follows from (c).

(e): Put $W = \sum \mathcal{M}$. By (a), $M = N \oplus W$ and so $M/W \cong N$. $N \cong M/W$. So (e) follows from (c) applied to W in place of N.

(f) follows from (e).

(g): Suppose N is simple. Then the set $\mathcal{T}$ from (e) only contains one element, say S. So $N \cong S$ and (g) is proved.

Suppose that N is a maximal R-submodule of M. Then the set $\mathcal{T}$ from (b) only contains one elements, say S. Thus $M/N \cong S$.

(i) follows from (f). □

Corollary 7.2.4. *Let R be a ring, M a semisimple R-module and A and B R-submodules of M with $A \leq B$. Then A/B is semisimple.*

Proof. 7.2.3(f) implies that B is semisimple. Then 7.2.3(d) applied to (A, B) in place of (N, M) shows that B/A is semisimple. □

Lemma 7.2.5. *Let M a semisimple R-module and N an R-submodule of M with $N \neq M$. Let $\mathcal{M}$ be the set of maximal R-submodules of M containing N. Then $\bigcap \mathcal{M} = N$.*

Proof. By 7.2.4 M/N is a semisimple R-module. Thus replacing M by M/N we may assyme that $N = 0$. Let $\mathcal{S}$ be a set of simple R-submodules of M with $M = \bigoplus \mathcal{S}$. For $S \in \mathcal{S}$, put $S^* = \sum_{S \neq T \in \mathcal{S}} T$. Then $M/S^* \cong S$ and so S^* is a maximal R-submodule of S. Then $0 \leq \bigcap \mathcal{M} \subseteq \bigcap_{S \in \mathcal{S}} S^* = 0$ and so $\bigcap \mathcal{M} = 0 = N$. □

7.3 Simple Rings

Lemma 7.3.1. *Let R be non-zero ring with identity. Then there exists a simple R-module.*

Proof. Let $\mathcal{C}$ be non-empty chain of proper left ideal in R. Then $1 \notin \bigcup \mathcal{C}$ and so $\mathcal{C}$ is a proper left ideal in R. Hence by Zorn's Lemma, R has a maximal left ideal I. Since R has an identity, $R^2 = R \nsubseteq I$ and so by 7.1.2 R/I is a simple R-module. □

Proposition 7.3.2. *Let R be a simple ring and M a simple R-module. Put $\mathbb{D} = \mathrm{End}_R(M)$. Then M is a faithful R-module and R is isomorphic to subring of $\mathrm{End}_{\mathbb{D}}(M)$ acting densely on M.*

Proof. By definition of a simple R-module, $RM \neq 0$ and so $\mathrm{Ann}_R(M) \neq R$. Since M is simple and $\mathrm{Ann}_R(M)$ is an ideal in M, $\mathrm{Ann}_R(M) = 0$. Thus $R \cong R|_M$. By 7.1.10, R and so also $R|_M$ acts densely on M. □

Proposition 7.3.3. *Let M be faithful, simple R-module and put $\mathbb{D} = \mathrm{End}_R(M)$. Suppose that $n := \dim_{\mathbb{D}} M$ is finite.*

(a) $R \cong R|_M = \mathrm{End}_{\mathbb{D}}(M)$.

(b) $R \cong M^n$ as a left R-module. In particular, R is semisimple as a left R-module.

(c) Let I be a maximal left ideal in R. Then $I = \mathrm{Ann}_R(m)$ for some $m \in M^\sharp$ and $R/I \cong M$ as an R-module.

(d) Let $I \subseteq R$. Then I is closed in M with respect to R if and only if I is a left ideal.

(e) Let $W \subseteq M$. Then W is closed in M with respect to R if and only if W is a $\mathbb{D}$-subspace M.

(f) The map $I \to \mathrm{Ann}_R(I)$ is an inclusion reversing bijection between the left ideals in R and the $\mathbb{D}$-subspaces of M with inverse $M \to \mathrm{Ann}_M(I)$.

(g) Each simple R-module is isomorphic to M.

(h) R is a simple ring with identity.

Proof. (a): Since M is faithful $\mathrm{Ann}_R(M) = 0$. Thus $R \cong R/\mathrm{Ann}_R(M)$ and (b) follows from 7.1.13.

(b) Let $(m_i)_{i=1}^n$ be $\mathbb{D}$ basis for M. M over $\mathbb{D}$. Define

$$\gamma : R \to M^n, r \to (rm_i)_{i=1}^n.$$

Then γ is R-linear, Let $(w_i)_{i=1}^n \in M^n$. By the density theorem there exists $r \in R$ with $rm_i = w_i$ for all $1 \leq i \leq n$. Hence γ is onto. Let $r \in \ker\gamma$. Then $rm_i = 0$ for all $1 \leq i \leq n$, Since $\mathrm{Ann}_M(r)$ is a $\mathbb{D}$-subspace of M we conclude that $\mathrm{Ann}_M(r) = M$. Since M is a faithful R-module, $r = 0$ and so γ is 1-1. Thus γ is an R-isomorphism.

(c) By (b) 7.2.3(h), $R/I \cong M$. Note that by (a), R has an identity 1. Let $\phi : R/I \to M$ be an R-isomorphism and put $m = \phi(1+I)$. Then $\mathrm{Ann}_R(m) = \mathrm{Ann}_R(1+I)$ and By 3.1.26 $\mathrm{Ann}_R(1+I) = I$.

(d) Let I be an left ideal in R and $\mathcal{M}$ the set of maximal ideals in R containing I. By (b), R is a semisimple R-module and so 7.2.5 implies that $\bigcap \mathcal{M} = I$. By (c), for each $J \in \mathcal{M}$ there exists $m_J \in M$ with $J = \mathrm{Ann}_R(m_J)$. Put $N = \{m_J \mid J \in \mathcal{M}\}$. Then

$$\mathrm{Ann}_R(N) = \bigcap_{J \in \mathcal{M}} \mathrm{Ann}_R(m_J) = \bigcap_{J \in \mathcal{M}} J = I.$$

So I is closed in R with respect to M. By 7.1.6 each closed subset of T is a left ideal in R and so (d) holds.

(e) Since M is finite dimensional over $\mathbb{D}$, any $\mathbb{D}$ subspace of M is finite dimensional over D and so by closed by 7.1.8. By 7.1.6 each closed subset of M is a $\mathbb{D}$-subspace and so (e) holds.

(f) By7.1.6 $I \to \mathrm{Ann}_M(I)$ is a inclusion reversing bijection between the closed subsets of R and the closed subsets of M with inverse $W \to \mathrm{Ann}_R(W)$. Thus (f) follows from (d) and (e).

(g) Let W be a simple R-module and $w \in W^\sharp$. Then $R/\mathrm{Ann}_R(w) \cong Rw = W$. Hence $\mathrm{Ann}_R(w)$ is maximal left ideal in R and so (c) $W \cong R/\mathrm{Ann}_R(w) \cong M$.

(h) Let I be an ideal in R. Then $\mathrm{Ann}_M(I)$ is an R-submodule of M. Since M is simple, $\mathrm{Ann}_M(I) = 0$ or $\mathrm{Ann}_M(I) = M$. By (f), $I = \mathrm{Ann}_R(\mathrm{Ann}_M(I)$ and so $I = \mathrm{Ann}_R(0) = R$ or $I = \mathrm{Ann}_R(M) = 0$. Since R has an identity, $R^2 \neq 0$ and so R is simple. □

Definition 7.3.4. *A ring R is called* Artinian *for every non-empty set of left ideals in* $\mathbb{R}$ *has a minimal element.*

Lemma 7.3.5. *Let R be an Artinian ring and M a simple R-module. Then M is finite dimensional over* $\mathbb{D} = \mathrm{End}_R(M)$.

Proof. Suppose that $\dim_{\mathbb{D}} M = \infty$. Then there exists an infinite strictly ascending series

$$M_1 < M_2 < M_3 < \ldots <$$

of finite dimensional $\mathbb{D}$-subspaces. By 7.1.8 each M_i is closed. Thus

$$\mathrm{Ann}_R(M_1) > \mathrm{Ann}_R(M_2) > \mathrm{Ann}_R(M_3) > \ldots$$

is a strictly descending chain of left ideals in R, contradicting the definition of an Artinian ring. □

Theorem 7.3.6. *Let R be a simple Artinian ring. Then there exists a simple R-module M, M is unqiue up to isomorphism and if* $\mathbb{D} := \mathrm{End}_R(M)^{\mathrm{op}}$, *then* $n = \dim_{\mathbb{D}} M$ *is finite and* $R \cong \mathrm{End}_{\mathbb{D}}(M) \cong \mathrm{M}_{nn}(\mathbb{D})$.

Proof. Since R is Artinian, R has a minimal left ideal M. Suppose that $RM = 0$ and put $I = \{r \in R \mid Rr = 0\}$. Then I is an ideal in R with $M \subseteq I$. Since R is simple we get $I = R$ and so $R^2 = 0$, a contradiction to the definition of a simple ring. Thus $RM \neq 0$ and so M is a simple R-module. By 7.3.5 $\dim_{\mathbb{D}}(M)$ is finite and by 7.3.2 M is a faithful R-module. Thus by 7.3.3(h), M is unique up to isomorphism and by 7.3.3(a), $R \cong \mathrm{End}_{\mathbb{D}}(M)$. □

Definition 7.3.7. *Let R be a ring and M an R-module. Let α be an ordinal and $T = (T_\beta)_{\beta\in\alpha}$ be family of R-submodules of M. For $0 < \beta \leq \alpha$ define $B_\beta = \bigcup_{\gamma<\alpha} T_\beta$. Then α is called an ascending composition series for R on M provided that*

(i) $T_0 = 0$ and $B_\alpha = M$.

(ii) for each $0 < \beta < \alpha$, B_β is a maximal R-submodule of T_β.

The R-modules T_β/B_β, $0 < \beta < \alpha$ are called the composition factors of T.

Example 7.3.8. *1. Let R be a ring, M an R-module, $n \in \mathbb{N}$ and*

$$0 = T_0 < T_1 < T_2 < \ldots < T_{i-1} < T_i < \ldots T_{n-1} < T_n = M$$

be finite chain of R-submodules such that T_i/T_{i-1} is simple R-module for all $0 \leq i \leq n$. Then $(T_i)_{0\leq i<n+1}$ is an ascending composition series of M with $B_i = T_{i-1}$ for all $0 < i \leq n+1$.

2. Let R be a ring and M an R-module and $(S_\beta)_{0\neq\beta\in\alpha}$ a family simple R-submodules of M with $M = \bigoplus_{0<\beta\in\alpha} S_\beta$. For $\beta < \alpha$ define $T_\beta = \sum_{0<\gamma\leq\beta} S_\gamma$. Then for $0 < \beta \leq \alpha$, $B_\beta = \sum_{0<\gamma<\beta} S_\gamma$. So $B_\alpha = M$ and for $0 < \beta < \alpha$, $B_b \leq T_\beta$, $T_\beta = B_\beta \oplus S_\beta$ and $T_\beta/B_\beta \cong S_\beta$. In particular, $(T_\beta)_{\beta\in\alpha}$ is a composition series for R.

3. Let R be a PID with field of fraction $\mathbb{F}$. Let p be prime in R and

$$R_{p^\infty} = \{\frac{a}{p^n} + R \mid a \in R, n \in \mathbb{N}\} \subseteq \mathbb{F}/R.$$

For $n \in \mathbb{N}$ define

$$T_n = \{\frac{a}{p^n} + R \mid a \in R, n \in \mathbb{N}\} \subseteq \mathbb{F}/R$$

Then $(T_n)_{n\in\mathbb{N}}$ is an ascending R-composition series for R_{p^∞}, and for all $0 \neq n \in \mathbb{N}$, $B_n = T_{n-1}$ and $T_n/B_n \cong R/pR$.

Lemma 7.3.9. *Let R be a ring, M an R-module and let T, B, T^*, B^* be R submodules of M. Suppose that*

$$T = (T \cap T^*) + B, \qquad T^* = (T \cap T^*) + B^* \qquad \text{and} \qquad T \cap B^* = T^* \cap B$$

Then

$$T/B \quad\cong\quad (T \cap T^*)/(B \cap B^*) \quad\cong\quad T^*/B^*$$

as R-modules.

Proof. Since $T \cap B^* = T^* \cap B$ we have $T^* \cap B = B \cap B^*$ and $(T \cap T^*) \cap B = T^* \cap B = B \cap B^*$. Using $T = \big(T \cap T^{)} + B$ and the Second Isomorphism Theorem for modules:

$$T/B = (T \cap T^*) + B/B \cong (T \cap T^*)/(T \cap T^*) \cap B = (T \cap T^*)/(B \cap B^*)$$

By symmetry, also $T^*/B^* \cong (T \cap T^*)/(B \cap B^*)$. □

Lemma 7.3.10. *Let R be a ring, M an R-module and let T, B, T^*, B^* be R submodules of M. Suppose B is a maximal R-submodule of T and B^* is a maximal R-submodule of T^*. Then the following statements are equivalent:*

(a) $(T \smallsetminus B) \cap T^* \neq \varnothing$ *and* $(T \smallsetminus B) \cap B^* = \varnothing$.

(b) $T = (T + T^*) + B$, $T^* = (T \cap T^*) + B^*$ *and* $T \cap B^* = T^* \cap B$.

(c) $(T^* \smallsetminus B^*) \cap T \neq \varnothing$ *and* $(T^* \smallsetminus B^*) \cap B = \varnothing$.

Proof. Note first that (a) is equivalent to

$$(*) \qquad T \cap T^* \nsubseteq B \qquad \text{and} \qquad T \cap B^* \subseteq B$$

Suppose that (*) holds. Suppose for a contradiction that $T^* \cap B \nleq B^*$. Since B^* is maximal R-submodule of T^*, $T^* = (T^* \cap B) + B^*$. Since $T^* \cap B \leq T \cap T^*$ the modular law implies

$$T \cap T^* = \big(T^* \cap B\big) + \big((T \cap T^*) \cap B^*\big) \leq B + (T \cap B^*) \leq B$$

a contradiction.

Hence $T^* \cap B \leq B^*$. Together with $T \cap B^* \leq B$, this gives $T^* \cap B = B \cap B^* = T \cap B^*$. So the last statement in (b) holds. Also since $T^* \cap B \leq B^*$ and $T \cap T^* \nleq B$ we conclude that $T \cap T^* \nleq B^*$. Since B is a maximal R-submodule of T^* and B^* is maximal R-submodule of T^* we get $T = (T \cap T^*) + B$ and $T^* = (T \cap T^*) + B^*$. Thus (b) holds.

Suppose that (b) holds. Since $T = (T \cap T^*) + B$ we get $T \cap T^* \nleq B$ and since $T \cap B^* = T^* \cap B$, $T \cap B^* \leq B$. So (*) holds.

We proved that (*) is equivalent to (b). Hence (a) is equivalent to (b). By symmetry, (c) is equivalent to (b) and the lemma is proved. □

If (a) and (b) are equivalent, then by symmetry also (c) and (b) are equivalent.

Theorem 7.3.11 (Jordan-Hölder)**.** *Let R be a ring, M and R-module and suppose $(T_\beta)_{\beta\in\alpha}$ and $(T^*_\beta)_{\beta\in\alpha^*}$ are ascending R-composition series for M. Then there exists a bijection $\Phi : \alpha \smallsetminus \{0\} \to \alpha^* \smallsetminus \{0\}$ such that*

$$T_\beta/B_\beta \cong T^*_{\Phi\beta}/B^*_{\Phi\beta}$$

for all $0 < \beta < \alpha$,

In particular, $|\alpha| = |\alpha^*|$ *and if* α *is finite,* $\alpha = \alpha^*$.

Proof. Let $0 < \beta < \alpha$. Then $T_\beta \smallsetminus B_\beta \neq \varnothing$. Since $M = B^*_{\alpha^*} = \bigcup_{\gamma\in\alpha^*} T^*_\gamma$ there exists $\gamma \in \alpha^*$ with $(T_\beta \smallsetminus B_\beta) \cap T^*_\gamma \neq \varnothing$. So we can choose $\Phi\beta \in \alpha^*$ minimal with

$$(T_\beta \smallsetminus B_\beta) \cap T^*_{\Phi\beta} \neq \varnothing.$$

Note that $\Phi\beta \neq 0$.

Let $\gamma \in \alpha^*$. If $\gamma < \Phi\beta$, then by minimality of $\Phi\beta$, $(T_\beta \smallsetminus B_\beta) \cap T^*_\gamma = \varnothing$. Since $B^*_\beta = \bigcup_{\gamma\in\beta} T^*_\gamma$ this gives $(T_\beta \smallsetminus B_\beta) \cap B^*_{\Phi\beta} = \varnothing$. If $\Phi\beta < \gamma$, then $\varnothing \neq (T_\beta \smallsetminus B_\beta) \cap T_\gamma \subseteq (T_\beta \smallsetminus B_\beta) \cap B^*_\gamma$. It follows that

$$\gamma = \Phi\beta \qquad \Longleftrightarrow \qquad \Big(\, (T_\beta \smallsetminus B_\beta) \cap T^*_\gamma \neq \varnothing \quad \text{and} \quad (T_\beta \smallsetminus B_\beta) \cap B^*_\gamma = \varnothing \,\Big)$$

For $0 \neq \gamma \in \alpha^*$ let $\Phi^*\gamma \in \alpha$ be minimal with $(T^*_\gamma \smallsetminus B^*_\gamma) \cap T_{\Phi^*\gamma} \neq \varnothing$. By symmetry.

$$\beta = \Phi^*\gamma \qquad \Longleftrightarrow \qquad \Big(\, (T^*_\gamma \smallsetminus B^*_\gamma) \cap T_\beta \neq \varnothing \quad \text{and} \quad (T^*_\gamma \smallsetminus B^*_\gamma) \cap B_\beta = \varnothing \,\Big)$$

Thus by 7.3.10 $\gamma = \Phi\beta$ if and only if $\beta = \Phi^*\gamma$. Hence Φ is a bijection with inverse Φ^*. If $\gamma = \Phi\beta$, 7.3.10 also shows that

$$T_\beta = (T_\beta \cap T^*_\gamma) + B_\beta, \quad T^*_\gamma = (T_\beta \cap T^*_\gamma) + B^*_\gamma, \quad T_\beta \cap B^*_\gamma = T^*_\gamma \cap B_\beta$$

and so by 7.3.9

$$T_\beta / B_\beta \cong T^*_\gamma / B^*_\gamma$$

as R-modules. □

Corollary 7.3.12. *Let R be a ring, M a semisimple R-module and suppose $\mathcal{S}$ and $\mathcal{T}$ are sets of simple R-submodules of M with $M = \bigoplus \mathcal{S}$ and $M = \bigoplus \mathcal{T}$. Then there exists a bijection $\Phi : \mathcal{S} \to \mathcal{T}$ such that for all S in $\mathcal{S}$, $S \cong \Phi S$ as an R-module.*

Proof. By 7.3.8(3) there exists ascending series for M with factors $\mathcal{S}$ and $\mathcal{T}$ respectively. Thus the corollary follows from the Jordan Hölder Theorem 7.3.11 □

Definition 7.3.13. *Let R be a ring and M an R module.*

(a) We say that a class $\mathcal{S}$ of R-modules is closed under isomorphism if $T \in \mathcal{S}$. whenever S and T are R-modules with $S \in \mathcal{S}$ and $S \cong_R T$.

(b) Let $\mathcal{S}$ be class of simple R-modules. Then M is called $\mathcal{S}$-semisimple of M is semisimple and any simple R-submodule is isomorphic to $S \in \mathcal{S}$.

(c) Let S be a simple R-module. Then M is called S- homogeneous if M is a semisimple R-module and any simple R-submodule of M is isomorphic to M.

Note that M is S-homogeneous if and only if M is $\{S\}$-semisimple.

Lemma 7.3.14. *Let R be a ring, M an R-module $\mathcal{S}$ a class of simple R-modules closed under isomorphism. Then the following statements are equivalent.*

(a) M is $\mathcal{S}$-semisimple.

(b) $M = \bigoplus \mathcal{T}$ for some set of $\mathcal{T}$ of R-submodules of M with $\mathcal{T} \subseteq \mathcal{S}$.

(c) $M = \sum \mathcal{T}$ for some set of $\mathcal{T}$ if R-submodules with $\mathcal{T} \subseteq \mathcal{S}$.

(d) $M \cong \bigoplus \mathcal{T}$ for some subset of $\mathcal{T}$ of $\mathcal{S}$.

Proof. (a) $\Longrightarrow$ (b): Since M is semisimple $M = \bigoplus \mathcal{T}$ for some set of simple R-submodules of R. Since M is $\mathcal{S}$-semisimple, each $T \in \mathcal{T}$ is contained in $\mathcal{S}$ and so $\mathcal{T} \subseteq \mathcal{S}$. So (b) holds.

(b) $\Longrightarrow$ (c): Obvious.

(c) $\Longrightarrow$ (a): By 7.2.3(i), M is semisimple. By 7.2.3(g), each simple R-submodule is isomorphic to one $T \in \mathcal{T}$ and so is contained in $\mathcal{S}$.

(b) $\Longleftrightarrow$ (d) : Obvious. □

Lemma 7.3.15. *Let R be a ring, $\mathcal{S}$ a class of simple R-module, M an S-homogeneous R module. If N is a $\mathcal{S}$-semisimple, then both N and M/N are $\mathcal{S}$-semisimple. R-modules.*

Proof. By 7.2.3(f), N is semisimple. Any simple R-submodule of N is also an R-submodule of M and so isomorphic to some $S \in \mathcal{S}$.

Let $M = \sum \mathcal{R}$ for some set of simple R-submodules of V. The by 7.2.3(c) $M/N \cong \bigoplus \mathcal{T}$ for some subset $\mathcal{T}$ of $\mathcal{R}$. Each element of $\mathcal{T}$ is contained in $\mathcal{R}$ and so isomorphic to some $S \in \mathcal{S}$. Hence M/N is $\mathcal{S}$-semisimple by 7.3.14(d). □

Remark 7.3.16. *Let R be a ring, M and R-module and $\mathbb{D} = \mathrm{End}_R(M)^{\mathrm{op}}$. Then M is a right $\mathbb{D}$-module via $m\alpha = \alpha m$ for all $m \in R$ and $\alpha \in \mathbb{D}$ and M is a $(R, \mathbb{D})$-bimodule.*

Proof. Since $\mathrm{End}_R(M)$ is subring of $\mathrm{End}(M)$, M is a left $\mathrm{End}_R(M)$-module and so a right $\mathbb{D}$-module. Moreover, for all $r \in R, m \in M$ and $\alpha \in \mathbb{D}$ we have

$$r(m\alpha) = r(\alpha m) = r(\alpha m) = r(m\alpha)$$

and so M is a $(R, \mathbb{D})$-bimodule. □

Lemma 7.3.17. *Let R be a ring, S a simple R-module and put $\mathbb{D} = \mathrm{End}_R(M)^{\mathrm{op}}$. Let U and $\tilde{U}$ be vector spaces over $\mathbb{D}$ and let V an S-homogeneous R-module.*

(a) $S \otimes_{\mathbb{D}} U$ is an S-homogeneous R-module.

(b) The function

$$U \to \mathrm{Hom}_R(S, S \otimes_{\mathbb{D}} U), u \to (s \to s \otimes u)$$

is an $\mathbb{D}$-isomorphism.

(c) The function

$$\mathrm{Hom}_{\mathbb{D}}(\tilde{U}, U) \to \mathrm{Hom}_R(S \otimes_{\mathbb{D}} \tilde{U}, S \otimes_{\mathbb{D}} U), \alpha \to \mathrm{id}_S \otimes \alpha$$

is a $\mathbb{Z}$-isomorphism.

(d) The function

$$\mathrm{End}_{\mathbb{D}}(U) \to \mathrm{End}_R(S \otimes_{\mathbb{D}} U), \alpha \to \mathrm{id}_S \otimes \alpha$$

is a ring homomorphism

(e) The function

$$S \times \mathrm{Hom}_R(S, V) \to V, (s, \alpha) \to \alpha s$$

is a $(R, \mathbb{Z})$*-tensor product for* $\mathrm{Hom}_R(S, V)$ *and* V *over* $\mathbb{D}$.

(f) The function $U \to S \otimes_R U$ *is inclusion preserving bijection between the* $\mathbb{D}$*-subspaces of* $\mathrm{Hom}_R(S, V)$ *and the R-submodules of V with inverse* $W \to \mathrm{Hom}_R(S, W)$.

(g) $\{\alpha S \mid 0 \neq \alpha \in \mathrm{Hom}_R(S, V)\}$ *is the set simple R-submodules of V.*

Proof. By Schur's Lemma $\mathbb{D}$ is a division ring and so by 3.2.15 U has a $\mathbb{D}$-basis $u = (u_i)_{i \in I}$. Thus by 3.2.3 $U \cong \mathbb{D}_I = \bigoplus_I \mathbb{D}$ as an $\mathbb{D}$-module for some set I. So also $\tilde{I} \cong \mathbb{D}_{\tilde{I}}$ for some set $\tilde{I}$. By 7.3.14 $V \cong S_J$ as an R-module for some set J.

(a) We have

$$S \otimes_{\mathbb{D}} U \cong S \otimes_{\mathbb{D}} \bigoplus_{i \in I} \mathbb{D} = \bigoplus_{i \in I} S \otimes_{\mathbb{D}} \mathbb{D} = \bigoplus_{i \in I} S = S_I$$

and so $S \otimes_{\mathbb{D}} U$ is S-homogeneous by 7.3.14.

(b) Since S is simple $S = Rm$ for all $0 \neq m \in S$. Thus S is a finitely generated R-module and we can apply 3.8.6(c). So

$$\mathrm{Hom}_R(S, S \otimes_{\mathbb{D}} U) \cong \mathrm{Hom}_R(S, \bigoplus_{i \in I} S) = \bigoplus_{i \in I} \mathrm{Hom}_R(S, S) = \bigoplus_{i \in I} \mathbb{D} \cong U$$

Let $u = \sum_{i \in I} d_i u_i \in U$. Under the above chain isomorphism

$$\big(s \to s \otimes u\big) \quad \to \quad \big(s \to (sd_i)_{i \in I}\big) \quad \to \quad (s \to sd_i)_{i \in I} \quad \to \quad (d_i)_{i \in I} \quad \to \quad u$$

So the function in (b) is indeed an isomorphism.

(c) We have

$$\begin{aligned} \mathrm{Hom}_R(S \otimes_{\mathbb{D}} \tilde{U}, S \otimes_{\mathrm{D}} U) &\cong \mathrm{Hom}_R(\bigoplus_{i \in \tilde{I}} S, S \otimes_{\mathbb{D}} U) \cong \bigtimes_{i \in \tilde{I}} \mathrm{Hom}_R(S, S \otimes_{\mathbb{D}} U) \cong \bigtimes_{i \in \tilde{I}} U \\ &\cong \bigtimes_{i \in \tilde{I}} \mathrm{Hom}_{\mathbb{D}}(\mathbb{D}, U) \cong \mathrm{Hom}_{\mathbb{D}}(\bigoplus_{i \in \tilde{I}} \mathbb{D}, U) \cong \mathrm{Hom}_{\mathbb{D}}(\tilde{U}, U) \end{aligned}$$

Let $(\tilde{u})_{i \in \tilde{I}}$ be a $\mathbb{D}$-basis for $\tilde{U}$. Let $\alpha \in \mathrm{Hom}_{\mathbb{D}}(U, \tilde{U})$ and define for $i \in \tilde{I}$ define $\alpha_i \in \mathrm{Hom}_{\mathrm{D}}(\mathrm{D}, U)$ by $\alpha(\tilde{u}_i d) = \alpha_i(d)$ for all $d \in D$. Put $v_i = \alpha(\tilde{u}_i) = \alpha_i(1)$. Then under the above chain of isomorphism

$$\begin{aligned} \mathrm{id}_S \otimes \alpha \quad &\to \quad \bigtimes_{i \in I} (\mathrm{id}_S \otimes \alpha_i) \quad \to \quad (\mathrm{id}_S \otimes \alpha_i)_{i \in I} \to (v_i)_{i \in \tilde{I}} \\ &\to \quad (\alpha_i)_{i \in I} \quad \to \quad \bigtimes_{i \in \tilde{I}} \alpha_i \quad \to \quad \alpha \end{aligned}$$

So the function in (c) is indeed an isomorphism.

(d) By (c) applied with $\tilde{U} = 0$ the function is a $\mathbb{Z}$-isomorphism. Let $\alpha, \beta \in \mathrm{End}_{\mathbb{D}}(U)$. Then $(\mathrm{id}_S \otimes \alpha) \circ (\mathrm{id}_S \otimes \beta) = \mathrm{id}_A \otimes (\alpha \circ \beta)$ and so the function a ring homomorphism.

(e) Let $s \in S, \alpha \in \mathrm{Hom}_R(S, V)$ and $d \in \mathbb{D}$. Since S is a (R, D)-bimodule, the opposite version of 3.6.5(a) shows that $\mathrm{Hom}_R(S, V)$ is a left D-module via

$$(d\alpha)s = \alpha(sd)$$

In particular, the function in (e) is $\mathbb{D}$-balanced. The function is also R-linear in the first coordinate and so by 3.6.12(c) there exists an R-linear function $\Phi : S \otimes_{\mathbb{D}} \mathrm{Hom}_R(S, V)$ with $\Phi(s \otimes \alpha) = \alpha s$ for all $s \in S$, $\alpha \in \mathrm{Hom}_R(S, V)$. T

$$S \otimes_{\mathbb{D}} \mathrm{Hom}_R(S, V) \cong S \otimes_{\mathbb{D}} \mathrm{Hom}_R\big(S, \bigoplus_{j\in J} S\big) \cong \bigoplus_{j\in J} \big(S \otimes_{\mathbb{D}} \mathrm{Hom}_{\mathbb{R}}(S, S)\big) = \bigoplus_{j\in J} (S \otimes_{\mathbb{D}} \mathbb{D}) = \bigoplus_{j\in J} S \cong V$$

Let $\tau : V \to S_I$ be an R-isomorphism, $s \in S$ and $\alpha \in \mathrm{Hom}_R(S)$. For $j \in J$ let $\tau_j = \pi_j \circ \tau$. So $\tau v = (\tau_j v)_{j\in J}$. Note also that $\tau_j \circ \alpha \in \mathrm{End}_R(S) = D$ and so $s(\tau_j \circ \alpha) = (\tau_j \circ \alpha)s = \tau_j(\alpha s)$. Thus the above chain of isomorphism:

$$s \otimes \alpha \quad \to \quad s \otimes \tau \circ \alpha \quad \to \quad \big(s \otimes (\tau_j \circ \alpha)\big)_{j\in J} = \big(s(\tau_j \circ \alpha)\big)_{j\in J} = \big(\tau_j(\alpha s)\big)_{j\in J} \quad \to \quad \alpha a$$

So Φ is an isomorphism and (e) is proved.

(f): By (e) $V = S \otimes_{\mathbb{D}} \mathrm{Hom}_R(S, V)$. So if U is a D-submodule of $\mathrm{Hom}_R(S, V)$, then $S \otimes_{\mathrm{D}} U$ is and R-submodule of V. Also if W is an R-submodule of V, $\mathrm{Hom}_{\mathbb{R}}(S, W)$ is D-submodule of $\mathrm{Hom}_R(S, V)$.

Let $u \in U$. Then $u \in \mathrm{Hom}_R(S, V)$. Let $s \in S$. Then by (e), $s \otimes u = us$. So function $s \to (s \otimes u)$ is just u. Thus the isomorphism in (b) is the identity function on U. Hence $U = \mathrm{Hom}_R(S, S \otimes_{\mathrm{D}} U)$.

By 7.3.15 W is S-homogeneous. So (e) applied with W in place of V gives $S \otimes_{\mathrm{D}} \mathrm{Hom}_R(S, W) = W$. So the functions in (f) are inverse to each other. □

Proposition 7.3.18. *Let R be a ring and $\mathcal{S}$ a set of representatives for the simple R-modules. Let M be an R-module, N an R-submodule of M and $\mathcal{P} \subseteq \mathcal{S}$. For $S \in \mathcal{S}$ let M_S be the sum of the R-submodules of M isomorphic to S. Define $M_{\mathcal{P}} = \sum_{S\in\mathcal{S}} M_S$, so $M_{\mathcal{P}}$ is the sum of R-submodules isomorphic to some member of $\mathcal{P}$.*

(a) N-is $\mathcal{P}$-semisimple of only if $N \leq M_{\mathcal{P}}$.

(b) Let $S \in \mathcal{S}$. Then N is S-homogeneous if and only if $N \leq M_S$.

(c) N is a semisimple R-module if and only if $N \leq M_{\mathcal{S}}$.

(d) Let $\mathcal{Q} \subseteq \mathcal{S}$. Then

$$M_{\mathcal{P}} \cap M_{\mathcal{Q}} = M_{\mathcal{P} \cap \mathcal{Q}} \qquad \textit{and} \qquad M_{\mathcal{P} \cup \mathcal{Q}} = M_{\mathcal{P}} + M_{\mathcal{Q}}.$$

(e) $M_{\mathcal{P}} = \bigoplus_{S \in \mathcal{P}} M_S$.

(f) $N_{\mathcal{P}} = M_{\mathcal{P}} \cap U$.

(g) If N is semisimple, then

$$N = \bigoplus_{S \in \mathcal{S}} (M_S \cap N)$$

Proof. (a) By 7.3.14 N is $\mathcal{P}$-homogeneous if and only if N is the sum of submodules isomorphic to a member of $\mathcal{P}$. Hence $M_{\mathcal{P}}$ is $\mathcal{P}$-semisimple and contains any $\mathcal{P}$-semisimple R-submodule of M. By 7.3.15 any submodule of the $\mathcal{P}$-semisimple module $M_{\mathcal{P}}$ is $\mathcal{P}$-semisimple.

(b) N is S-homogeneous if and only if N is $\{S\}$-semisimple. So (a) implies (b).

(c) N is semisimple if and only if N is $\mathcal{S}$-semisimple. So (a) implies (c).

(d) Observe that N is $\mathcal{P} \cap \mathcal{Q}$-semisimple if and only if N is $\mathcal{P}$-semisimple and $\mathcal{Q}$-semisimple. Thus by (a), $N \leq M_{\mathcal{P} \cap \mathcal{Q}}$ if and only if $N \leq M_{\mathcal{P}} \cap M_{\mathcal{Q}}$. Thus $M_{\mathcal{P} \cap \mathcal{Q}} = M_{\mathcal{P}} \cap M_{\mathcal{Q}}$. The second statement in (d) follows immediately from the definition of $\mathcal{P} \cup \mathcal{Q}$.

(e) By definition $M_{\mathcal{P}} = \sum_{S \in \mathcal{P}} M_S$. Let $S \in \mathcal{P}$. Since $\{S\} \cap (\mathcal{P} \setminus \{S\} = \varnothing$, (d) gives

$$M_S \cap \sum_{S \neq T \in \mathcal{P}} M_T = M_{\{S\}} \cap M_{\mathcal{P} \setminus \{S\}} = M_{\varnothing} = 0$$

So (e) holds by definition of an internal direct sum.

(f) Let U be an R-submodule of N. By (a) applied to N and to M, U is $\mathcal{P}$-semisimple if and only if $U \leq N$ and if and only if $U \leq N \cap M_{\mathcal{P}}$. Thus $N_{\mathcal{P}} = N \cap M_{\mathcal{P}}$.

(g) Since N is semisimple, $N = N_{\mathcal{S}}$. By (e) applied to N in place of M, $N = N_{\mathcal{S}} = \bigoplus_{S \in \mathcal{S}} N_S$. By (g), $N_S = M_S \cap N$ and so (g) holds. □

Proposition 7.3.19. *Let R be a ring and $\mathcal{S}$ a set of representatives for the simple R-modules. Let M and N be R-modules. For $S \in \mathcal{S}$ define $\mathbb{D}_S = \operatorname{End}_R(S)^{\text{op}}$ and $\tilde{M}_S = \operatorname{Hom}_S(R, M)$.*

(a) $\operatorname{Hom}_R(M_S, N) = \operatorname{Hom}_R(M_S, N_S)$.

(b) $\tilde{N}_S = \operatorname{Hom}_R(S, N_S)$.

(c) Suppose M is semisimple. Then the function

$$\operatorname{Hom}_R(M, N) \to \bigtimes_{S \in \mathcal{S}} \operatorname{Hom}_R(M_S, N_S), \quad \alpha \to \left(\alpha|_{M_S}\right)_{S \in \mathcal{S}}$$

is a $\mathbb{Z}$-isomorphism and

$$\mathrm{Hom}_R(M,N) \cong \bigtimes_{S\in\mathcal{S}} \mathrm{Hom}_{\mathbb{D}_S}(\tilde{M}_S, \tilde{N}_S)$$

as abelian groups.

(d) Suppose M is semisimple. Then the function

$$\mathrm{End}_R(M) \to \bigoplus_{S\in\mathcal{S}} \mathrm{Hom}_R(M_S), \quad \alpha \to \left(\alpha|_{M_S}\right)_{S\in\mathcal{S}}$$

is a ring isomorphism and

$$\mathrm{End}_R(M) \cong \bigoplus_{S\in\mathcal{S}} \mathrm{End}_{\mathbb{D}_S}(\tilde{M}_S)$$

as rings.

Proof. (a) Let $\alpha \in \mathrm{Hom}_R(M_S, N)$. Then $\mathrm{Im}\, a \cong M_S/\ker\alpha$. Since M_S is S-homogeneous, 7.3.15 shows that $M_S/\ker\alpha$ is S-homogeneous. Hence also $\mathrm{Im}\,\alpha$ is S-homogeneous. Thus 7.3.18(b) shows that $\mathrm{Im}\,\alpha \leq N_S$.

(b) Follows from (a) applied with $M = S$.

(c) Since M is semisimple, 7.3.18(g) shows that $M = \oplus_{S\in\S} M_S$. Hence using (a) and 3.8.6(a)

$$\mathrm{Hom}_R(M,N) = \mathrm{Hom}_R(\oplus_{S\in\mathcal{S}}, N) \cong \bigtimes_{S\in\mathcal{S}} \mathrm{Hom}_R(M_S, N) = \bigtimes_{S\in\mathcal{S}} \mathrm{Hom}_R(M_S, N_S)$$

By (b) $\tilde{N}_S = \mathrm{Hom}(S, N_S)$. Since N_S is S-homogeneous 7.3.17(f) show that $N_S = S \otimes_{\mathbb{D}_S} \tilde{N}_S$. By symmetry $M_S = S \otimes_{\mathbb{D}_S} \tilde{M}_S$ and so by 7.3.17(d)

$$\mathrm{Hom}_R(M_S, N_S) \cong \mathrm{End}_{\mathbb{D}_S}(M_S, N_S)$$

Thus (c) holds.

(d) follows (c) and observing that the relevant functions are multiplicative homomorphism. □

Definition 7.3.20. *Let R be ring.*

(a) Let M be an R-module. A submodule N of M is called regular if $M = \langle RM\rangle + N$. $\mathrm{J}_M(R)$ is the intersection of the regular maximal R-submodules of M, with $\mathrm{J}_M(R) = M$ if M has no regular maximal R-submodule. $\mathrm{J}_M(R)$ is called the Jacobson radical of the R-module M.

(b) Define

$$\mathrm{J}(R) = \bigcap\{\mathrm{Ann}_R(S) \mid S \text{ a simple } R\text{-module}\}$$

$\mathrm{J}(R)$ is called the Jacobson radical of R.

Remark 7.3.21. *Let R be ring.*

(a) *Let M be an R-module and N a maximal R-submodule if M. Then N is a regular R-submodule if and only if $RM \nsubseteq N$, if and only if M/N is simple, and if and only if $\mathrm{Ann}_R(M/N) \neq R$.*

(b) *Suppose R has an identity and I is maximal left ideal in R. Then $\mathrm{Ann}_R(R/I) \leq I$.*

Proof. (a) Since N is maximal R-submodule of R, either $M = \langle RM\rangle + N$ or $RM \subseteq N$. Thus N is regular if and only if $RM \nsubseteq N$, if and only if $\mathrm{Ann}_R(M/N) \neq R$, if and only if $R(M/N) \neq 0$ and if and only if M/N is simple.

(b) Just observe that $I = \mathrm{Ann}_R(1 + I/I)$. □

Lemma 7.3.22. *Let R be a ring and M an R-module.*

(a) *Let I be an ideal of R with $I \leq \mathrm{Ann}_R(M)$ and note that M is an R/I module. Then*

$$\mathrm{J}_M(R) = \mathrm{J}_M(R/I).$$

(b) *Let U be an R-submodule of M. Then*

$$\mathrm{J}_{M/U} \leq (\mathrm{J}_M(R) + U)/U$$

and if $U \leq \mathrm{J}_M(R)$ then

$$\mathrm{J}_{M/U} = \mathrm{J}_M(R)/U.$$

In particular, $\mathrm{J}_{M/\mathrm{J}_M(R)}(R) = 0$.

(c) *Let I be an ideal of R. Then*

$$\mathrm{J}(R/I) \leq \mathrm{J}(R) + I/I,$$

and if $I \leq \mathrm{J}(R)$, then

$$\mathrm{J}(R/I) = \mathrm{J}(R)/I.$$

In particular, $\mathrm{J}(R/\mathrm{J}(R)) = 0$.

Proof. (a) Just note that a regular maximal R-submodule of M is the same as regular maximal R/I-submodule of M.

(b) Let N be an R-submodule of M with $U \leq N \leq M$. Then U is maximal regular submodule of M if and only if N/U is regular maximal regular R-submodule of M/N. Taking intersection shows that the first statement in (b) holds. If $U \leq \mathrm{J}_M(R)$ then $U \leq N$ for all regular maximal submodule of M and so (b) holds.

(c) Note that every simple R/I module is also a simple R-module. So the first statements holds. If $I \leq \mathrm{J}(R)$, then every simple R-module is also an R/I module and so (c) holds. □

Lemma 7.3.23. *Let R be a ring and M an R-module.*

(a) *Then* $\mathrm{J}_M(R) = 0$ *if and only if M isomorphic to a subdirect product of simple R-modules, that is if and only if there exists family* $(S_i)_{I\in I}$ *of simple R-modules and a 1-1 R-linear function* $\phi : M \to \times_{i\in I} S_i$ *such that* $\pi_i \circ \phi : M \to S_i$ *is onto for all* $i \in I$.

(b) $J_M(R) = 0$ *for all semisimple R-modules.*

Proof. (a) Let $\mathcal{B}$ be the set regular maximal R-submodules of M. Then $\mathrm{J}_M(R) = \bigcap \mathcal{B}$.

Suppose first that $\mathrm{J}_M(R) = 0$ and let $\mathcal{B}$ be the set regular maximal R-submodules of M. Define

$$\phi : M \to \bigtimes_{B\in\mathcal{B}} M/M_B, m \to (m + B)_{B\in\mathcal{B}}$$

Then

$$\ker\phi = \bigcap_{B\in\mathcal{B}} B = \mathrm{J}_M(R) = 0$$

Hence ϕ is 1-1. Also M/B is a simple R-module and $\pi_B \circ \phi$ is onto for all $B \in \mathcal{B}$. Thus M is isomorphic to a subdirect product of simple R-modules.

Suppose next that $(S_i)_{i\in I}$ is family of simple R-modules and $\phi : M \to \times_{I\in I} S_i$ is 1-1 R-linear map such that $\pi_i \circ \phi$ is onto for all $i \in I$. Then $S_i = \mathrm{Im}(\pi_i \circ \phi) \cong M/\ker(\pi_i \circ \phi)$ is a simple R-module and so $\ker(\pi_i \circ \phi)$ is a regular maximal R-submodule of M. Moreover

$$\mathrm{J}_M(R) = \bigcap \mathcal{B} \subseteq \bigcap_{i\in I} \ker(\pi_i \circ \phi) = \ker\phi = 0.$$

and so $\mathrm{J}_M(R) = 0$.

(a) A semisimple R-module is a direct sum of simple R-modules and so also a subdirect product of semisimple R-modules. Thus (a) follows from (b). □

Lemma 7.3.24. *Let R be a ring. Let* $\mathcal{S}$ *be set of representatives for the isomorphism classes of simple R-modules. Then*

$$\mathrm{J}(R) = \bigcap\{\mathrm{Ann}_R(S) \mid S \text{ a minimal } R\text{-module}\} \qquad \textit{and} \qquad \mathrm{J}(R) = \mathrm{Ann}_R(\bigoplus \mathcal{S})$$

In particular, $\mathrm{J}(R) = 0$ *if and only if R has a faithful semisimple R-module.*

Proof. The first statement holds since $\mathrm{Ann}_R(S) = R$ for all minimal R-modules. For the second just observe that $\mathrm{Ann}_R(\bigoplus \mathcal{S}) = \bigcap_{S\in\mathcal{S}} \mathrm{Ann}_R(S)$. □

Lemma 7.3.25. *Let R be a ring. Then* $\mathrm{J}_R(R) \le \mathrm{J}(R)$ *with equality if R has an identity.*

Proof. Let M be simple R-module and $0 \neq m \in R$. Then $R/\mathrm{Ann}_R(m) \cong Rm = M$ is simple and so $\mathrm{Ann}_R(m)$ is a regular maximal R-submodule of R. So $\mathrm{J}_R(R) \le \mathrm{Ann}_R(m)$ and hence $\mathrm{J}_R(R) \le \mathrm{Ann}_R(M)$ and $\mathrm{J}_R(R) \le \mathrm{J}(R)$. Suppose now that R has an identity and let I be (regular) maximal submodule of R. Then R/I is a simple R-module and so $\mathrm{J}(R) \le \mathrm{Ann}_R(R/I) \le \mathrm{Ann}_R(1 + I/I) = I$. So $\mathrm{J}(R) \le \mathrm{J}_R(R)$. □

Theorem 7.3.26 (Artin-Wedderburn)**.** *Let R be an Artinian ring with $\mathrm{J}(R) = 0$. Let $\mathcal{S}$ be set of representatives for the isomorphism classes of simple R-modules. Put $M = \bigoplus \mathcal{S}$ and $\mathbb{D} = \mathrm{End}_R(M)$. For $S \in \mathcal{S}$ put $\mathbb{D}_S = \mathrm{End}_R(S)^{\mathrm{op}}$ and $n_S = \dim_{\mathbb{D}_S} S$. Then $\mathcal{S}$ is finite and*

$$R \cong R|_M = \mathrm{End}_{\mathbb{D}}(M) \cong \bigoplus_{S \in \mathcal{S}} \mathrm{End}_{\mathbb{D}_S}(S) \cong \bigoplus_{S \in \mathcal{S}} \mathrm{M}_{n_S n_S}(\mathbb{D}_S)$$

where all the isomorphism are ring isomorphism.

Proof. By 7.3.19(d) $\mathrm{End}_R(M) \cong \bigoplus_{S \in \mathcal{S}} \mathrm{End}_R(S)$ and so $\mathbb{D} \cong \bigoplus_{S \in \mathcal{S}} \mathbb{D}_S$. It follows that M_S is maximal homogeneous $\mathbb{D}$-submodule of M and applying 7.3.19(d) to $\mathbb{D}$ in place of R the function

$$\mathrm{End}_{\mathbb{D}}(M) \to \bigoplus_{S \in \mathcal{S}} \mathrm{End}_{\mathbb{D}_S} S, \alpha \to (\alpha|_{M_S})_{S \in \mathcal{S}}$$

is ring isomorphism.

Let $S \in \mathcal{S}$. Then by 7.3.5 n_S is finite and hence by 7.1.13 $R/\mathrm{Ann}_R(S) \cong R|_S = \mathrm{End}_{\mathbb{D}_S}(S)$, $R/\mathrm{Ann}_R(S)$ has an identity, $R/\mathrm{Ann}_R(S)$ is a simple ring and any simple $R/\mathrm{Ann}_R(S)$ -module is isomorphic to S. In particular, since R has an identity, $R = R^2 + \mathrm{Ann}_R(S)$.

Let $S, T \in \mathcal{S}$. If $\mathrm{Ann}_R(S) \leq \mathrm{Ann}_R(T)$. Then both T and S are simple modules for $R/Ann_R(S)$. Thus S and T are isomorphic as $R/\mathrm{Ann}_R(S)$-module and so also as R-modules. Thus $S = T$. So if $S \neq T$ then $\mathrm{Ann}_R(T) < \mathrm{Ann}_R(S) + \mathrm{Ann}_R(T)$ and since $R/\mathrm{Ann}_R(T)$ is a simple ring $R = \mathrm{Ann}_R(S) + \mathrm{Ann}_R(T)$.

Since $\mathrm{J}(R) = 0$, $\bigcap_{S \in \mathcal{S}} \mathrm{Ann}_R(S)$, The Chinese remainder theorem 2.4.23 now shows that the function

$$R \to \bigoplus_{S \in \mathcal{S}} R/\mathrm{Ann}_R(S), \quad r \to (r + \mathrm{Ann}_R(S))_{S \in \mathcal{S}}$$

is an isomorphism. Thus

$$R \cong \bigoplus_{S \in \mathcal{S}} R/\mathrm{Ann}_R(S) \cong \bigoplus_{S \in \mathcal{S}} \mathrm{End}_{\mathbb{D}_S}(S) \cong \mathrm{End}_{\mathbb{D}}(M)$$

Note the composition of the isomorphism is just homomorphism from R to $\mathrm{End}(M)$ given by ring action of R on M and so has image $R|_M$. Thus $R|_M = \mathrm{End}_D(M)$.

Finally, $\mathrm{End}_{\mathbb{D}_S}(S) \cong \mathrm{M}_{n_S n_S}(\mathbb{D}_S)$ and so all parts of the Theorem are proved.

□

Lemma 7.3.27. *Let R be a ring, I a nilpotent ideal in R and S simple R-module. Then $IS = 0$. In particular, $I \leq \mathrm{J}(R)$.*

Proof. Since I is nilpotent, $I^n = 0$ for some $n \in \mathbb{Z}^+$. Hence also $I^n S = 0$ and we can choose $m \in \mathbb{Z}^+$ minimal with $I^m S = 0$. If $m = 1$, then $IS = 0$. So suppose $m = k + 1$ for some $k \in \mathbb{Z}^+$. By minimality of m, $I^k S \neq 0$. Note that $\langle I^k S \rangle$ is an R-submodule of S and since S is simple, $S = \langle I^k S \rangle$. Thus

$$IS \subseteq \langle IS \rangle = \langle II^k S \rangle = \langle I^m S \rangle = \langle 0 \rangle = 0$$

and the lemma holds. □

Proposition 7.3.28. *Let R be an Artinian ring. Then $\mathrm{J}(R)$ is nilpotent, that is $\mathrm{J}(R)^n = 0$ for some $n \in \mathbb{N}$.*

Proof. Put $J = \mathrm{J}(R)$ and choose $n \in \mathbb{N}$ with $K := \langle J^n \rangle$ minimal. If $K^2 = 0$, then $J^{2n} = 0$ and J is nilpotent. So suppose for a contradiction that $K^2 \neq 0$. Put $A := \{a \in K \mid Ka = 0\} = \mathrm{Ann}_K(K)$. Then A is an ideal in K with $A \neq K$ and we can choose left ideal L of R in K minimal with $A \neq L$. Then either L/A is a simple R-module or $RL \subseteq A$. In either case $JL \subseteq A$ and so $KJL = 0$. Thus also $\langle KJ \rangle L = 0$. By minimality of K, $K = \langle J^{n+1} \rangle = \langle KJ \rangle$. Thus $KL = 0$, contrary to the choice of L. □

Proposition 7.3.29. *Let R be a ring with identity. Then the following statements are equivalent:*

(a) R is semisimple R-module (by left multiplication).

(b) R is direct sum a finite family of simple R-modules.

(c) R is Artinian and $\mathrm{J}(R) = 0$.

(d) There exists a finite set $\mathcal{M}$ of maximal left ideals with $\bigcap \mathcal{M} = 0$.

(e) All unitary R-modules are semisimple.

(f) All short exact sequence of unitary R-modules split.

(g) All unitary R-modules are projective.

(h) All unitary R-modules are injective.

(i) Each maximal R-submodule of R is a direct summand of R (as an R-module).

Proof. (a) $\Longrightarrow$ (b): Suppose R is semisimple R-module. Then $R = \bigoplus \mathcal{S}$ for some set of $\mathcal{S}$ if simple R-submodules of R, Then $1_R \sum_{S \in \mathcal{S}} e_S$ for some almost zero family $(e_s)_{s \in §}$ with $e_s \in S$ for all $s \in \mathcal{S}$. Put $\mathcal{T} = \{S \in \mathcal{S} \mid e_S \neq 0\}$. Then $1_R = \sum_{T \in \mathcal{T}} e_t$ and so $R = R1_R \subseteq \sum_{T \in \mathcal{T}} Re_t \subseteq \sum \mathcal{T}$. Hence $R = \bigoplus \mathcal{T}$ and (b) holds.

(b) $\Longrightarrow$ (c): Let $\mathcal{S}$ be a finite set of simple R-submodules of R with $R = \bigoplus \mathcal{S}$. Then R is a semisimple R module and since R has an identity, R is a faithful R-module. Hence by 7.3.24 $\mathrm{J}(R) = 0$.

Let I be an R-submodule of R. Then by 7.2.3(e), $I \cong \bigoplus \mathcal{T}$ for some subset $\mathcal{T}$ of $\mathcal{S}$. Define $\deg(I) = |\mathcal{T}|$ and note that by 7.3.12, this does not depended on the choice of $\mathcal{T}$. We claim that $\deg(I) < \deg(K)$ for all R-submodules K of I with $I < K$. Indeed by 7.2.3(f), K is semisimple R-module and so by 7.2.3(a), $K = I \oplus L$ for some R-submodule L of K. It follows that $\deg(K) = \deg(I) + \deg(L) > \deg I$.

Now let $\mathcal{I}$ be any non-empty set of left ideals in R. Choose $I \in \mathcal{I}$ with $\deg I$ minimal. The claim implies that I is minimal element of $\mathcal{I}$ and so R is Artinian.

(c) $\Longrightarrow$ (d): Let $\mathcal{B}$ be the set of maximal left ideal of R. Then

$$\bigcap \mathcal{B} \subseteq \mathrm{J}_R(R) \leq \mathrm{J}(R) = 0$$

Since R is Artinian we can choose a finite subset $\mathcal{M}$ of $\mathcal{B}$ with $\bigcap \mathcal{M}$ minimal. Then for all $B \in \mathcal{B}$,

$$B \supseteq \bigcap \left(\mathcal{M} \cup \{B\}\right) \subseteq \bigcap \mathcal{M}.$$

The minimality of $\bigcup \mathcal{M}$ shows that $\bigcap \mathcal{M} \subseteq B$ and so $\bigcap \mathcal{M} \subseteq \bigcap \mathcal{B} = 0$.

(d) $\Longrightarrow$ (a): Define

$$\phi : R \to \bigtimes_{M \in \mathcal{M}} R/M, r \to (r + M)_{M \in \mathcal{M}}.$$

Then ϕ is R-linear and $\ker \phi = \bigcap \mathcal{M} = 0$. So ϕ is 1-1. Since R as an identity, each R/M, $M \in \mathcal{M}$ is a simple R-module. Since $\mathcal{M}$ is finite we conclude that $\bigtimes_{M \in \mathcal{M}} R/M = \bigoplus_{M \in \mathcal{M}} R/M$ is semisimple. Hence by 7.2.3(f) also $\phi(R)$ is semisimple. Since ϕ is 1-1 this shows that R is semisimple as an R-module.

(a) $\Longrightarrow$ (e): Let T be the sum of simple M-submodules of R. Then by 7.2.3(i), T is a semisimple R-module and so it suffices to show that $m \in T$ for all $0 \neq m \in M$. Since M is unitary $m \in Rm$. Now $Rm \cong R/\mathrm{Ann}_R(m)$. Since R is semisimple, 7.2.3(c) shows that $R/\mathrm{Ann}_R(m)$ is semisimple. So $Rm \leq T$ and $m \in T$.

(e) $\Longrightarrow$ (f): Let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact of sequence of unitary R-modules. If (e) holds, then B is a semisimple R-module and so by 7.2.3(a), $\mathrm{Im}\, f$ is a direct summand of B. Hence by 3.5.9 the short exacts sequence splits.

(f) $\Longleftrightarrow$ (g) : Note that (f) holds if and only if for all unitary R-modules C all short exact sequences

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

of unitary R-modules split. By 3.7.6 this holds if an only if all unitary R-modules C are projective.

(f) $\Longleftrightarrow$ (h) : Note that (f) holds if and only if for all unitary R-modules A all short exact sequences

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

of unitary R-modules split. By 3.7.21 this holds if an only if all unitary R-modules A are injective.

(f) $\Longrightarrow$ (i): Let M be maximal R-submodule of R. Then by assumption the short exact sequence $0 \to M \to R \to R/A \to 0$ splits and so by 3.5.9, M is a direct summand of R.

(i) $\Longrightarrow$ (a): Let T be the sum of the simple R-submodules of R. Suppose that $T \neq R$. Since R has an identity, T is contained in a maximal left ideal M if R. By assumption $R = M \oplus S$ for some R-submodule S of R. Then $S \cong R/M$ is simple and so $S \leq T$. Then the $S \leq T \cap S \leq M \cap S$, a contradiction.

□

Lemma 7.3.30. *Let R be a ring and $\mathbb{F}$ a subring of R. Suppose that $\mathbb{F}$ is a division ring and R is a finite dimensional vector space over $\mathbb{F}$ as $\mathbb{F}$-module by left multiplication.*

(a) R is an Artinian ring.

(b) Any simple R-module is, as an $\mathbb{F}$-module, a finite-dimensional vector space.

Proof.

Let $\mathcal{M}$ be non-empty set of left ideal in R. Then each $M \in \mathcal{M}$ is $\mathbb{F}$-subspace of R. Since R is finite dimensional over R we can choose $M \in \mathcal{M}$ with $\dim_{\mathbb{F}}$ minimal. Then M is a minimal element of $\mathcal{M}$ and so $\mathcal{M}$ is finite dimensional.

Let S be a simple R-module and choose $0 \neq s \in S$. Then $S \cong R/\mathrm{Ann}_R(s)$. Since R is a finite dimensional $\mathbb{E}$-space also $R/\mathrm{Ann}_R(s)$ and S are finite dimensional $\mathbb{F}$-spaces. □

Definition 7.3.31. *Let $\mathbb{F}$ be a field. An $\mathbb{F}$-algebra is a ring R with identity such that $\mathbb{F}$ is a subring of $\mathrm{Z}(R)$ and $1_{\mathbb{F}} = 1_{\mathbb{R}}$. R is called a finite dimensional $\mathbb{F}$-algebra if R is finite-dimensional as $\mathbb{F}$-module by left multiplication.*

Lemma 7.3.32. *Let $\mathbb{D}$ be a division ring and $\mathbb{F}$ an algebraically closed subfield of $\mathrm{Z}(\mathbb{D})$. If $\dim_{\mathbb{F}} \mathbb{D}$ is finite then $\mathbb{F} = \mathbb{D}$.*

Proof. Let $d \in \mathbb{D}$. Since $da = ad$ for all $d \in \mathbb{D}$ we conclude from 2.2.19 that the function

$$\Phi : \mathbb{F}[x] \to \mathbb{D}, f \to f(d)$$

is a homomorphism. Since $\mathbb{F}[x]$ is infinite dimensional over $\mathbb{F}$ and $\mathbb{D}$ is finite dimensional Φ is not 1-1. So we can choose $0 \neq f \in \Phi$ of minimal degree with $f(d) = 0$. Then $\deg f \neq 0$ and since f is algebraically closed, $f = (x - a) \cdot g$ for some $g \in \mathbb{F}[x]$. By minimality $g(d) \neq 0$. Since $0 = f(d) = (d - a) \cdot g(a)$ and $\mathbb{D}$ is a division ring we conclude that $d - a = 0$ and so $d = a \in \mathbb{F}$. □

Lemma 7.3.33. *Let $\mathbb{F}$ be a field and R a finite dimensional $\mathbb{F}$-algebra. Let $\mathcal{S}$ be set of representatives for the simple R-modules. Let $S \in \mathcal{S}$. Put $\mathbb{D}_S = \mathrm{End}_R(S)^{\mathrm{op}}$, $n_S = \dim_{\mathbb{D}_S} S$ and let $\mathbb{F}|_S$ be the image of $\mathbb{F}$ in $\mathrm{End}(S)$.*

(a) $\mathbb{F} \cong \mathbb{F}|_S$ as a ring, $\mathbb{F}|_S \leq \mathrm{Z}(\mathbb{D}_S)$ and $\mathbb{D}_S$ is finite dimensional over $\mathbb{F}|_S$.

(b) If $\mathbb{F}$ is algebraically closed, $\mathbb{F}|_S = \mathbb{D}_S$.

(c) If $\mathbb{F}$ is algebraically closed and $\mathrm{J}(R) = 0$ then

$$R \cong \bigoplus_{S \in \mathcal{S}} \mathrm{End}_{\mathbb{F}}(S) \cong \bigoplus_{S \in \mathcal{S}} \mathrm{M}_{n_S n_S}(\mathbb{F})$$

Proof. (a) By 7.3.30(b), S is a finite dimensional vector space over $\mathbb{F}$. Since $S \neq 0$ this shows that S is a faithful S-module and so $\mathbb{F} \cong \mathbb{F}|_S$. For $r \in R$ let $\tilde{r}r : S \to S, s \to rs$ be the image r in $\mathrm{End}(S)$. Let $g \in \mathrm{End}(S)$ and $s \in S$. Then

$$r(gs) = \tilde{r}(gs) = (\tilde{r} \circ g)s \qquad \text{and} \qquad g(rs) = g(\tilde{r})s = (g \circ \tilde{r})s$$

Hence

$$(*) \qquad g \in \mathbb{D}_S \qquad \Longleftrightarrow \qquad \tilde{r} \circ g = g \circ \tilde{r} \text{for all} r \in R$$

Let $f \in \mathbb{F}$. Recall that $\mathbb{F} \leq \mathbb{Z}(R)$. So (*) applied with $g = \tilde{f}$ shows that $\tilde{f} \in \mathbb{D}_S$. Thus $\mathbb{F}|_S \leq \mathbb{D}_S$. Applying (*) with $r = f$ now shows that $\mathbb{F}|_S \leq \mathbb{Z}(\mathbb{D}_S)$.

Since $\mathbb{F} \leq R$, $\mathbb{D}_S = \mathrm{End}_R(S) \leq \mathrm{End}_{\mathbb{F}}(S)$. Since S is finite dimensional over $\mathbb{F}$, also $\mathrm{End}_{\mathbb{F}}(S)$ and $\mathbb{D}_S$ are finite dimensional over $\mathbb{F}$ (and so also over $\mathbb{F}|_S$.

follows from (a) and Lemma 7.3.32.

By 7.3.30(a) R is an Artinin ring. Since $\mathrm{J}(R) = 0$ the Artin-Wedderburn-Theorem 7.3.26 shows that

$$R \cong \bigoplus_{S \in \mathcal{S}} \mathrm{End}_{\mathbb{D}_S}(S) \cong \bigoplus_{S \in \mathcal{S}} \mathrm{M}_{n_S n_S}(\mathbb{D}_S)$$

Thus (c) follows from (b). □

Theorem 7.3.34 (Maschke)**.** *Let $\mathbb{F}$ be a field and G a finite group and put $n = |G|$. Let V be an $\mathbb{F}[G]$-module and W be an $\mathbb{F}[G]$-submodule of V.*

(a) There exists an $\mathbb{F}[G]$-submodule U of V with $W \cap U = \mathrm{Ann}_W(n)$ and $nV \leq W + U$.

(b) If char $\mathbb{F}$ *does not divide n, then W is a direct summand of V as an $\mathbb{F}[G]$-module.*

Proof. Let T be an $\mathbb{F}$-subspace of V with $V = W \oplus T$. Let α be the projection of V on W, so $\alpha|_W = \mathrm{id}_W$ and $\mathrm{Im}\,\alpha = W$. Define

$$\beta : V \to V, v \to \sum_{g \in G} g^{-1}(\alpha(gv))$$

Then β is $\mathbb{F}$-linear and for all $h \in G$.

$$\beta(hv) = \sum_{g \in G} g^{-1}\alpha(ghv) = \sum_{g \in G} hh^{-1}g\alpha(gh)) = h \sum \sum_{g \in G}(gh)\alpha(gh)) = h \sum_{g \in G} g\alpha(gv) = h\beta(v)$$

So β is $\mathbb{F}[G]$-linear. In particular, $U := \ker\beta$ is an $\mathbb{F}[G]$-subspace of V. Let $w \in W$. Then also $gw \in W$ and so $\alpha(gw) = gw$ for all $g \in G$. Then

$$\beta(w) = \sum_{g \in G} g^{-1}\alpha(gw) = \sum_{g \in G} g^{-1}gw = \sum_{g \in G} w = nw$$

So $w \in \ker\alpha$ if and only if $nw = 0$. Thus $U \cap W = \mathrm{Ann}_W(n)$.

Let $v \in V$. Since $\alpha(gv) \in W$ and W is $\mathbb{F}[G]$-submodule, $g^{-1}\alpha(gv) \in W$ and so also $\beta(v) \in W$.

$$\beta(\beta(v)) = n\beta(v) = \beta(nv)$$

Thus $nv - \beta(v) \in \ker\beta$ and $nv = \beta(v) + (nv - \beta(v)) \in \mathrm{Im}\beta + \ker\beta \leq W + U$. So $nV \leq W + U$ and (a) is proved.

(a) Suppose char $\mathbb{F}$ does not divide n. Then $n1_F \neq 0$ and so $(n1_{\mathbb{F}})$ is invertible in $\mathbb{F}$. It follows that $\mathrm{Ann}_V(n) = \mathrm{Ann}_V(n1_{\mathbb{F}}) = 0$ and $nV = (n1_{\mathbb{F}}) = V$. So (a) gives $W \cap U = 0$ and $V = W + U$. So $V = W \oplus U$ and W is a direct summand of V. □

Corollary 7.3.35. *Let* $\mathbb{F}$ *be field and* G *a finite group. Suppose that* char $\mathbb{F} \nmid |G|$. *Then* $\mathbb{F}[G]$ *is an Artinian ring with* $\mathrm{J}(\mathbb{F}[G]) = 0$.

Proof. Note that $\mathbb{F}[G]$ is a finite dimensional $\mathbb{F}$-algebra and so by 7.3.30, $\mathbb{F}[G]$ is an Artinian ring. By 7.3.34(b) any maximal left ideal in $\mathbb{F}[G]$ is a direct summand of $\mathbb{F}[G]$ has left $\mathbb{F}[G]$-module and so 7.3.29 implies that $\mathrm{J}(\mathbb{F}[G]) = 0$. □

Chapter 8

Representations of finite groups

8.1 Semisimple Group Algebra

Definition 8.1.1. *Let R be a ring and V and W R-modules.*

(a) $\mathrm{FHom}_R(V,W) = \{f \in \mathrm{Hom}_R(V,W) \mid \mathrm{Im}\, f \subseteq \langle I\rangle_R$ *for some finite* $I \subseteq W\}$.

(b) $\mathrm{FEnd}_R(V) = \mathrm{FHom}_R(V,V)$.

Lemma 8.1.2. *Let R,S,T be rings, V an (R,S)-bimodule and W an (R,T) bimodule. Put* $V^* = \mathrm{Hom}_R(V,R)$.

(a) $\mathrm{FHom}_R(V,W)$ *is an (S,T)-submodule of* $\mathrm{Hom}_R(V,W)$.

(b) There exists a unique $\mathbb{Z}$-linear function

$$\Phi = \Phi(V,W) : V^* \otimes_R W \to \mathrm{FHom}_R(V,W), \text{ with } \alpha \otimes v \ \to \ \big(\ v \to (\alpha v)w\ \big)$$

Moreover Φ is (S,T)-linear.

(c) Let $f : \tilde{V} \to V$ and $h : W \to \tilde{W}$ be R-linear. Put $\tilde{\Phi} = \Phi(\tilde{V},\tilde{W})$. Then

$$\tilde{\Phi}(\alpha \circ f, hw) = h \circ \Phi(\alpha, w) \circ f$$

for all $\alpha \in V^*$ and $w \in W$.

Proof. (a) Let $f,g \in \mathrm{FHom}_R(V,W)$, $s \in S$ and $t \in T$. Then $\mathrm{Im}\, f \subseteq \langle I\rangle_R$ and $\mathrm{Im}\, g \subseteq \langle J\rangle_R$ for some finite subsets I and J is W. Then $\mathrm{Im}(f+g) \subseteq \mathrm{Im}\, f + \mathrm{Im}\, g \leq \langle I \cup J\rangle_R$. $\mathrm{Im}(sf) = f(Vs) \subseteq \mathrm{Im}\, f \subseteq \langle I\rangle R$ and $\mathrm{Im}(ft) = (\mathrm{Im}\, f)t \leq \langle I\rangle_R t = \langle It\rangle_R$.

(b) Let $\alpha \in V^*$ and $w \in V$. Since α and $R \to W, r \to rw$ are both R-linear, the composition $\phi(a,w) : V \to W\ v \to (\alpha v)w$ is also R-linear. Note that $\mathrm{Im}(\phi(a,w)) \leq Rw \leq \langle w\rangle_R$ and so $\phi(a,w) \in \mathrm{FHom}_R(V,W)$. So we obtain a function:

$$\phi : V^* \times W \to \mathrm{FHom}_R(V, W), (\alpha, w) \to \phi(a, w)$$

Note that ϕ is $\mathbb{Z}$-bilinear. Let $r \in R$, $s \in S$, $t \in T$, $v \in V$ and w in W. Then

$$\phi(\alpha r, w)v = ((\alpha r)v)w = ((\alpha v)r)w = (\alpha v)(rw) = \phi(\alpha, rw)v$$
$$\phi(s\alpha, w)v = ((s\alpha)v)w = (\alpha(vs))w = \phi(\alpha, w)(vs) = (s\phi(\alpha, w))v$$

and

$$\phi(\alpha, wt)v = (\alpha v)(wt) = ((\alpha v)w)t = (\phi(\alpha, w)v)t = (\phi(\alpha, w)t)v$$

Hence

$$\phi(\alpha r, w) = \phi(\alpha, rw), \qquad \phi(s\alpha, w) = s\phi(\alpha, w) \qquad \phi(\alpha, wt) = \phi(\alpha, w)t$$

So ϕ is (S, R, T)-linear. The uniqueness and existence of Φ now follows from definition of a tensor product. Moreover, by Lemma 3.6.12 $V^* \otimes_R W$ is also an (S, T)-tensor product of V^* and W over R and so Φ is (S, T)-linear.

(c) Let $u \in \tilde{V}$. Then

$$\Big(\tilde{\Phi}(\alpha \circ f, hw)\Big)u = \big((\alpha \circ f)u\big)\big(hw\big) \quad = \big(\alpha(fu)\big)\big(hw\big)\big) \quad = h\Big(\big(\alpha(fu)\big)w\Big)$$
$$= h\Big(\big(\Phi(\alpha, w)\big)(fu)\Big) = \Big(h \circ \Phi(\alpha, w) \circ f\Big)u$$

□

Lemma 8.1.3. *Let R be a ring, V an R-module and W a free R-module with basis $(w_i)_{i \in I}$. Let $\pi_i \in \mathrm{Hom}_R(W, R)$ be defined by $w = \sum_{i \in I}(\pi_i w)w_i$ for all $w \in W$. Let $f \in \mathrm{Hom}_R(V)$ and define $f_i = \pi_i \circ f$.*

(a) $f \in \mathrm{FHom}_R(V, W)$ if and only of $(f_i)_{i \in I}$ is almost 0.

(b) The function

$$\mathrm{FHom}_R(V, W) \to \bigoplus_{i \in I} V^*, f \to (f_i)_{i \in I}$$

is a well defined $\mathbb{Z}$ isomorphism.

(c) The function

$$\Psi : \mathrm{FHom}_R(V, W) \to V^* \otimes W, f \to \sum_{i \in I} f_i \otimes w_i$$

is inverse to the function $\Phi : V^* \otimes_R W, \alpha \otimes w \to (v \to (\alpha v)w)$.

Proof. (a) For $K \subseteq I$ put $W_K = \langle w_k \mid k \in K\rangle_R$. We claim that that $f \in \mathrm{FHom}_R(V,W)$ and only if $\mathrm{Im}\, f \subseteq W_K$ for some finite $K \subseteq I$. The backwards direction is obvious. Suppose now that $\mathrm{Im}\, f \subseteq \langle L\rangle_R$ for some finite subsets L of V. Then for each $l \in L$ the exists a finite subset K_l of I with $l \in W_{K_l}$. Put $K = \bigcup_{l\in L} W_{K_l}$. Then $l \in W_K$ for all $l \in L$ and so $\mathrm{Im}\, f \subseteq \langle L\rangle_R \subseteq W_K$. This proves the claim.

Note that $\mathrm{Im}\, f \subseteq W_K$ if and only if $\pi_i(\mathrm{Im}\, f) = 0$ for all $i \in I \smallsetminus K$ and if and only if $f_i = 0$ for all $i \in I \smallsetminus K$. The above claim now shows that $f \in \mathrm{FHom}_R(V,W)$ if and only if there exists a finite subset K of I with $f_i = 0$ for all $i \in I \smallsetminus K$ and so if and only if $(f_i)_{i\in I}$ is almost trivial. Thus (a) holds.

(b) Since the function $\mathrm{Hom}_R(V,W) \to \times_{i\in I} V^*, f \to (f_i)_{i\in I}$ is an $\mathbb{Z}$-isomorphism, (b) follows from (a).

(c) We have

$$\Phi\big(\sum_{i\in I} f_i \otimes w_i\big)v = \sum_{i\in I}(f_i v)w_i = \sum_{i\in I}(\pi_i(fv))w_i = fv$$

and so $\Phi(\Psi(f)) = f$.

Let $\alpha \in V^*$, $v \in V$ and $w \in W$. Put $f = \Phi(\alpha \otimes w)$.

$$\pi_i(fv) = \pi_i\big((\alpha v)w\big) = (\alpha v)(\pi_i w) = (\alpha \cdot (\pi_i w))v$$

So $f_i = \alpha \cdot (\pi_w)$ and

$$\sum_{i\in I} f_i \otimes w_i = \sum_{i\in I}(\alpha \cdot (\pi_i w)) \otimes w_i = \sum_{i\in I} \alpha \otimes (\pi_i w)w_i = \alpha \otimes \sum_{i\in I}(\pi_i w)w_i = \alpha \otimes w$$

and so $\Psi(\Phi(\alpha \otimes w)) = \alpha \otimes w$. □

Lemma 8.1.4. *Let R be a commutative ring and V a free R-module with basis $(w_i)_{i\in I}$. Let $f \in \mathrm{End}_R(V)$ and let be A the matrix of f with respect to $(w_i)_{i\in I}$.*

(a) There exists a unique $\mathbb{Z}$-linear function

$$\mathrm{tr} : \mathrm{FEnd}_R(V) \to R \textit{ with } (v \to (\alpha v)w) \to \alpha w$$

for all $w \in V$ and $\alpha \in \mathrm{Hom}_R(V,R)$.

(b) Let $g \in \mathrm{FEnd}_R(V)$. Then $\mathrm{tr}(f \circ g) = \mathrm{tr}(g \circ f)$.

(c) Let $h : V \to U$ be an R-isomorphism and $g \in \mathrm{FEnd}_R(V)$. Then $\mathrm{tr}(h \circ g \circ h^{-1}) = \mathrm{tr}(g)$.

(d) $f \in \mathrm{FEnd}_R(V)$ if and only almost all columns of A are zero.

(e) Suppose $f \in \mathrm{FEnd}_R(V)$ and define $\mathrm{tr}(A) = \sum_{i\in I} A_{ii}$. Then $\mathrm{tr}(f) = \mathrm{tr}(A)$.

Proof. (a) Let $r \in R$, $\alpha \in V^*$ and w in V. Since R is commutative,

$$(\alpha r)w = (\alpha w)r = r(\alpha w) = \alpha(rw)$$

and so the function $V^* \times_R V \to R$, $(\alpha, w) \to \alpha w$ is R-balanced. So the exists unique $\mathbb{Z}$-linear function

$$\Lambda : V^* \otimes_R V \to R \quad \text{ with } \quad \alpha \otimes w \to \alpha w$$

for all $\alpha \in V^*$ and $w \in V$. By 8.1.2 there exists a $\mathbb{Z}$ isomorphism

$$\Phi : V^* \times_R V \to \mathrm{Hom}_R(V, W) \quad \text{ with } \quad \alpha \otimes w \ \to \ (v \to (\alpha v)w)$$

Thus (a) holds with $\mathrm{tr} = \Lambda \circ \Phi^{-1}$.

(b) Note that V is an $\big(R, \mathrm{End}_R(V)^{\mathrm{op}}\big)$-bimodule and so by 8.1.2 Φ is $\big(\mathrm{End}_R(V), \mathrm{End}_R(V)\big)$-linear. Hence for all $\alpha \in V^*$, $w \in V$.

$$\mathrm{tr}\big(f \circ \Phi(\alpha \otimes v)\big) = \mathrm{tr}\big(\Phi(\alpha \circ f, v)\big) = (\alpha \circ f)v = \alpha(fv)) = \mathrm{tr}(\Phi(\alpha \otimes fv)) = \mathrm{tr}\big(\Phi(a \otimes v) \circ f\big)$$

The uniqueness assertion in (a) now implies that $\mathrm{tr}(f \circ g) = \mathrm{tr}(g \circ f)$ for all $g \in \mathrm{FEnd}_R(V)$

(c) Put $\tilde{\Phi} = \Phi(U, U)$ and let $\alpha \in V^*$ and $w \in V$. By 8.1.2(c)

$$h \circ \Phi(\alpha, w) \circ h^{-1} = \tilde{\Phi}(\alpha \circ h^{-1}, hw).$$

and so

$$\begin{aligned} \mathrm{tr}\big(h \circ \Phi(\alpha \otimes w) \circ h^{-1}\big) &= \mathrm{tr}\big(\tilde{\Phi}(\alpha \circ h^{-1}, hw)\big) = (\alpha \circ h^{-1})(hw) \\ &= \alpha\big(h^{-1}(hw)\big) \qquad = \alpha(w) = \mathrm{tr}(\Phi(\alpha \otimes w)) \end{aligned}$$

The uniqueness assertion in (a) now implies that $\mathrm{tr}(h \circ g \circ h^{-1}) = \mathrm{tr}(g)$ for all $g \in \mathrm{FEnd}_R(V)$.

(d) Define π_i and f_i as in 8.1.3. Since $fw_i = \sum_{j \in I} A_{ij} w_j$, $f_j w_i = \pi_j(fw_i) = A_{ij}$. Note $f_j = 0$ if and only if $f_j w_i = 0$ for all $i \in I$ and so if and only if column j of A is zero. So by 8.1.3(a), $f \in \mathrm{FEnd}_R(V)$ if and only if almost all columns of A are zero.

(e) By 8.1.3(c) , $f = \Phi\big(\sum_{j \in I} f_j \otimes w_j\big)$ and so and

$$\mathrm{tr}(f) = \sum_{j \in I} f_j w_j = \sum_{j \in J} A_{jj}$$

□

Remark 8.1.5. *Let R be a ring with identity and suppose there exists elements a, b in R such that a is invertible and $ab \neq ba$. Then the trace of the 1-1 matrix $[b]$ is b, while the trace of the 1-1 matrix $[a][b][a]^{-1}$ is aba^{-1}. So for non-commutative ring similar matrix can have distinct trace. In particular, there does not exists a canonical definition of the trace of R-linear functions.*

Hypothesis 8.1.6. *For the remainder of this chapter G is a finite group and $\mathbb{K}$ is an algebraically closed field with* $\mathrm{char}\,\mathbb{K} \nmid |G|$. *$\mathcal{S} = \mathcal{S}(\mathbb{K}[G])$ is a set representatives for the isomorphism classes of simple $\mathbb{K}[G]$ modules. For $\mathcal{S} \in S$ put $d_S = \dim_{\mathbb{K}} S$ and $A_S = \bigcap_{S \neq T \in \mathcal{S}} \mathrm{Ann}_{\mathbb{K}[G]}(T)$. Let e_S is be the multiplicative identity of A_S.*

Let $\mathcal{C}$ be the set of conjugacy classes of G , that is the set of orbits of G acting on G by conjugation. For $H \subseteq G$ put $a_H = \sum_{h \in H} h \in \mathbb{K}[G]$. For $C \in \mathcal{C}$ choose $g_C \in C$.

Theorem 8.1.7. *Let $S \in \mathcal{S}$.*

(a) $\mathrm{J}(\mathbb{K}[G]) = 0$ *and all unitary* $\mathbb{K}[G]$*-modules are semisimple.*

(b) $\mathbb{K}[G] = \bigoplus_{S \in \mathcal{S}} A_S$.

(c) $A_S \cong \mathbb{K}[G]|_S = \mathrm{End}_{\mathbb{K}}(S)$ *is simple ring and* $\dim_{\mathbb{K}} A_S = d_S^2$.

(d) $\mathrm{End}_{\mathbb{K}[G]}(S) = \mathbb{K}\,|_S$ *for all* $S \in \mathcal{S}$.

(e) $|G| = \sum_{S \in \mathcal{S}} d_S^2$.

(f) Then $\mathrm{Z}(A_S) = \mathbb{K}e_S$ *and* $(e_S)_{S \in \mathcal{S}}$ *is a basis for* $\mathrm{Z}(\mathbb{K}[G])$ *over* $\mathbb{K}$

(g) Let $b = \sum_{g \in G} b_g g \in \mathbb{K}[G]$. *Then* $b \in \mathrm{Z}(\mathbb{K}[G])$ *if and only if* $b_g = b_h$ *for any conjugate* $g, h \in G$.

(h) $(a_C)_{C \in \mathcal{C}}$ *is a* $\mathbb{K}$*- basis for* $\mathrm{Z}(\mathbb{K}[G])$.

(i) $|\mathcal{S}| = \dim_{\mathbb{K}} \mathrm{Z}(\mathbb{K}[G]) = |\mathcal{C}|$.

Proof. (a) By 7.3.35 $\mathrm{J}(R) = 0$ and so by 7.3.29 all $\mathbb{K}[G]$-modules are semisimple.

Since $\mathrm{J}(R) = 0$, (b), (c) and (d) follow from 7.3.33(c)

(e) Follows immediately from (b) and (c).

(f) Since $\mathbb{K}$ is commutative, $\mathbb{K}|_S \le \mathrm{End}_{\mathbb{K}}(S)$ and by Exercise 3(d) on Homework 6. $\mathrm{End}_{\mathrm{End}_{\mathbb{K}}(S)}(S) = \mathbb{K}|_S$. Thus $Z(\mathrm{End}_{\mathbb{K}}(S)) = \mathbb{K}|_S = \mathbb{K}_S \mathrm{id}_S$. Since A_S is isomorphic to $\mathrm{End}_{\mathbb{K}}(S)$, this gives $\mathrm{Z}(A_S) = \mathbb{K}e_S$. Using (b) we get

$$\mathrm{Z}(\mathbb{K}[G]) = \mathrm{Z}(\Big(\bigoplus_{S \in \mathcal{S}} A_S\Big) = \bigoplus_{S \in \mathcal{S}} \mathrm{Z}(A_S) = \bigoplus_{S \in \mathcal{S}} Ke_S$$

and so (f) holds.

(g) Let $b = \sum_{g \in G} b_g g \in \mathbb{K}[G]$. Then the following are equivalent:

$$\begin{array}{rl}
b \in \mathrm{Z}(\mathbb{K}[G]) & \\
ab = ba & \forall b \in \mathbb{K}[G] \\
bh = hb & \forall h \in G \\
hbh^{-1} = b & \forall h \in G \\
\sum_{g \in G} b_g hgh^{-1} = \sum_{g \in G} b_g g & \forall h \in G \\
\sum_{g \in G} b_{h^{-1}gh} g = \sum_{b \in G} k_g g & \forall h \in G \\
b_{h^{-1}gh} = k_g & \forall h \in G \\
b_g = b_h & \forall C \in \mathcal{C}, g, h \in C
\end{array}$$

So (g) holds.

(i) follows immediately from (f) and (h). □

Definition 8.1.8. *Let $\alpha \in \mathrm{Hom}(G, \mathbb{K}^\sharp)$, so α is homomorphism form G to the multiplicative group $(\mathbb{K}^\sharp, \cdot)$. The S_α is the $\mathbb{K}[G]$ with $S_\alpha = \mathbb{K}$ as a $\mathbb{K}$-module and $gk = \alpha(g)k$ for all $g \in G$ and $k \in \mathbb{K}$.*

Lemma 8.1.9. *(a) Every 1-dimensional unitary $\mathbb{K}[G]$-module is simple.*

(b) Let S be a 1-dimensional simple $\mathbb{K}[G]$-module. Then there exists a unique $\alpha \in \mathrm{Hom}(G, \mathbb{K}^\sharp)$ with $S \cong S_\alpha$ has $\mathbb{K}[G]$-module.

Proof. (a) A 1-dimensional $\mathbb{K}[G]$-module has no proper $\mathbb{K}$-subspace and so also no proper $\mathbb{K}[G]$-submodules. (b) Pick $0 \neq s \in S$. Let $g \in G$. Since $\dim_{\mathbb{K}} S$ is 1-dimensional here exists $\alpha(g) \in \mathbb{K}^\sharp$ with $gs = \alpha(g)s$. Let $k \in \mathbb{K}$. Since $\mathbb{K} \leq \mathbb{Z}(\mathbb{K}[G])$, $g(ks) = (gk)s = (kg)s = k(ks) = k(\alpha(g)s) = \alpha(g)(ks)$. So $\alpha(g)$ does not depend on the choice of s, the function $S_\alpha \to S, k \to ks$ is a $\mathbb{K}[G]$-isomorphism and α is unique such that $S_\alpha \cong S$. □

Lemma 8.1.10. *Suppose G is abelian.*

(a) $|G| = |\mathcal{C}| = |\mathcal{S}$.

(b) All simple $\mathbb{K}[G]$-modules are 1-dimensional over $\mathbb{K}$.

(c) For each simple $\mathbb{K}[G$-module S there exists a unique $\alpha \in \mathrm{Hom}(G, \mathbb{K}^\sharp)$ with $S \cong S_\alpha$ as an $\mathbb{K}[G]$-module.

(d) $|\mathrm{Hom}(G, \mathbb{K}^\sharp)| = |G|$.

(e) Let V be any unitary $\mathbb{K}[G]$-module. Then there exists a $\mathbb{K}$-basis $(v_i)_{i \in I}$ and a family $(\alpha_i)_{i \in I}$ in $\mathrm{Hom}(G, \mathbb{K}^\sharp)$ with

$$gv_i = \alpha_i(g)v_i$$

for all $g \in G$, $i \in I$. In particular, then matrix of $g|_V$ with respect to $(v_i)_{i \in I}$ is diagonal.

Proof. (a) Since G is abelian, ${}^h g = g$ for all $h, g \in G$ and so $\mathcal{C} = \big\{\{g\} \mid g \in G\big\}$. Thus $|\mathcal{C}| = |G|$. By 8.1.7(i), $|\mathcal{C}| = |\mathcal{S}|$ and so (a) holds.

(b)8.1.7(e), $|G| = \sum_{S \in \mathcal{S}} d_S^2$. Since $d_S \geq 1$ and $|\mathcal{S}| = |G|$ this gives $d_S = 1$ for all $S \in \mathcal{S}$.

(c) By (a) S is 1-dimensional and so (c) follows from 8.1.9

(d) By (c) $|\mathrm{Hom}(G, \mathbb{K}^\sharp)| = |\mathcal{S}$ and so (d) follows from (a).

(e) By 8.1.7(g), V is a semisimple $\mathbb{K}[G]$-module and so $V = \bigoplus_{i \in I} V_i$ for a family $(V_i)_{i \in I}$ of simple R-submodules of V. For $i \in I$ let $0 \neq v_i \in V_i$. By (c) V_i is 1-dimensional over $\mathbb{K}$ and so $(v_i)_{i \in I}$ is a $\mathbb{K}$-basis for V. By (c) $V_i \cong S_{\alpha_i}$ for some $\alpha_i \in \mathrm{Hom}(G, \mathbb{K}^\sharp)$ and so $gv_i = \alpha(g)v_i$. □

Lemma 8.1.11. *Suppose G is abelian and $G = \bigoplus_{i=1}^m G_i$ for some family $(G_i)_{i=1}^n$ of cyclic subgroups of G. Let $g_i \in G$ with $G_i = \langle g_i \rangle$.*

(a) Let $\alpha \in \operatorname{Hom}(G, \mathbb{K}^\sharp)$ and define $\xi_i = \alpha(g_i)$. Then $\xi^{|g_i|} = 1$ and

$$\alpha\Big(\prod_{i=1}^{n} g_i^{l_i}\Big) = \prod_{i=1}^{n} \xi_i^{l_i}$$

for all $l \in \mathbb{Z}^n$.

(b) Let $(\xi_i)_{i=1}^m$ be a family of elements in $\mathbb{K}^\sharp$ with $\xi_i^{|g_i|} = 1$. Define

$$\alpha : G \to \mathbb{K}^\sharp, \prod_{i=1}^{m} g_i^{l_i} \to \prod_{i=1}^{n} \xi_i^{l_i}$$

Then α is a well-defined homomorphism and $\alpha(g_i) = \xi_i$ for all $1 \le i \le m$.

Proof. Readily verified. □

8.2 Characters

Definition 8.2.1. *Let M be a finite dimensional $\mathbb{K}[G]$-submodule. Recall that for $r \in \mathbb{K}[G]$, $r|_M$ is the function*

$$r|_M : \mathrm{M} \to M, m \to rm$$

and note that $r|_M \in \operatorname{End}_{\mathbb{K}}(M)$. Define

$$\operatorname{tr}_M : \mathbb{K}[G] \to \mathbb{K}, r \to \operatorname{tr}(r|_M)$$

and let

$$\chi_M : \mathbb{K}[G] \to \mathbb{K}, g \to \operatorname{tr}(g|_M)$$

be the restriction of tr_M to G. χ_M is called the character of the $\mathbb{K}[G]$-module M.

The $\mathcal{S} \times \mathcal{C}$ matrix

$$[\chi_S(g_C)]_{\substack{S \in \mathcal{S} \\ C \in \mathcal{C}}}$$

is called the character table of G over $\mathbb{K}$.

Definition 8.2.2. *(a) A class function is a function $f : G \to \mathbb{K}$ which is constant on every conjugacy class. (So $f(g) = f(g_c)$ for all $C \in \mathcal{C}$ and $g \in C$.)*

(b) $\operatorname{Fun}_c(G, \mathbb{K})$ denotes the set of all class function.

(c) For any function $f : G \to \mathbb{K}$, $\tilde{f}$ denotes the unique $\mathbb{K}$-linear function

$$\tilde{f} : \mathbb{K}[G] \to \mathbb{K}, \text{ with } \tilde{f}(g) = f(g) \text{ for all } g \in G$$

(So $\tilde{f}\big(\sum_{k_g} g\big) = \sum k_g f(g)$)

Lemma 8.2.3. *Let M be a finite dimensional unitary $\mathbb{K}[G]$-module.*

(a) $\chi_M(1) = \dim_{\mathbb{K}} V$.

(b) Let $\alpha \in \mathrm{Hom}(G, \mathbb{K}^\sharp)$. *Then* $\chi_{S_\alpha} = \alpha$.

(c) Let $g \in G$ *and let* $(\alpha)_{i=1}^m$ *be a family in* $\mathrm{Hom}(\langle g\rangle, \mathbb{K}^\sharp)$ *with* $M \cong \bigoplus_{i=1}^m S_{\alpha_i}$ *as a* $\mathbb{K}[\langle g\rangle]$*-module. Then* $m = \dim_{\mathbb{K}} V$ *and*

$$\chi_M(g) = \sum_{i=1}^m \alpha_i(g)$$

In particular $\chi_M(g)$ *is a sum of* m $|g|$*-th root of unities in* $\mathbb{K}$.

Proof. (a) Since M is a unitary module, $1|_M = \mathrm{id}_M$ and so $\chi(1) = \mathrm{tr}(\mathrm{id}_M) = \dim_{\mathbb{K}} M$.

(b) Note the matrix of $g|_M$ with respect to the basis 1 of S_α is the 1×1- matrix $[\alpha(g)]$. So $\chi_M(g) = \alpha(g)$.

(c) Note that the matrix of g with respect to the standard basis of $\bigoplus_{i=1}^m S_{\alpha_i} = \mathbb{K}^m$ is the diagonal matrix

$$\begin{bmatrix} \alpha_1(g) & 0 & \dots & 0 & 0 \\ 0 & \alpha_2(g) & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \alpha_{m-1}(g) & 0 \\ 0 & 0 & \dots & 0 & \alpha_m(g) \end{bmatrix}$$

and so $\chi_M(g) = \sum_{i=1}^m \alpha_i(g)$. □

Lemma 8.2.4. *Let* $f \in \mathrm{Fun}(G, \mathbb{K})$. *Then* $f \in \mathrm{Fun}_c(G, \mathbb{K})$ *if and only if* $\sum_{g\in G} f(g)g \in \mathrm{Z}(\mathbb{K}(G))$.

Proof. This follows immediately from 8.1.7(g). □

Remark 8.2.5. *By definition* $\mathbb{K}[G]$, *as a set, consists of all almost-zero functions from G to* $\mathbb{K}$. *Since G is finite* $\mathbb{K}[G] = \mathrm{Fun}(G, \mathbb{K})$. *On other words there is no difference between the element* $\sum_{g\in G} k_g g \in \mathbb{K}[G]$ *and the function* $g \to k_g$ *in* $\mathbb{K}$. *8.2.4 now says that* $\mathrm{Fun}_c(G, \mathbb{K}) = \mathrm{Z}(\mathbb{K}[G])$.

Also if $f \in \mathrm{Fun}(G, \mathbb{K}) = \mathbb{K}[G]$, *then* $\tilde{f}$ *is in* $\mathbb{K}[G]^* = \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}[G], \mathbb{K})$ *and the function*

$$\mathbb{K}[G] \to \mathbb{K}[G]^*, f \to f^*$$

is $\mathbb{K}$*-isomorphism.*

Lemma 8.2.6. *Let M be a* $\mathbb{K}G$*-module.*

(a) χ_M *is a class function.*

(b) If N is an $\mathbb{K}G$*-module isomorphic to M, then* $\chi_N = \chi_M$.

(c) If $(M_i)_{i=1}^m$ be a family of R-submodules of M with $M = \bigoplus_{i=1}^m M_i$. Then

$$\chi_M = \sum_{i=1}^m \chi_{M_i}$$

Proof. (a) Let $h, g \in G$. Since $*_M$ is a homomorphism and using 8.1.4(c) we have

$$\chi_M({}^h g) = \operatorname{tr}\big(h|_M \circ g|_M \circ h|_M^{-1}\big) = \operatorname{tr}\big(g|_M\big) = \chi_M(g)$$

(b) Let $\phi : M \to N$ be $\mathbb{K}[G]$-isomorphism. Then $g|N = \phi \circ g|_M \circ \phi^{-1}$ and a similar calculation as in (a) proved (b).

(c) For $g \in G$. For $1 \leq i \leq m$ let $\mathcal{B}_i$ be a basis for M_i and A_i matrix of $g|_{M_i}$ with respect to $\mathcal{B}_i$. Put $\mathcal{B} = \bigcup_{i=1}^m \mathcal{B}_i$. Then $\mathcal{B}$ is basis for M and the matrix A of $g|_M$ with respect to $\mathcal{B}$ is the block diagonal matrix

$$A = \begin{bmatrix} A_1 & 0 & \dots & 0 & 0 \\ 0 & A_2 & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & A_{m-1} & 0 \\ 0 & 0 & \dots & 0 & A_m \end{bmatrix}$$

and so

$$\chi_M(g) = \operatorname{tr}(A) = \sum_{i=1}^m \operatorname{tr}(A_i) = \sum_{i=1}^m \chi_{M_i}(g).$$

□

Lemma 8.2.7. *Let I be finite G-set and recall from 3.1.6 that $\mathbb{K}_I$ is a $\mathbb{K}[G]$-module via $gf = f \circ g^{-1}|_I$ for all $f \in \mathbb{K}_I$ and $g \in \mathbb{K}$. Then*

$$\chi_{\mathbb{K}^I}(g) = |\operatorname{Fix}_I(g)|.$$

Proof. For $i \in I$ let $v_i = (\delta_{ij})_{j \in I}$ in $\mathbb{K}_I$, then $(v_i)_{i \in I}$ is a basis for $\mathbb{K}_I$ and $gv_i = v_{gi}$ for all $g \in G$. [1] Hence matrix of $g|_{\mathbb{K}_I}$ with respect to the basis $(v_i)_{i \in I}$ is

$$A = [\delta_{gi,j}]_{\substack{i \in I \\ j \in I}}$$

In particular, $A_{ii} = 1$ if $gi = i$ and $A_{ii} = 0$ if $gi \neq i$. In other words $A_{ii} = 1$ of $i \in \operatorname{Fix}_I(g)$ and $A_{ii} = 0$ if $i \notin \operatorname{Fix}_I(g)$. It follows that

$$\chi_{\mathbb{K}_I}(g) = \sum_{i \in I} A_{ii} = \sum_{i \in \operatorname{Fix}_I(g)} 1 = |\operatorname{Fix}_I(g)|$$

[1] Thus $g \sum_{i \in I} k_i v_i = \sum_{i \in I} k_i v_{gi}$.

□

Lemma 8.2.8. *Let $g \in G$.*

(a) $\mathbb{K}[G] \cong \sum_{S \in \mathcal{S}} S^{d_S}$ *as* $\mathbb{K}[G]$*-module by left multiplication.*

(b) $\chi_{\mathbb{K}[G]} = \sum_{S \in \mathcal{S}} d_S \chi_S$.

(c) $\chi_{\mathbb{K}[G]}(1) = |G|$.

(d) If $g \neq 1$, *then* $\chi_{\mathbb{K}[G]}(g) = \sum_{S \in \mathcal{S}} d_S \chi_S(g) = 0$.

Proof. (a): By 8.1.7(b), $\mathbb{K}[G] \cong \bigoplus_{S \in \mathcal{S}} A_S$ as a ring and by 7.3.3(b), $A_S \cong S^{d_S}$ as a left A_S-module. So (a) holds.

(b) follows from (a) and 8.2.6(c).

(c) and (d): View G as a G-set by left multiplication and note that $\mathbb{K}[G] = \mathbb{K}_G$ as $\mathbb{K}[G]$-module. Thus by 8.2.7 $\chi_{\mathbb{K}[G]}(g) = |\mathrm{Fix}_G(g)|$. Note that $\mathrm{Fix}_G(1) = G$ and if $1 \neq g \in G$, then $\mathrm{Fix}_G(g) = \emptyset$. Thus (c) and (d) hold. □

Lemma 8.2.9. *Let $S \in \mathcal{S}$ and $C \in \mathcal{C}$.*

(a) $e_S = \frac{d_S}{|G|} \sum_{g \in G} \chi_S(g^{-1})g = \frac{d_S}{|G|} \sum_{C \in \mathcal{C}} \chi_S(g_C^{-1})a_C$.

(b) $a_C = \sum_{S \in \mathcal{S}} \frac{|C|}{d_S} \chi_S(g_C) e_S$.

Proof. (a) Let $e_S = \sum_{g \in G} k_g g$ with $k_g \in \mathbb{K}$. Let $h \in G$. Then $he_S = \sum_{g \in G} k_g hg$. Hence by 8.2.8(c), (d), $\chi_{\mathbb{K}[G]}(hg) = |G|$ if $h = g^{-1}$ and 0 otherwise. So

$$(*) \qquad \tilde{\chi}_{\mathbb{K}[G]}(he_S) = k_{h^{-1}}|G|.$$

On the other hand

$$(**) \qquad e_S|_T = 0 \text{ for all } S \neq T \in \mathcal{S} \qquad \text{and} \qquad e_S|_S = \mathrm{id}_S$$

Thus

$$\tilde{\chi}_T(he_S) = 0 \qquad \text{and} \qquad \tilde{\chi}_S(he_S) = \chi_S(h).$$

By 8.2.8(b)

$$\chi_{\mathbb{K}[G]} = \sum_{S \in \mathcal{S}} d_S \chi_S \quad \text{and so} \quad \tilde{\chi}_{\mathbb{K}[G]}(he_S) = d_S \chi_S(h).$$

Hence (*) implies

$$k_{h^{-1}} = \frac{d_S}{|G|}\chi_S(h) \quad \text{and so} \quad k_h = \frac{d_S}{|G|}\chi_S(h^{-1}).$$

Thus (a) holds.

(b) By 8.1.7 $a_C = \sum_{S\in\mathcal{S}} l_S e_S$ for some $l_S \in \mathbb{K}$. By (**) $\tilde{\chi}_T(e_S) = \delta_{ST} d_S$ and so

$$l_T d_T = \tilde{\chi}_T(a_C) = \sum_{g\in C} \chi_T(g) = |C|\chi_T(g_C).$$

So $l_T = |C|\frac{\chi_T(g_C)}{d_T}$. □

Theorem 8.2.10 (Orthogonality Relations)**.** *(*OR 1) *For all $S, T \in \mathcal{S}$,*

$$\sum_{C\in\mathcal{C}} \frac{1}{|\mathrm{C}_G(g_C)|}\chi_S(g_C)\chi_T(g_C^{-1}) = \frac{1}{|G|}\sum_{g\in G}\chi_S(g)\chi_T(g^{-1}) = \delta_{ST}$$

*(*OR 2) *For all $C, D \in \mathcal{C}$,*

$$\sum_{S\in\mathcal{S}} \chi_S(g_C)\chi_S(g_D^{-1}) = |\mathrm{C}_G(g_C)|\delta_{CD}.$$

Proof. Note first that

$$(*) \qquad |C| = \frac{|G|}{|\mathrm{C}_G(g_C)|}$$

for all $C \in \mathcal{C}$. Let A and B be the matrices for the change of bases for $\mathrm{Z}(\mathbb{K}G)$ from $(a_C)_{C\in\mathcal{C}}$ to $(e_S)_{S\in\mathcal{S}}$ and back. Then by 8.2.9

$$A = \left[\frac{d_S}{|G|}\chi_S(g_C^{-1})\right]_{SC} \qquad \text{and} \qquad B = \left[\frac{|C|}{d_S}\chi_S(g_C)\right]_{CS}.$$

Since $AB = \mathrm{I}_{\mathcal{S}}$ we get for all $T, S \in \mathcal{S}$

$$\begin{aligned}\delta_{ST} &= \sum_{C\in\mathcal{C}} \frac{d_T}{|G|}\chi_T(g_C^{-1})\frac{|C|}{d_S}\chi_S(g_C) = \frac{1}{|G|}\frac{d_T}{d_S}\sum_{C\in\mathcal{C}}|C|\chi_T(g_C^{-1})\chi_S(g_C)\\ &= \frac{1}{|G|}\frac{d_T}{d_S}\sum_{C\in\mathcal{C}}\sum_{g\in C}\chi_T(g^{-1})\chi_S(g) = \frac{1}{|G|}\frac{d_T}{d_S}\sum_{g\in G}\chi_T(g^{-1})\chi_S(g)\end{aligned}$$

Together with (*) this gives (1).

Since $BA = \mathrm{I}_{\mathcal{C}}$ we get for all $C, D \in \mathcal{C}$

$$\sum_{S\in\mathcal{S}} \frac{|C|}{d_S}\chi_S(g_C)\frac{d_S}{|G|}\chi_S(g_D^{-1}) = \delta_{CD}.$$

and so

$$\sum_{S\in\mathcal{S}} \chi_S(g_C)\chi_S(g_D^{-1}) = \frac{|G|}{|C|}\delta_{CD}.$$

Together with $(*)$ this gives (2). □

8.3 Integral Extensions

Definition 8.3.1. *Let R and S be commutative rings with identity such that $R \leq S$ and $1_R = 1_S$. Then s is called integral over R if there exists a monic polynomial $f \in R[x]$ with $f(s) = 0$. $\mathbb{A}(R, S)$ is the set of elements of S integral over R.*

Lemma 8.3.2. *Let R and S be commutative rings with identities such that $R \leq S$ and $1_R = 1_S$.*

(a) Let $s \in S$. Then s is integral over R if and only of $R[s]$ is finitely generated as an R-module by left multiplication.

(b) If R is a PID, then $\mathbb{A}(R, S)$ is subring of R.

Proof. (a) Suppose first that $f(s) = 0$ for some monic polynomial $f \in R[x]$. Put $m = \deg f$ and let $g \in R[x]$. Then $g = qf + r$ for some $q, r \in R[x]$ with $\deg r < m$. It follows that $g(s) = r(s)$ and so $R[s] = \langle s^i \mid 0 \leq i < m\rangle_R$.

Suppose next that $R[s]$ is finitely generated as an R-module. Then there exists $f_1, \ldots, f_n \in R[x]$ with $R[s] = \langle f_i(s) \mid 1 \leq i \leq n\rangle_R$. Put $m = \max_{1\leq i\leq n} \deg f_i$. Then $R[s] = \langle s^i \mid 0 \leq i \leq m\rangle$. It follows that $s^{m+1} = \sum_{i=0}^m r_i s^i$ for some $r_i \in R$ and so s is integral over R.

(b) Let $a, b \in S$ be integral over R. Then b is also integral over $R[a]$. Thus by (a) $R[a]$ is a finitely generated R-module and $R[a, b]$ is a finitely generated $R[a]$-module. Hence 4.1.5(a) implies $R[a, b]$ is a finitely generated R-module. Since R is a PID, 3.2.8 shows that every R-submodule of $R[a, b]$ is finitely generated. It follows that $R[s]$ is a finitely generated R-module for all $s \in R[a, b]$. Hence $R[a, b] \subseteq \mathbb{A}(R, S)$ and $\mathbb{A}(R, S)$ is a subring of $\mathbb{F}$.

□

Lemma 8.3.3. *Let R be a PID and $\mathbb{F}$ a field containing R. Put*

$$\mathbb{F}_R = \{ab^{-1} \mid a, b \in R, b \neq 0\}^2 \qquad \textit{and} \qquad \mathbb{A} = \mathbb{A}(R, \mathbb{F}).$$

(a) $\mathbb{A} \cap \mathbb{F}_R = R$.

(b) Let $a \in \mathbb{A}$. Then $m_a^{\mathbb{F}_R} \in R[x]$.

[2] Note that $\mathbb{F}_R$ is a field of fraction of R.

Proof. (a) See Lemma L on the solutions of Homework 3.

(b) Let $\mathbb{E}$ be splitting field of $m_a = m_a^{\mathbb{F}_R}$ over $\mathbb{F}$ and $f \in R[x]$ a monic polynomial in $R[x]$ with $f(a) = 0$. Then m_a divides f in $\mathbb{E}[x]$ and so each root of m_a is also a root of f. It follows that all roots of m_a are integral over R and so are contained in $\mathbb{B} := \mathbb{A}(R, \mathbb{E})$. Since $\mathbb{B}$ is a subring of $\mathbb{E}$ and $m_a = \prod_{i=1}^m (x - a_i)$ with $a_i \in \mathbb{B}$, $m_a \in \mathbb{B}[x]$. By (a) $\mathbb{B} \cap \mathbb{F}_R = R$ and since $m_a \in \mathbb{F}_R[x]$, $m_a \in R[x]$. □

Lemma 8.3.4. *Let R be a PID and V and W finitely generated unitary R-module.*

(a) $\mathrm{Hom}_R(V, W)$ *is a finitely generated R-module.*

(b) Let $\alpha \in \mathrm{End}_R(V)$. *Then there exist a monic polynomial* $f \in \mathbb{F}[x]$ *with* $f(\alpha) = 0$*,*

Proof.

Since V is finitely generated, $V = \langle v_1, \ldots, v_n \rangle_R$ for some finite family $(v_i)_{i=1}^n$ in V. Note that the R-linear function

$$\pi : R^n \to V, (r_i)_{i\in 1}^n \to \sum_{i=1}^n r_i v_i$$

is onto and so the R-linear function

$$\mathrm{Hom}_R(V, W) \to \mathrm{Hom}_R(R^n, W), \ \alpha \to \alpha \circ \pi$$

is 1-1. Also

$$\mathrm{Hom}_R(R^n, W) \cong \mathrm{Hom}_R(R, W)^n \cong W^n$$

and so $\mathrm{Hom}_R(R^n, W)$ is a finitely generated R-module. Since R is PID any R-submodule of $\mathrm{Hom}_R(R^n, W)$ is finitely generated and so also $\mathrm{Hom}_R(V, W)$ is finitely generated.

Let $S = R|_V$ be the image of R in $\mathrm{End}_R(V)$. By (a), $\mathrm{End}_R(V)$ is a finitely generated R-module and since R is a PID also the submodule $S[\alpha]$ of $\mathrm{End} - R(V)$ is a finitely generated R-module. It follows that $S[\alpha]$ is a finitely generated S module and so by 8.3.2(a) there exists a monic polynomial $g = \sum_{i=0}^n g_i x^i \in S[x]$ with $g(\alpha) = 0$. Then $g_i = f_i|_M$ for some $f_i \in R$ with $f_n = 1$. Put $f = \sum_{i=0}^m f_i x^i$. Then $f(\alpha) = g(\alpha) = 0$. □

8.4 Complex character

Lemma 8.4.1. *Let* $\lambda, \lambda_1, \ldots \lambda_d$ *be roots of unity on* $\mathbb{C}$. *Put* $a = \sum_{i=1}^d \lambda_i$.

(a) λ *is algebraic integer,* $|\lambda| = 1$ *and* $\overline{\lambda} = \lambda^{-1}$.

(b) a is an algebraic integer, that is a is integral over $\mathbb{Z}$.

(c) $|a| \leq d$.

(d) $|a| = d$ *if and only if* $\lambda_1 = \lambda_2 = \ldots = \lambda_d$.

(e) $a = d$ *if and only if* $\lambda_1 = \lambda_2 = \ldots = \lambda_d = 1$.

(f) If $\frac{a}{d}$ *is an algebraic integer, then either* $a = 0$ *or* $|a| = d$.

Proof. (a) Let $m \in \mathbb{Z}^+$ with $\lambda^m = 1$. Then λ is a root of $x^m = 1$ and so an algebraic integer. Also $(\lambda\overline{\lambda})^m = \lambda^m\overline{\lambda^m} = 1$ and since $\lambda\overline{\lambda}$ is a positive real number, $\lambda\overline{\lambda} = 1$. So $|\lambda| = 1$, $\lambda\overline{\lambda} = 1$ and $\overline{\lambda} = \lambda^{-1}$.

(b) By (d) $\lambda_i \in \mathbb{A}(\mathbb{Z}, \mathbb{C})$ for all $1 \leq i \leq d$. By 8.3.2(b), $\mathbb{A}(\mathbb{Z}, \mathbb{C})$ is a subring of $\mathbb{C}$ and so (b) holds.

(c) By the tringualar inequality and (a)

$$(*) \qquad |a| \leq \sum_{i=1}^{d} |\lambda_i| = \sum_{i=1}^{d} 1 = d$$

(d) Equality holds in (*) if and only if there exists $r_i \in \mathbb{R}^{\geq 0}$, $1 \leq i \leq d$ with $\lambda_i = r_i\lambda_1$. Then

$$1 = |\lambda_i| = |r_i\lambda_1| = r_i|\lambda_i| = r_1 1 = r_1$$

and so $\lambda_i = \lambda_1$ for all $1 \leq i \leq d$.

(e) If $a = d$, (d) shows that $\lambda_i = \lambda_1$ for all $1 \leq i \leq d$ and so $d = a = d\lambda_1$ and $\lambda_1 = 1$.

(f) Let $n \in \mathbb{N}$ with $\lambda_i^n = 1$ for all $1 \leq i \leq d$. Let $\mathbb{F}$ be splitting field of $x^n - 1$ over $\mathbb{Q}$ in $\mathbb{C}$. Then $\mathbb{Q} \leq \mathbb{F}$ is normal and separable and so Galois. Let f be the minimal polynomial of $\frac{a}{d}$ over $\mathbb{Q}$, $H = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{F})$ and $E = \{h\frac{a}{d}) \mid h \in H\}$. Since $\mathbb{Q} \leq \mathbb{F}$ is Galois, $\mathrm{Fix}_{\mathbb{F}}(H) = \mathbb{Q}$ and 4.3.6(b:a) shows that

$$f = \prod_{e\in E} x - e$$

Put $k = \prod_{e\in E} e$. If $e \in R$ then $e = h(\frac{a}{d})$ for some $h \in H$. Note that

$$h(a) = \sum_{i=1}^{d} h(\lambda_i)$$

and each $h(\lambda_i$ is a root of unity in $\mathbb{C}$. So by (d), $|h(a)| \leq d$ and $|e| = |h(\frac{a}{d})| \leq 1$. Thus

$$|k| = \prod_{e\in E} |e| \leq 1.$$

Suppose now that $\frac{a}{d}$ is an algebraic integer. Then by 8.3.3(b) $f \in \mathbb{Z}[x]$. Since the constant coefficient of f is $(-1)^d k$ we get $k \in \mathbb{Z}$. Since $|k| \leq 1$ this gives $k = 0, 1$ or -1. In the first case, since f is irreducible, $f = x$ and so also $\frac{a}{d} = 0$ and $a = 0$. If $|k| = 1$ we get $|e| = 1$ for all $e \in E$. In particular, $|\frac{a}{d}| = 1$ and so $|a| = d$. □

Lemma 8.4.2. *Let* M *be a finite dimensional unitary* $\mathbb{C}[G]$*-module and put* $d_M = \dim_{\mathbb{C}} M$ *and* $M^* = \mathrm{Hom}_{\mathbb{C}}(M, \mathbb{C})$.

(a) $\chi_M(g)$ *is an algebraic integer for all* $g \in G$.

(b) $\chi_M(g^{-1}) = \overline{\chi_M(g)}$.

(c) $\overline{\chi_M} = \chi_{M^*}$

(d) $|\chi_M(g)| \leq d_M$.

(e) $|\chi_M(g)| = d_M$ *if and only if g acts as a scalar on M, that is* $g_M = \lambda \mathrm{id}_M$ *for some* $\lambda \in \mathbb{C}$.

(f) $\chi_M(g) = d_M$ *if and only if* $g \in \mathrm{Stab}_G(M)$.

Proof. Put $d = d_M$. By 8.1.10(e) applied to $\langle g \rangle$ in place of G there exists a $\mathbb{C}$ basis $(v_i)_{i=1}^d$ of M with

$$gv_i = \lambda_i v_i$$

for all $1 \leq i \leq d$, where $\lambda_i = \alpha_i(g)$ for some $\alpha_i \in \mathrm{Hom}(\langle g \rangle, \mathbb{C}^\sharp)$. In particular, λ_i is $|g|$-root of unity and so $\lambda_i^{-} = \overline{\lambda}$. Also the matrix A of $g|_M$ with respect to $(v_i)_{i=1}^d$ is a $d \times d$-diagonal matrix with diagonal entries $\lambda_i, 1 \leq i \leq d$.

(a) We have $\chi_M(g) = \sum_{i=1}^m \lambda_i$ and so by 8.4.1(b), $\chi_M(g)$ is an algebraic integer.

(b) The matrix of $g^{-1}|_M$ is $A^{-1} = \overline{A}$ and so $\chi_M(g^{-1}) = \mathrm{tr}(\overline{A}) = \overline{\mathrm{tr} A} = \overline{\chi_M(g)}$.

(c) Define $\phi_i \in M^*$ by $\phi_i(v_j) = \delta_{ij}$. Then $(\phi_i)_{i=1}^n$ is $\mathbb{C}$ basis for M^*. We compute

$$(g\phi_i)(v_j) = \phi_i(g^{-1}v_j) = \phi_i(\lambda_j^{-1}v_j) = \overline{\lambda_j}\phi_i(v_j) = \overline{\lambda_i}\delta_{ij}$$

and so $g\phi_i = \overline{\lambda_i}\phi_i$. So the matrix of $g|_{M^*}$ with respect to $(\phi_i)_{i=1}^d$ is $\overline{A}$ and so (c) holds.

(d) Since $\chi_M(g) = \sum_{i=1}^d \lambda_i$, this follows from 8.4.1(d).

(e) By 8.4.1(e) $|\chi_M(g)| = d$ if and only if $\lambda_1 = \lambda_2 = \ldots = \lambda_d$ and so if and only if $A = \lambda_1 \mathrm{Id}_d$ and if and only if $g\ |_M = \lambda_1 \mathrm{id}_M$.

(f) By 8.4.1(e) $\chi_M(g) = d$ if and only if $\lambda_1 = \lambda_2 = \ldots = \lambda_d = 1$ and so if and only if $A = \mathrm{Id}_d$, if and only if $g\ |_M = \mathrm{id}_M$ and if and only if $g \in \mathrm{Stab}_G(M)$. e. □

Lemma 8.4.3. *$(a_C)_{C \in \mathcal{D}}$ is a $\mathbb{Z}$-basis for $\mathrm{Z}(\mathbb{Z}[G])$. In particular, there exists integers k_{CDE}, $C, D, E \in \mathcal{C}$ with*

$$a_C a_D = \sum_{E \in \mathcal{C}} k_{CDE} a_E.$$

for all C, D, E.

Proof. Let $b \in \mathrm{Z}(\mathbb{Z}(G))$. Then $bg = gb$ for all $g \in G$ and so $b \in \mathrm{Z}(\mathrm{C}[G])$. It follows that $b = \sum_{C \in \mathcal{C}} k_c a_C$ for some unique $k_C \in \mathbb{C}$. Since $b \in \mathrm{Z}(\mathbb{Z}(G))$, $k_C \in \mathbb{Z}$ for all $C \in \mathcal{C}$ and so the first statement holds. For the second just observe that $a_C a_D \in \mathrm{Z}(\mathbb{Z}[G])$. □

Lemma 8.4.4. *Suppose $\mathbb{K} = \mathbb{C}$ and let $C \in C$ and $S \in \mathcal{S}$. Then $a_C|_S = \frac{|C|}{d_S}\chi_S(g_C)\mathrm{id}_S$ and $\frac{|C|}{d_S}\chi_S(g_C)$ is an algebraic integer.*

Proof. By 8.2.9(b) $a_C = \sum_{T\in\mathcal{S}} \frac{|C|}{d_T}\chi_T(g_C)e_T$. Since $e_T\mid_S = \delta_{ST}\mathrm{id}_S$ the first statement holds.

Define $\alpha_C : \mathbb{Z}[G]) \to \mathbb{Z}(G)), b \to a_C b$. By 8.3.4(b) there exists a monic polynomial $f \in \mathbb{Z}[x]$ with $f(\alpha_C) = 0$. Then $f(a_C)b = 0$ for all $b \in \mathbb{Z}[G]$. In particular, $f(a_C)1 = 0$ and $f(a_C) = 0$. Hence also $f(a_C)\mid_S = 0$ and the first statement shows that

$$0 = f(a_C)|_S = f\big(\frac{|C|}{d_S}\chi_S(g_C)\mathrm{id}_S\big) = f\big(\frac{|C|}{d_S}\chi_S(g_C)\big)\mathrm{id}_S$$

so $f\big(\frac{|C|}{d_S}\chi_S(g_C)\big) = 0$. Hence $\frac{|C|}{d_S}\chi_S(g_C)$ is the root of a monic integral polynomial in $\mathbb{C}$ and so an algebraic integer.

□

Proposition 8.4.5. *Suppose $\mathbb{K} = \mathbb{C}$. Then d_S divides $|G|$ for all $S \in \mathcal{S}$.*

Proof. By the first orthogonality relation 8.2.10(1) applied with $S = T$,

$$\frac{1}{|G|}\sum_{C\in\mathcal{C}} \frac{1}{|\mathrm{C}_G(g_C)|}\chi_S(g_C)\chi_S(g_C^{-1}) = 1.$$

Multiplication with $\frac{|G|}{d_S}$ gives:

$$\sum_{C\in\mathcal{S}} \frac{|C|\chi_S(g_c)}{|d_S|}\chi_S(g_C^{-1}) = \frac{|G|}{d_S}.$$

By 8.4.4 $\frac{|C|\chi_S(g_c)}{|d_S|}$ is an algebraic intgeger, by 8.4.2(a), $\chi_S(g_C^{-1})$ is an algebraic integer and so by 8.4.1(b), also $\frac{|G|}{d_S}$ is an algebraic integer. Hence by 8.4.1(c), $\frac{|G|}{d_S}$ is an integer. □

The next lemma shows how the class algebra constants can be computed from the character table.

Lemma 8.4.6. *(a) For all $C, D, E \in \mathcal{C}$:*

$$k_{CDE} = \frac{|G|}{|C_G(g_C)||C_G(g_D)|}\sum_{S\in\mathcal{S}} \frac{1}{d_S}\chi_S(g_c)\chi_S(g_D)\overline{\chi}_S(g_E)$$

(b) For all $C, D \in \mathcal{C}$

$$a_C a_D = \frac{|G|}{|C_G(g_C)||C_G(g_D)|}\sum_{S\in\mathcal{S}} \frac{\overline{\chi}_S(g_c)\overline{\chi}_S(g_D)}{d_S}\chi_S$$

Proof. (a) By definition of the k_{CDF},

$$a_C a_D = \sum_{F\in\mathcal{C}} k_{CDF}a_F$$

and so also

$$\rho_S(a_C)\rho_S(a_D) = \sum_{F\in\mathcal{C}} k_{CDF}\rho(a_F)$$

Thus 8.4.4 gives

$$\frac{|C|\chi_S(g_C)}{d_S}\frac{|D|\chi_S(g_D)}{d_S} = \sum_{F\in\mathcal{C}} k_{CDF}\frac{|F|\chi_S(g_F)}{d_S}$$

Thus

$$\frac{|C||D|}{d_S}\chi_S(g_C)\chi_S(g_D) = \sum_{F\in\mathcal{C}} |F|k_{CDF}$$

Multiplying with $\overline{\chi}_S(g_E)$ and summing over all $S \in \mathcal{S}$ gives

$$\begin{aligned}
|C||D|\sum_{S\in\mathcal{S}}\frac{1}{d_S}\chi_S(g_C)\chi_S(g_D)\overline{\chi}_S(g_E) &= \sum_{F\in\mathcal{C}}|F|k_{CDF}\sum_{S\in\mathcal{S}}\chi_S(g_F)\overline{\chi}_S(g_E)\\
\text{(2nd Orthogonality relation)} &= \sum_{F\in\mathcal{C}}|F|k_{CDF}|C_G(g_E)\delta_{EF}\\
&= |E|k_{CDE}|C_G(g_E)|
\end{aligned}$$

Since $|X| = \frac{|G|}{|C_G(g_X)|}$ for $X = C, D$ and E, (a) holds.
(b) Note that k_{CDE} is real valued. So (b) follows from (a). □

8.5 Burnside's p^aq^b Theorem

In this short section we will show that all finite groups of order p^aq^b are solvable, where p and q are primes and a and b are integers.

Definition 8.5.1. *Let χ be a character of G over $\mathbb{C}$. Then*

$$\begin{aligned}
\ker\chi &= \{g\in G \mid \chi(g) = \chi(1)\}\\
\mathrm{Z}(\chi) &= \{g\in G \mid |\chi(g)| = \chi(1)\}
\end{aligned}$$

Lemma 8.5.2. *Suppose $\mathbb{K} = \mathbb{C}$ and let $S \in \mathcal{S}$. Then*

(a) $\ker\chi_S = \mathrm{Stab}_G(S)$.

(b) $\mathrm{Z}(\chi_S)$ *consists of all $g \in G$ which act as scalars on S. Moreover,* $\mathrm{Z}(\chi_S)/\ker\chi_S = \mathrm{Z}(G/\ker\chi_S)$.

Proof. (a) follows from 8.4.2(f).

(b) The first part of (b) follows from 8.4.2(e). For the second statement note that $G/\ker\chi_S \cong G|_M$ and so we may assume that $G \subseteq \mathrm{End}_{\mathbb{K}}(M)$.

Then $\mathrm{Z}(G) = G \cap \mathrm{End}_{\mathbb{K}G}(S)$. By 8.1.7(d) $\mathrm{End}_{\mathbb{K}G}(S) = \mathbb{K}|_S$ and so $Z(G) = G \cap \mathbb{K}|_S$. Thus also the second statement in (b) holds. □

Lemma 8.5.3. *Suppose $\mathbb{K} = \mathbb{C}$ and there exist $S \in \mathcal{S}$ and $C \in \mathcal{S}$ with $\gcd\big(d_S, |C|\big) = 1$. Then either $\chi(g_C) = 0$ or $C \subseteq \mathrm{Z}(\chi_S)$.*

Proof. Since $\gcd\big(d_S, |C|\big) = 1$ there exist integers a, b with $ad_S + b|C| = 1$. Multiplying with $\frac{\chi_S(g_C)}{d_S}$ gives

$$a\chi_S(g_C) + b\frac{|C|\chi_S(g_C)}{d_S} = \frac{\chi_S(g_C)}{d_S}.$$

By 8.4.4,8.4.2(a) and 8.4.1(b) the left side of this equation is an algebraic integer. The right side is the sum of d_S roots of unity devided by d_S. So by 8.4.1(f), $\chi_S(g_C) = 0$ or $|\chi_S(g_C)| = d_S = \chi_S(1)$. In the second case $C \subseteq \mathrm{Z}(\chi_S)$. □

Proposition 8.5.4. *Suppose there exits $C \in \mathcal{C}$ with $|C| = p^t$ for some prime p and some $t \in \mathbb{N}$. If $\mathbb{K} = \mathbb{C}$ and $G \neq 1$, then there exists $S \in \mathcal{S}$ with $C \subseteq \mathrm{Z}(\chi_S)$ and $\ker\chi_S \neq G$.*

Proof. Let T be the unique simple module in $\mathcal{S}$ with $\mathrm{Stab}_G(T) = G$ (so $\dim_{\mathbb{K}} T = 1$ and $gt = t$ for all $g \in G, t \in T$.) Since $G \neq 1$, $|\mathcal{S}| = |\mathcal{C}| \neq 1$ and $\mathcal{S} \neq \{T\}$. If $C = \{1\}$, the proposition holds for any $T \neq S \in \mathcal{S}$.

So suppose $C \neq \{1\}$. The Second Orthogonality Relation applied with $D = \{1\}$ gives

$$\sum_{S \in \mathcal{S}} \chi_S(g_C)\chi_S(1) = 0$$

and so

$$1 = -\sum_{T \neq S \in \mathcal{S}} \chi_S(g_C) d_S.$$

Put $\mathbb{A} = \mathbb{A}(\mathbb{Z}, \mathbb{C})$. By 8.4.1(c), $\frac{1}{p} \notin \mathbb{A}$. Thus $1 \notin p\mathbb{A}$ and the preceeding equation shows that there exists $T \neq S \in \mathcal{S}$ with $\chi_S(g_C)d_S \notin p\mathbb{A}$. Then $\chi_S(g_C) \neq 0$ and since $\chi_S(g_C) \in \mathbb{A}$ we conclude that p does not divide d_S in $\mathbb{Z}$. Since $|C| = p^t$ we get $\gcd\big(d_S, |C|\big) = 1$ and the proposition follows from 8.5.3. □

Definition 8.5.5. *A group H is called solvable if there exists a finite chain of subgroups*

$$A_0 = 1 \trianglelefteq A_1 \trianglelefteq \ldots \trianglelefteq A_{n-1} \trianglelefteq A_n = H$$

of H such that A_i/A_{i-1} is abelian for all $1 \leq i \leq n$.

Theorem 8.5.6 (Burnside's $p^a p^b$-Theorem)**.** *Let p and q be primes, $a, b \in \mathbb{N}$ and G a finite group of order $p^a q^p$. Then G is solvable.*

Proof. By induction on $|G|$. Since trivial groups are solvable, the theorem holds for $G| = 1$. Suppose $|G| \neq 1$ and say $q^b \neq 1$. Let Q be a Sylow q-subgroup of G. Then $Q \neq 1$ and by 1.7.38(a) $\mathrm{Z}(Q) \neq 1$. Choose $1 \neq g \in Z(Q)$. Then $q^b \,\big|\, |\mathrm{C}_G(g)|$ and so $|G/\mathrm{C}_G(g)| = p^t$ for some $0 \leq t \leq a$. Put $C = {}^G g$. Then $|C| = p^t$ and by 8.5.4 $C \subseteq \mathrm{Z}(\chi)$ for some character χ of G over $\mathbb{C}$ with $\ker\chi \neq G$. Thus by induction

$\ker\chi$ is solvable. By 8.5.2, $Z(\chi)/\ker\chi$ is abelian and so solvable. Since $C \subseteq Z(\chi)$, $Z(\chi) \neq 1$. Hence $G/Z(\chi)$ has smaller order than G and by induction also $G/Z(\chi)$ is solvable. Thus

$$1 \trianglelefteq \ker(\chi) \triangleleft \mathrm{Z}(\chi) \trianglelefteq G$$

is a subnormal series of G with all factors solvable. The definition of a solvable group now shows that G is solvable. □

Appendix A

Set Theory

A.1 Relations and Function

Definition A.1.1. *Let x and y be objects. Then $(x,y) = \{\{x\},\{x,y\}\}$. (x,y) is called the ordered pair of x and y.*

Lemma A.1.2. *Let a,b,c,d be objects. Then $(a,b) = (c,d)$ if and only of $a = c$ and $b = d$.*

Proof. We first show

1°. *Let $\tilde{a},\tilde{b},\tilde{c}$ and $\tilde{d}$ be objects with $\tilde{a} = \tilde{c}$ and $\{\tilde{a},\tilde{b}\} = \{\tilde{c},\tilde{d}\}$. Then $\tilde{b} = \tilde{d}$.*

Since $\tilde{b} \in \{\tilde{a},\tilde{b}\}$ and $\{\tilde{a},\tilde{b}\} = \{\tilde{c},\tilde{d}\}$, we have $\tilde{b} \in \{\tilde{c},\tilde{d}\}$. So $\tilde{b} = \tilde{c}$ or $\tilde{b} = \tilde{d}$. In the second case (1°) holds. Thus we may assume $\tilde{b} = \tilde{c}$. Since $\tilde{a} = \tilde{c}$ this gives $\tilde{b} = \tilde{a}$. Since $\tilde{d} \in \{\tilde{c},\tilde{d}\}$ and $\{\tilde{c},\tilde{d}\} = \{\tilde{a},\tilde{b}\}$, $\tilde{d} \in \{\tilde{a},\tilde{b}\}$ and so $\tilde{d} = \tilde{a}$ or $\tilde{d} = \tilde{b}$. Since $\tilde{b} = \tilde{a}$ either case gives $\tilde{d} = \tilde{b}$ and so also $\tilde{b} = \tilde{d}$. Thus (1°) is proved.

Suppose now that that $(a,b) = (c,d)$. By the definition of an ordered pair, $(a,b) = \{\{a\},\{a,b\}\}$ and $(c,d) = \{\{c\},\{c,d\}\}$. Thus

$$(*) \qquad \{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}.$$

Since $\{a\} \in \{\{a\},\{a,b\}\}$, (*) implies $\{a\} \in \{\{c\},\{c,d\}$ and so $\{a\} = \{c\}$ or $\{a\} = \{c,d\}$. Since $c \in \{c\}$ and $c \in \{c,d\}$ either case gives $c \in \{a\}$. Thus

$$(**) \qquad c = a.$$

Hence also $\{a\} = \{c\}$ and so (*) shows that the assumptions of (1°) are fulfilled for $\tilde{a} = \{a\}$, $\tilde{b} = \{a,b\}$, $\tilde{c} = \{c\}$ and $\tilde{d} = \{c,d\}$. Thus (1°) implies $\{a,b\} = \{c,d\}$. Since $a = c$, another application of (1°) gives $b = d$. □

Definition A.1.3. *(a) A relation R is a class all of whose members are ordered pairs.*

(b) *If R is relation then $\grave{R} = \{(b,a) \mid (a,b) \in R\}$. $\grave{R}$ is called the opposite of R.*

(c) *Let R be a class. Then*

$$\mathrm{Dom}(R) = \{x \mid (y,x) \in R \textit{ for some } y\}$$

$\mathrm{Dom}(F)$ *is called the domain of F.*

$$\mathrm{Im}(R) = \{y \mid (y,x) \in R \textit{ for some } x\}$$

$\mathrm{Im}\, R$ *is called the image of R.*

(d) *Let R be a relation and x, y objects. Then we say that x is in R-relation to y and write xRy if $(x,y) \in R$.*

(e) *A function is a relation F such that for all x, y, z, $(y,x) \in F$ and $(z,x) \in F$ imply $y = z$.*

(f) *Let F be a function and $x \in \mathrm{Dom}(F)$. Then Fx denotes the unique object such that $(Fx, x) \in F$. So $y = Fx$ if and only if yFx. We will also use the notations $F(x)$ and F_x for Fx.*

(g) *Let A and B be classes. We says that F is a function from A to B and write $F : A \to B$, if F is a function, $A = \mathrm{Dom}(F)$ and $\mathrm{Im}(F) \subseteq B$.*

Example A.1.4. *(a) Let A be any class. Then $\mathrm{id}_A = \{(a,a) \mid a \in A\}$ is a function from A to A, called the identity function on A.*

(b) *Let A and B be classes with $A \subseteq B$. Then id_A is a function from A to B.*

Definition A.1.5. *Let R and S be relations. Then $R \circ S$ is the relation defined by*

$$R \circ S = \{(a,c) \mid aRb \textit{ and } bSc \textit{ for some } b\}$$

Lemma A.1.6. *(a) Let R, S and T be relations. Then*

$$R \circ (S \circ T) = \{(a,d) \mid aRb, bSc \textit{ and } cTd \textit{ for some } c,d\} = (R \circ S) \circ T$$

(b) *Let f and g be functions. Then $f \circ g$ is a function,*

$$\mathrm{Dom}(f \circ g) = \{a \in \mathrm{Dom} f \mid ga \in \mathrm{Dom} f\} = \{a \mid a \in \mathrm{Dom} f \textit{ and } ga \in \mathrm{Dom} f\}$$

and

$$(f \circ g)a = f(ga)$$

f or all $a \in \mathrm{Dom}(f \circ g)$.

(c) *Let $R : A \to B$ and $S : B \to C$ be functions. Then $S \circ R$ is a function from A to C and*

$$(S \circ R)a = S(Ra)$$

for all $a \in A$.

Proof. Readily verified. □

Definition A.1.7. *Let R be a relation.*

(a) $\check{R}$ is the function with domain the class of all functions and $\check{R}S = R \circ S$ for all functions S.

(b) Let R^* is the function with domain the class of all functions and $R^*S = S \circ R$ for all functions S.

(c) Let a be an object. Then Ev_a is the function with domain the class of all functions f with $a \in \mathrm{Dom} f$ and $\mathrm{Ev}_a f = fa$.

Lemma A.1.8. *Let R and S be relations. Then*

$$(R \circ S)\check{} = \check{R} \circ \check{S}$$
$$(R \circ S)^* = S^* \circ R^*$$

and

$$R^* \circ \check{S} = \check{S} \circ R^*$$

Proof. Let T be a function. Then

$$(R \circ S)\check{}T = (R \circ S) \circ T = R \circ (S \circ T) = R \circ (\check{S}T) = \check{R}(\check{S}T) = (\check{R} \circ \check{S})T$$
$$(R \circ S)^*T = T \circ (R \circ S) = (T \circ R) \circ S = (R^*T) \circ S = S^*(R^*T) = (S^* \circ R^*)T$$

and

$$(R^* \circ \check{S})T = R^*(\check{S}T) = (S \circ T) \circ R = S \circ (T \circ R) = \check{S}(R^*T) = (\check{S} \circ R^*)T$$

□

Lemma A.1.9. *Let f be function and a an object. Then*

$$\mathrm{Ev}_a \circ \check{f} = f \circ \mathrm{Ev}_a$$

Proof. Note that the domain of both functions is contain in the class of functions. Let g be a function. Then $g \in \mathrm{Dom}\check{f}$. Thus $g \in \mathrm{Dom}(\mathrm{Ev}_a \circ \check{f})$ if and only if $\check{f}g \in \mathrm{Dom}(\mathrm{Ev}_a)$, if and only if $g \circ f \in \mathrm{Dom}(\mathrm{Ev}_a)$ and if and only if $a \in \mathrm{Dom}(f \circ g)$. In this case

$$(\mathrm{Ev}_a \circ \check{f})g = \mathrm{Ev}_a(\check{f}g) = (\check{f}g)a = (f \circ g)a$$

$g \in \mathrm{Dom}(f \circ \mathrm{Ev}_a)$ if and only if ($g \in \mathrm{Dom}(\mathrm{Ev}_a)$ and $\mathrm{Ev}_a g \in \mathrm{Dom} f$). This holds if and only if a is in the domain of g and ga is in the domain of f and so if and only if $a \in \mathrm{Dom}(f \circ g)$. In this case

$$(f \circ \mathrm{Ev}_a)g = f(\mathrm{Ev}_a g) = f(ga) = (f \circ g)a$$

□

Proposition A.1.10. *Let A and B be partially ordered sets and $f : A \to B$ and $g : B \to A$ be functions. Suppose that f and g are non-decreasing and for all $a \in A, b \in B$*

$$(*) \qquad fa \leq b \iff a \leq gb$$

Put

$$\tilde{A} = \{a \in A \mid f(ga) = a\} \qquad \textit{and} \qquad \tilde{B} = \{b \in B \mid g(fb) = b.\}$$

(a) $a \leq g(fa)$ for all $a \in A$.

(b) $f(gb) \leq b$ for all $b \in B$.

(c) $\tilde{A} = \operatorname{Im} g$

(d) $\tilde{B} = \operatorname{Im} f$.

(e) The function $f\,|_{\tilde{A}} : \tilde{A} \to \tilde{B}$ is a well-defined bijection with well-defined inverse $g\,|_{\tilde{B}} : \tilde{B} \to \tilde{A}$.

Proof. Observe first that the assumption of the lemma are fulfilled for $(B, A, g, f, \geq)$ in place of $(A, B, f, g, \leq)$. Hence (a) implies (b) and (c) implies (d).

(a) : Note that $fa \leq fa$ and so by (*) applied with $b = fa$, $a \leq g(fa)$. Thus (a) and so also (b) holds.

(c): If $a = g(fa)$, then $a = gb$ for $b = ga$. So suppose $a = gb$ for some $b \in B$. (b) implies $fa = f(gb) \leq b$. Since g is non-decreasing this gives $g(fa) \leq gb = a$. By (a) $a \leq g(fa)$ and so $a = g(fa)$. Thus (c) and so also (d) holds.

(e) By (c) $fa \in \tilde{B}$ for all $a \in \tilde{A}$ and so functions are well-defined. By definition of $\tilde{A}$ and $\tilde{B}$ they are inverse to each other. □

Definition A.1.11. *Let R be a relation and A and B be sets.*

(a) $R_A B$ denotes the set

$$R_A B = \{a \in A \mid aRb \textit{ for all } b \in B\}$$

$R_A B$ is called the R-complement of B in A.

(b) Let $D \subseteq B$. We say that D is A-closed in B with respect to R if

$$D = \grave{R}_B(R_A D)$$

Example A.1.12. *(a) Let A and B be sets and $\neq$ the unequal relation. Then $\neq_A B = A \setminus B$.*

(b) Let G be a group and R the commuting relation on G. (So aRb if $a, b \in G$ and $ab = ba$). Then $R_A B = \mathrm{C}_A(B)$.

(c) Let G be group acting on a set S. Let $R = \{(g, s) \in G \times S \mid gs = s\}$. Let $A \subseteq G$ and $T \subseteq S$. Then $R_T S = \operatorname{Stab}_A(T)$ and $\grave{R}_T A = \operatorname{Fix}_T(A)$.

(d) *Let S be a ring, M an R-module, $I \subseteq S$ and $W \subseteq M$. Put $R = \{(s,m) \in S \times M \mid sm = 0\}$. Then $R_S(W) = \mathrm{Ann}_S(W)$ and $\grave{R}_M(I) = \mathrm{Ann}_M(I)$.*

Proposition A.1.13. *Let R be relation and A and B sets. Let $C \subseteq \tilde{C} \subseteq A$ and $D \subseteq \tilde{D} \subseteq B$.*

(a) *$C \subseteq R_A D$, if and only of cRd for all $c \in C, d \in D$, if and only if $d\grave{R}c$ for all $d \in D, c \in C$ and if and only if $D \subseteq \grave{R}_B C$.*

(b) *$R_A D = \bigcap_{d \in D} R_A\{d\}$ and $\grave{R}_B C = \bigcap_{c \in C} \grave{R}_B\{c\}$*

(c) *$R_A \tilde{D} \subseteq R_A D$ and $\grave{R}_B \tilde{C} \subseteq \grave{R}_B C$.*

(d) *$D \subseteq \grave{R}_B(R_A D)$ and $C \subseteq R_A(\grave{R}_B C)$.*

(e) *D is A-closed in B with respect to R if and only if $D = \grave{R}_B E$ for some $E \subseteq A$. C is B-closed in A with respect to $\grave{R}$ if and only if $C = R_A F$ for some $F \subseteq B$.*

(f) *Let $\mathcal{A}$ be set of all subsets of A which are B-closed in A with respect to $\grave{R}$ and $\mathcal{B}$ be set of all subsets of B which are A-closed in B with respect to R. Then*

$$\mathcal{A} \to \mathcal{B}, \quad C \to \grave{R}_B C$$

is well-defined, inclusion reversing, bijection with well-defined inclusion reversing, inverse

$$\mathcal{B} \to \mathcal{A}, \quad D \to R_A D$$

Proof. (a) and (b) follow immediately from the definition of $R_A B$.

(c) follows from (a).

Partial order the set of subsets of A by inclusion and the set of subsets of B by reverse inclusion. Then (a) and (c) show that the assumptions of A.1.10 are fulfilled. Hence (d) to (f) hold. □

A.2 Functions and Magma

Definition A.2.1. *Let A be a set, $(B,+)$ a magma and $f,g : A \to B$ be functions. Define*

$$f + g : A \to B, \quad a \to f(a) + f(b)$$

Remark: Here and below I'm using the symbol + for the binary operations since the main applications will be to the additive group of the ring. But I will only sometimes assume that "+" is commutative.

Lemma A.2.2. *(a) Let $f : A \to B$ and $g : B \to C$ be magma homomorphisms. Then $g \circ f$ is a magma homomorphism.*

(b) Let A, B be sets and C a magma. Let $f : A \to B$ and $g, h : B \to C$ be functions. Then

$$(g+h)\circ f = g\circ f + h\circ f$$

(c) Let A be a set, B and C magma. Let $f, g : A \to B$ be functions and $h : B \to C$ a magma homomorphism. Then

$$h\circ(f+g) = h\circ f + h\circ g$$

(d) Let $f : A \to B$ and $g : A \to B$ be magma homomorphism and suppose that $(w+x)+(y+z) = (w+y)+(x+z)$ for all $w, x, y, z \in B$.[1] *Then $f+g$ is a magma homomorphism.*

Proof. Let $x, y \in A$.

(a)

$$(f\circ g)(x+y) = f(g(x+y)) = f((g(x)+g(y)) = f(g(x)) + f(g(y)) = (f\circ g)(x) + (f\circ g)(y)$$

(b)

$$((g+h)\circ f)(x) = (g+h)(f(x)) = g(f(x)) + h(f(x)) = (g\circ f)(x) + (h\circ f)(x) = (g\circ f + h\circ f)(x)$$

(c)

$$\begin{aligned}(h\circ(f+g))(x) = h((f+g)(x)) &= h(f(x)+g(x)) = h(f(x)) + h(g(x))\\ = (h\circ f)(x) + (h\circ g)(x) &= (h\circ f + h\circ g)(x)\end{aligned}$$

(d)

$$\begin{aligned}(f+g)(x+y) = f(x+y) + g(x+y) &= (f(x)+f(y)) + (g(x)+g(y))\\ = (f(x)+g(x)) + (f(y)+g(y)) &= (f+g)(x) + (f+g)(y)\end{aligned}$$

□

Lemma A.2.3. *(a) Let $f : A \to B$ a magma homomorphism and C a set. Then*

$$\check{f} : \operatorname{Fun}(C, A) \to \operatorname{Fun}(C, B),\ g \to f\circ g.$$

is a magma homomorphism.

(b) Let $f : A \to B$ a function and C a magma. Then

$$f^* : \operatorname{Fun}(B, C) \to \operatorname{Fun}(A, C), g \to g\circ f$$

is a magma homomorphism.

[1] This holds for example if B is an abelian semigroup. If B has an identity it holds if and only if B is an abelian monoid.

Proof. (a) follows from A.2.2(b) and (b) from A.2.2(a). □

Lemma A.2.4. *Let A and B be sets. Note that* $\mathrm{Fun}(A,A)$ *is a monoid under composition.*

(a) The function

$$\mathrm{Fun}(B,B) \to \mathrm{Fun}\big(\mathrm{Fun}(A,B),\mathrm{Fun}(A,B)\big), f \to \check{f} = (g \to f \circ g)$$

is homomorphism of monoids,

(b) The function

$$\mathrm{Fun}(A,A) \to \mathrm{Fun}\big(\mathrm{Fun}(A,B),\mathrm{Fun}(A,B)\big), f \to f^* = (g \to g \circ f)$$

is anti-homomorphism of monoids.

Proof. By A.2.2(c) the function in (a) is a magma homomorphism and the function in (b) is a magma anti-homomorphism. Since $g \circ \mathrm{id}_A = g = \mathrm{id}_B \circ g$ for all $g \in \mathrm{Fun}(A,B)$, the functions are (anti) homomorphism of monoids. □

Lemma A.2.5. *Let A, B be sets and C a magma. Then the function*

$$\mathrm{Fun}(A \times B, C) \to \mathrm{Fun}\big(A, \mathrm{Fun}(B,C)\big), \quad f \to f_A$$

is magma isomorphism.

Proof. Let $f, g : A \times B \to C$ be function and $a \in A$, $b \in B$. Then

$$(f+g)_a b = (f+g)(a,b) = f(a,b) + g(a,b) = f_a b + g_a b$$

Thus $(f+g)_a = f_a + g_a$ for all $a \in A$ and $(f+g)_A = f_A + g_A$. □

Definition A.2.6. *Let $f : A \times B \to C$ be functions.*

(a) Suppose B and C are magma. Then f is called magma-homomorphism in the second coordinate if

$$f(a, b + \tilde{b}) = f(a,b) + f(a,\tilde{b})$$

for all $a \in A$ and $b, \tilde{b} \in B$.

(b) Suppose A, B and C are magma. Then f is called a magma bihomomorphism if f is a magma homomorphism in the first and second coordinate.

Lemma A.2.7. *Let $f : A \times B \to C$ be a function and suppose B and C are magma. Then the following are equivalent:*

(a) f is a magma-homomorphism in the second coordinate.

(b) f_a is magma -homomorphism for all $a \in A$.

(c) f_A *is a function from* A *to* $\mathrm{Hom}(B,C)$.

(d) f_B *is a magma homomorphism from* B *to* $\mathrm{Fun}(A,C)$.

Proof. (a) $\Longleftrightarrow$ (b) :

$$\begin{array}{llll} & f(a,b+\tilde{b}) = f(a,b)+f(a,\tilde{b}) & \text{for all } a\in A, b,\tilde{b}\in B \\ \Longleftrightarrow & f_a(b) \quad = f_a(\tilde{b}) & \text{for all } a\in A, b,\tilde{b}\in B \end{array}$$

(b) $\Longleftrightarrow$ (c) : Obvious.

(a) $\Longleftrightarrow$ (d) :

$$\begin{array}{llll} & f(a,b+\tilde{b}) & = f(a,b)+f(a,\tilde{b}) & \text{for all } a\in A, b,\tilde{b}\in B \\ \Longleftrightarrow & f_{b+\tilde{b}}(a) & = f_b(a)+f_{\tilde{b}}(a) & \text{for all } a\in A, b,\tilde{b}\in B \\ \Longleftrightarrow & f_{b+\tilde{b}} & = f_b+f_{\tilde{b}} & \text{for all } b,\tilde{b}\in B \end{array}$$

□

Example A.2.8. Let A be a set and B a magma.

Consider the function

$$\pi: \ \mathrm{Fun}(A,B)\times A \ \to B, \quad (f,a)\to fa$$

Then for $f\in\mathrm{Fun}(A,B)$ and $a\in A$, $\pi_f a = \pi(f,a) = fa$ and so $\pi_f = f$. Thus $\pi_{\mathrm{Fun}(A,B)} = \mathrm{id}_{\mathrm{Fun}(A,B)}$ is a magma homomorphism. Thus π is magma homomorphism in the first coordinate. Hence for all $a\in A$,

$$\pi_a: \ \mathrm{Fun}(A,B)\to B, \quad f\to fa$$

is a magma homomorphism and we obtain a function:

$$\pi_A: \ A\to\mathrm{Hom}\big(\mathrm{Fun}(A,B),B\big), \quad a\to\pi_a$$

Lemma A.2.9. *Let* A,B,C *be magma and* $f: A\times B\to C$ *a function. Then the following are equivalent:*

(a) f *is a magma bihomomorphism.*

(b) f_A *is a magma homomorphism from* A *to* $\mathrm{Hom}(B,C)$.

(c) f_B *is a magma homomorphism from* B *to* $\mathrm{Hom}(A,C)$.

Proof. By A.2.7 f is a magma homomorphism in the second coordinate if and only if f_A is function from A to $\mathrm{Hom}(B,C)$; and f is magma homomorphism in first coordinate if and only if f_A magma homomorphism from A to $\mathrm{Fun}(B,C)$. So (a) and (b) are equivalent. By symmetry also (a) and (c) are equivalent. □

A.3 Zorn's Lemma

This chapter is devoted to prove Zorn's lemma: Let M be a nonempty partially ordered set in which every chain has an upper bound. Then M has a maximal element.

To be able to do this we assume throughout this lecture notes that the *axiom of choice* holds:

Hypothesis A.3.1 (Axiom of choice)**.** *Let I be a non-empty set and $(A_i)_{i\in I}$ a family of non-empty sets. Then*

$$\bigtimes_{i\in I} A_i \neq \varnothing$$

Note that this means that there exists a function f with domain I and $f(i) \in A_i$ for all $i \in I$. Naively this just means that we can pick an element from each of the sets A_i.

Definition A.3.2. *A* partially ordered set *is a set M together with a reflexive, anti-symmetric and transitive relation "$\leq$". That is for all $a, b, c \in M$*

(a) $a \leq a$ *(*reflexive*)*

(b) $a \leq b$ *and* $b \leq a \Longrightarrow a = a$ *(*anti-symmetric*)*

(c) $a \leq b$ *and* $b \leq c \Longrightarrow a \leq c$ *(*transitive*)*

Definition A.3.3. *Let $(M, \leq)$ be a partially ordered set, $a, b \in M$ and $C \subseteq M$.*

(a) a are called comparable *if $a \leq b$ or $b \leq a$.*

(b) $(M, \leq)$ is called totally ordered *if any two elements are comparable.*

(c) C is called a chain *if any two elements in C are comparable.*

(d) An upper bound *m for C is an element m in M such that that $c \leq m$ for all $c \in C$.*

(e) An element $m \in M$ is called a smallest element *(or a least element) of C if $m \in C$ and $m \leq c$ for all $c \in C$.*

(f) An element $m \in C$ is called a largest element *(or a greatest) elements of C if $m \in C$ and $c \leq m$ for all $c \in C$.*

(g) An element $m \in C$ is called a maximal element *of C if $c = m$ for all $c \in C$ with $m \leq c$.*

(h) An element $m \in C$ is called a minimal element *of C if $c = m$ for all $c \in C$ with $c \leq m$.*

(i) A function $f : M \to M$ is called increasing if $a \leq f(a)$ for all $a \in M$.

Lemma A.3.4. *Let M be partially ordered set and $A \subseteq M$. Then A has at most one least element.*

Proof. Let a and b be least elements of A. Since $a \in A$ and b a least element of A, $b \leq a$. By symmetry $b \leq a$. Since $\leq$ is anti-symmetric, $a = b$. □

As the main step toward our proof of Zorn's lemma we show:

Lemma A.3.5. *Let M be a non-empty partially ordered set in which every non-empty chain has a least upper bound. Let $f : M \to M$ be an increasing function. Then $f(m_0) = m_0$ for some $m_0 \in M$.*

Proof. Since $M \neq \varnothing$ we can choose $a \in M$. Let $B := \{m \in M \mid a \leq m\}$. If $b \in B$, then $a \leq b$ and $b \leq f(b)$. So $a \leq f(b)$ and $f(b) \in B$. Note also that the least upper bound of any non-empty chain in B is contained in B. So replacing M by B we may assume that

1°. *$a \leq m$ for all $m \in M$.*

Define a subset A of M to be closed if:

(Cl i) $a \in A$

(Cl ii) $f(b) \in A$ for all $b \in A$.

(Cl iii) If C is a non-empty chain in A then its least upper bound is in A.

Since M is closed, there exists at least one closed subset of M.

2°. *Let D be chain in M and suppose D is closed. Then D has a least upper bound d in M and $f(d) = d$.*

By (i), D is not empty and so D has a least upper bound d. By (iii), $d \in D$ and by (ii), $f(d) \in D$. Since d is a upper bound for D, $f(d) \leq d$ and since f is increasing, $d \leq f(d)$. Since $\leq$ is antisymmetric $f(d) = d$.

In view of(2°) we just have to find a closed chain in M. For this let A be the intersection of all the closed subsets of M and observe that A itself is closed.

$e \in A$ is called extreme if

$$\text{(Ex)} \qquad f(b) \leq e \text{ for all } b \in A \text{ with } b < e$$

Note that a is extreme, so the set E of extreme elements in A is not empty.

3°. *Let e be extreme and $b \in A$. Then $b \leq e$ or $f(e) \leq b$. In particular, e and b are comparable.*

To prove (3°) put

$$A_e = \{b \in A \mid b \leq e \text{ or } f(e) \leq b\}$$

We need to show that $A_e = A$. Since A is the unique minimal closed set this amounts to proving that A_e is closed.

Clearly $a \in A_e$. Let $b \in A_e$. If $b < e$, then as e is extreme, $f(b) \leq e$ and so $f(b) \in A_e$. If $b = e$, then $f(e) = f(b) \leq f(b)$ and again $f(b) \in A_e$. If $f(e) \leq b$, then $f(e) \leq b \leq f(b)$ and $f(e) \leq f(b)$ by transitivity. So in all cases $f(b) \in A_e$.

Let D be a non-empty chain in A_e and m its least upper bound. If $d \leq e$ for all d in D, then e is an upper bound for D and so $m \leq e$ and $m \in A_e$. So suppose that $d \nleq e$ for some $d \in D$. As $d \in A_e$, $f(e) \leq d \leq m$ and again $m \in A_e$.

We proved that A_e is closed. Thus $A_e = A$ and (3°) holds.

4°. *E is closed*

As already mentioned, $a \in E$. Let $e \in E$. To show that $f(e)$ is extreme let $b \in A$ with $b < f(e)$. By (3°) $b \leq e$ or $f(e) \leq b$. In the latter case is $b < b$, a contradiction. If $b < e$, then since e is extreme, $f(b) \leq e \leq f(e)$. If $e = b$, then $f(b) = f(e) \leq f(e)$. So $f(e)$ is extreme.

Let D be a non-empty chain in E and m its least upper bound. We need to show that m is extreme. Let $b \in A$ with $b < m$. As m is a least upper bound of D, b is not an upper bound and there exists $e \in D$ with $e \nleq b$. By (3°), e and b are comparable and so $b < e$. As e is extreme, $f(b) \leq e \leq m$ and so m is extreme. Thus E is closed.

As E is closed and $E \subseteq A$, $A = E$. Hence by (4°) , any two elements in A are comparable. So A is a closed chain and by (2°), the lemma holds. □

As an immediate consequence we get:

Corollary A.3.6. *Let M be a non-empty partially ordered set in which every non-empty chain has a least upper bound. Then M has a maximal element.*

Proof. Suppose not. For $m \in M$ let $U_m = \{u \in M \mid m < u\}$. Then U_m is not empty and so by the Axiom of choice there exists

$$f \in \bigtimes_{m \in M} U_m$$

Then f is a function from M to M and $m < f(m)$ for all $m \in M$. But this contradicts A.3.5. □

Lemma A.3.7. *Let M be any partial ordered set. Order the set of chains in M by inclusion. Then M has a maximal chain.*

Proof. Let $\mathcal{M}$ be the set of chains in M. The union of a chain in $\mathcal{M}$ is clearly a chain in M and is a least upper bound for the chain. Thus by A.3.6 $\mathcal{M}$ has a maximal element. □

Theorem A.3.8 (Zorn's Lemma)**.** *Let M be a nonempty partially ordered set in which every chain has an upper bound. Then M has a maximal element.*

Proof. By A.3.7 there exists a maximal chain C in M. By assumption C has an upper bound m. Let $l \in M$ with $m \leq l$. Then $C \cup \{m, l\}$ is a chain in M and the maximality of C implies $l \in C$. Thus $l \leq m$, $m = l$ and m is maximal element. □

As an application of Zorn's lemma we prove the Well-Ordering Principal.

Definition A.3.9. *(a) A totally ordered set M is called* well-ordered *if every non-empty subset of M has a minimal element.*

(b) We say that a set T can be well-ordered *if there exists a relation $\leq$ on T such that $(T, \leq)$ is a well ordered set.*

Example A.3.10. Let J be a non-empty well-ordered set and let $(I_j)_{j\in J}$ a family of non-empty well -ordered sets. Let m_j be the minimal element of I_j. For $a, b \in \bigtimes_{j\in J} I_j$ define

$$\operatorname{Supp}(a) = \{j \in J \mid a_j \neq m_j\} \quad J(a,b) = \{j \in J \mid a_j \neq b_j\}.$$

Put

$$K = \left\{a \in \bigtimes_{j\in J} I_j \;\middle|\; |\operatorname{Supp}(a)| \text{ is finite}\right\}.$$

Note that $J(a,b) \subseteq \operatorname{Supp}(a) \cup \operatorname{Supp}(b)$ and so $J(a,b)$ is finite for all $a \neq b \in K$ and we can define $j(a,b) \in J = \max J(a,b)$. Define an ordering on K by

$$a < b \qquad \Longleftrightarrow \qquad a \neq b \text{ and } a_j < b_j \text{ where } j = j(a,b)$$

We claim that this is a well ordering on K.

Suppose $a < b$ and $b < c$ and let $j = j(a,b)$ and $k = j(b,c)$. If $j \leq k$, then $a_l = b_l = c_l$ for all $l > k$ and $a_k \leq b_k < c_k$ so $a < c$. And if $j > k$, then $a_l = b_l = c_l$ for all $l > j$ and $a_j < b_j = c_j$ and again $a < c$. So K is totally ordered.

Let A be a non-empty subset of K. Suppose A has no minimal element. Note that if $b, a \in A$ with $b < a$ and $j = j(a,b)$, then $b_j < a_j$. So $a_j \neq m_j$ and $j(a,b) \in \operatorname{Supp}(a)$. Thus we can define

$$j(a) = \max_{\substack{b\in A\\ b<a}} j(a,b) \qquad \text{and} \qquad j = \min_{a\in A} j(a)$$

Under all $a \in A$ with $j(a) = j$ pick one with a_j minimal Let $b < a$. Then $j(a,b) \leq j(a)$ and so $a_k = b_k$ for all $k > j = j(a)$. Let $c < b$. Then $c < a$ and so also $a_k = c_k$ and an thus $j(b,c) \leq j$. Thus $j(b) \leq j$ and by minimality of j, $j(b) = j$. The minimality of a_j implies $b_j = a_j$. Since also $c < a$, we get $c_j = b_j$ and so $j(c,b) < j$. Thus implies $j(b) < j$, a contradiction.

Theorem A.3.11 (Well-ordering principal)**.** *Every set M can be well ordered.*

Proof. Let W be the set of well orderings $\alpha = (M_\alpha, \leq_\alpha)$ with $M_\alpha \subseteq M$. As the empty set can be well ordered, W is not empty. For $\alpha, \beta \in W$ define $\alpha \leq \beta$ if

< 1 $M_\alpha \subseteq M_\beta$

< 2 $\leq_\beta|_{M_\alpha} = \leq_\alpha$.

< 3 $a \leq_\beta b$ for all $a \in M_\alpha, b \in M_\beta \setminus M_\alpha$

It is easy to see that $\leq$ is a partial ordering on W. We would like to apply Zorn's lemma to obtain a member in W. For this let $\mathcal{A}$ be a chain in W. Put $M_* = \bigcup_{\alpha\in\mathcal{A}} M_\alpha$ and for $a, b \in M_*$ define $a \leq_* b$ if there exists $\alpha \in \mathcal{A}$ with $a, b \in M_\alpha$ and $a \leq_\alpha b$. Again it is readily verified that $\leq_*$ is a well-defined partial ordering on M_*. To show that $\leq_*$ is a well-ordering, let I be any non-empty subset of M^* and pick $\alpha \in \mathcal{A}$ so that $I \cap M_\alpha \neq \varnothing$. Let m be the least element of $I \cap M_\alpha$ with respect to $\leq_\alpha$. We claim that m is also the least element of I with respect to $\leq_*$. Indeed let $i \in I$. If $i \in M_\alpha$, then $m \leq_\alpha i$ by choice of m. So also $m \leq_* i$. If $i \notin M_\alpha$, pick $\beta \in \mathcal{A}$ with $i \in M_\beta$. As $\mathcal{A}$ is a chain, α and β are comparable.

As $i \in M_\beta \setminus M_\alpha$ we get $\alpha < \beta$ and (< 3) implies $m \leq_\beta i$. Again $m \leq_* i$ and we conclude that $(M_*, \leq_*)$ is a well-ordered set and so an element of W. Observe that $(M_*, \leq_*)$ is an upper bound for $\mathcal{A}$ in W.

So by Zorn's Lemma there exists a maximal element $\alpha \in W$. Suppose that $M_\alpha \neq M$ and pick $m \in M \setminus M_\alpha$. Define the partially ordered set $(M_*, \leq_*)$ by $M_* = M_\alpha \cup \{m\}$, $\leq_*|_{M_\alpha \times M_\alpha} = \leq_\alpha$ and $i <_* m$ for all $i \in M_\alpha$. Then $(M_*, \leq_*)$ is contained in W and $\alpha < (M_*, \leq_*)$, a contradiction to the maximality of α.

Thus $M_\alpha = M$ and $\leq_\alpha$ is a well-ordering on M. □

Remark A.3.12 (Induction)**.** *The well ordering principal allows to prove statement about the elements in an arbitrary set by induction.*

This works as follows. Suppose we like to show that a statement $P(m)$ is true for all elements m in a set M. Endow M with a well ordering $\leq$ and suppose that we can show

$$P(a) \text{ is true for all } a < m \qquad \Longrightarrow \qquad P(m) \text{ is true}$$

then the statement is to true for all $m \in M$.

Indeed suppose not and put $I = \{i \in M \mid P(i) \text{ is false }\}$. Then I has a least element m. Put then $P(a)$ is true for all $a < i$ and so $P(i)$ is true by the induction conclusion.

A.4 Ordinals

Definition A.4.1. *Let a, b be sets. Then $a \underline{\in} b$ means $a \in b$ or $a = b$.*

Definition A.4.2. *An ordinal is a set S such that*

(i) Each element of S is a subset of S.

(ii) $\underline{\in}$ is a well-ordering on S.

Example A.4.3. *The following sets are ordinals:*

$$\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, ...$$

If we denote $\varnothing$ by 0, $\{\varnothing\}$ by 1, $\{\varnothing, \{\varnothing\}\}$ by 2 and so on, then

$$n + 1 = n \cup \{n\} = \{0, 1, 2, \ldots, n\}.$$

Lemma A.4.4. *Let α, β and γ be a ordinal.*

(a) Define $\alpha + 1 = \alpha \cup \{\alpha\}$. Then $\alpha + 1$ is an ordinal.

(b) Every element of ordinal is an ordinal.

(c) Exactly one of $\beta \in \alpha, \alpha = \beta$ and $\beta \in \alpha$ holds.

(d) If $\alpha \in \beta$ and $\beta \in \gamma$. Then $\alpha \in \gamma$.

(e) $\alpha \in \beta$ *if and only if* $\alpha \subsetneq \beta$ *and if and only if* $\alpha + 1 \underline{\in} \beta$.

(f) $\alpha \underline{\in} b$ *if and only if* $\alpha \subseteq \beta$ *and if and only if* $\alpha \in \beta + 1$.

(g) Let A *be a non-empty set of ordinals, then* $\bigcap A$ *is an ordinal. Moreover,* $\bigcap A \in A$ *and so* $\bigcap A$ *is the minimal element of* A.

(h) Let A *be a set of ordinals. Then* $\bigcup A$ *is an ordinal.*

Proof. (a) Let $x \in \alpha + 1$. Then $x \in \alpha$ or $x = \alpha$. If $x \subseteq \alpha$ and so also $x \subseteq \alpha + 1$. Then $x = \alpha$, then again $x \subseteq \alpha$. So every element of $\alpha + 1$ is a subset of α. Now let y by any non-empty subset of $\alpha + 1$. If $y = \{\alpha\}$, then α is a minimal element of y. If $y \neq \{\alpha\}$, then $y \smallsetminus \{\alpha\}$ is a subset of α and so has minimal element m with respect to $\in$. Then $m \in \alpha$ and so m is also a minimal element of y. Since $z \in \alpha$ for all $z \in \alpha + 1$ with $z \neq \alpha$ it is readily verified that '$\in$' is a total ordering on $\alpha + 1$.

(b) Let $\beta \in \alpha$ and $\gamma \in \beta$. Since β is subset of α, γ is an element and so also a subset of α. If $\delta \in \gamma$, we conclude that $\delta \in \alpha$. Since $\delta \in \gamma$ and $\gamma \in \beta$ and '$\in$' is a transitive relation on α have that $\delta \in \beta$. Thus γ is a subset of β. Since '$\in$' is a well-ordering on α and β is a subset of α, '$\in$' is also a well-ordering on α.

(c) Let $\gamma \in \alpha$. By induction (on the elements of $\alpha + 1$) we may assume that $\gamma \in \beta$, $\gamma = \beta$ or $\beta \in \gamma$. If $\gamma = \beta$, then $\beta \in \alpha$. If $\beta \in \gamma$ then $\beta \in \alpha$, since γ is a subset of α. So we may assume that $\gamma \in \beta$ for all $\gamma \in \alpha$. Thus $\alpha \subseteq \beta$. We also may assume that $\alpha \neq \beta$ and so there exist δ minimal in β with $\delta \notin \alpha$. Let $\eta \in \delta$. Then $\eta \in \beta$ and so $\eta \in \alpha$ by minimality of δ. Thus $\delta \subseteq \alpha$. Since $\delta \notin \alpha$ and γ is both and element of α and a subset of α, $\delta \neq \gamma$ and $\delta \notin \gamma$. As both δ and γ are in β and '$\in$' is an ordering on β we conclude that $\gamma \in \delta$. Thus $\alpha \subseteq \delta$ and so $\alpha = \delta \in \beta$.

(d) This follows since β is a subset of γ

(e) and (f): If $\alpha \in \beta$, then since β is an ordinal. $\alpha \subseteq \beta$. Also no set is an element of itself and so $\alpha \neq \beta$ and

Suppose now that $\alpha \subsetneq \beta$. Then $\alpha \neq \beta$. Note also that $\beta \notin \beta$ and so $\beta \notin \alpha$. Thus (c) implies $\alpha \in \beta$ and so $\alpha + 1 = \alpha \cup \{\alpha\} \subseteq \beta$.

Thus

$$\alpha \in \beta \qquad \Longleftrightarrow \qquad \alpha \subsetneq \beta$$

and so also

$$\alpha \underline{\in} \beta \qquad \Longleftrightarrow \qquad \alpha \subseteq \beta$$

Thus

$$\alpha + 1 \underline{\in} \beta \iff \alpha + 1 \subseteq \beta \iff \alpha \subseteq \beta \text{ and } \alpha \in \beta \iff \alpha \subseteq \beta \text{ and } \alpha \subsetneq \beta \iff \alpha \subsetneq \beta$$

and

$$\alpha \in \beta + 1 \iff \alpha \in \beta \text{ or } \alpha = \beta \iff \alpha \underline{\in} \beta$$

So (e) and (f) are proved.

(g) Any subset of a well-ordered set is well-ordered. So $\bigcap A$ is well-ordered with respect to '$\in$. Let $x \in \bigcap A$. Then $x \in a$ for all $a \in A$ and so $x \subseteq a$ for all $a \in A$. Hence $x \subseteq \bigcup A$. Thus $\bigcup A$ is an ordinal. If $\bigcap A \neq a$ for all $a \in A$, then $\bigcap A \subsetneq a$ and by (e), $\bigcap A \in a$ for all $a \in A$. Hence $\bigcap A \in \bigcap A$, a contradiction to (e).

(h) Let $x_1, x_2, x_3 \in \bigcup A$. Then $x_i \in a_i$ for some $a_i \in A$. Then $x_i \subseteq a_i$ and so $x_i \subseteq A$. By (c) and (d) there exists $a \in \{a_1, a_2, a_3\}$ with $a_i \leq a$ for all a. Thus $x_1, x_2, x_3 \in a$. Since '$\in$' is an ordering on a we conclude that '$\in$' is also an ordering on $\bigcup A$. Let d be a non-empty subset of $\bigcup A$ and define $B = \{a \in A \mid d \cap a \neq \varnothing\}t$. By (g), B has a minimal element b. Then $b \cap d$ has a minimal element m and m is also a minimal element of d. Thus '$\in$' is a well-ordering on $\bigcup A$. □

Definition A.4.5. *(a) Let A be a set. $|A|$ is the smallest ordinal such that there exist a bijection from A to $|A|$. $|A|$ is called the cardinality of A.*

(b) A cardinal is the cardinality of some set.

(c) $\aleph_0$ is the smallest ordinal such that $\alpha + 1 \in \aleph_0$ for all $\alpha \in \aleph_0$.

(d) An ordinal α is called finite of $\alpha \in \aleph_0$.

(e) A set A is called finite if $|A|$ is finite, otherwise its called infinite. A is called countable infinite if $|A| = \aleph_0$. A is called countable if its finite or countable infinite. A is called uncountable if is not countable, that is $\aleph_0 \in |A|$.

(f) ω_1 is the smallest uncountable cardinal, that is ω_1 is the smallest cardinal with $\aleph_0 \in \omega_1$.

Lemma A.4.6. *(a) ω_1 has no maximal element.*

(b) Any countable subset of ω_1 has an upper bound in ω_1.

Proof. Note first that by minimal choice of ω_1, all elements of ω_1 are countable.

(a) Let $\alpha \in \omega_1$. Since α is countable, also $\alpha + 1$ is countable. So $\alpha + 1 \neq \omega_1$. Note that $\omega_1 \notin \alpha + 1$ and so by A.4.4(c) , $\alpha + 1 \in \omega_1$. So α is not maximal in ω_1 and so ω_1 has no maximal elements.

(b) Let A be a countable subset of ω_1 and put $\alpha = \bigcup A$. By A.4.4 α is an ordinal. Also all elements of ω_1 are subsets of ω_1 and so α is a subset of ω_1. Since countable unions of countable sets are countable, α is countable. The minimal choice of ω_1 shows that $\alpha \in \omega_1$ Let $b \in A$. Then $\beta \subseteq \alpha$ and so by A.4.4(f) $\beta \underline{\in} \alpha$. Thus α is an upper bound for A. □

Definition A.4.7. *Let G be a function and α an ordinal.*

(a) Let $f \in \mathrm{Fun}(\alpha)$. Then f is called G-defined if for all $\beta \in \alpha$, $f|_\beta \in \mathrm{Dom}(G)$ and $f(\beta) = G(f|_\beta)$.

(b) G is called an α-defining function if $f \in \mathrm{Dom}(G)$ for all $\beta \in \alpha$ and all G-defined $f \in \mathrm{Fun}(\beta)$.

Lemma A.4.8. *Let α be an ordinal and G an α-defining function. Then there exists a unique G-defined function $f \in \mathrm{Fun}(\alpha)$.*

Proof. Put

$$I = \{\gamma \underline{\in} \alpha \mid \text{ there exists a unique } G\text{-defined } g_\gamma \in \mathrm{Fun}(\gamma)\}$$

Let $\beta \underline{\in} \alpha$ with $\beta \subseteq I$. We will show that $\beta \in I$. Define $f \in \mathrm{Fun}(\beta)$ by $f(\gamma) = G(g_\gamma)$ for all $\gamma \in \beta$. Note here that $\gamma \in I$. Also $g_\gamma \in \mathrm{Dom}(G)$ since g_γ is G-defined and G is an α-defining function.

1°. *Suppose $\gamma \underline{\in} \beta$ and $h \in F(\gamma)$ is G-defined. Then $h = f|_{\gamma}$.*

Let $\delta \in \gamma$. Then $h|_{\delta}$ is G-defined and since $\delta \in \beta \subseteq I$, $h|_{\delta} = g_{\delta}$. Since h is G-defined

$$h(\delta) = G(h|_{\delta}) = G(g_{\delta}) = f(\delta).$$

2°. *f is G-defined.*

Let $\gamma \in \beta$. Then g_{γ} is G-defined and (1°) implies $f|_{\gamma} = g_{\gamma}$ and so

$$f|_{\gamma} \in \operatorname{Dom}(G) \qquad \text{and} \qquad f(\gamma) = G(g_{\gamma}) = G(f|_{\gamma})$$

Thus f is G-defined.

Conversely let $h \in \operatorname{Fun}(\beta)$ be G-defined. Then by (1°) $h = f$. So f is the unique G-defined function on β .

We proved that $\beta \in I$ for all $\beta \underline{\in} \alpha$ with $\beta \subseteq I$. Thus $\alpha \in I$ and the theorem is proved. □

Corollary A.4.9. *Let $H : A \to A$ be function and $a \in A$. Then there exists a unique family $(a_i)_{i \in \mathbb{N}}$ in A with with $a_0 = a$ and $Ha_i = a_{i+1}$ for all $i \in \mathbb{N}$.*

Proof. Let $i \in \mathbb{N}$ and $f \in \operatorname{Fun}(i, A)$. If $i = 0$ define $G(f) = a$. If $i > 0$ define $Gf = H(f(i-1))$. So G is function from $\bigcup_{i \in \mathbb{N}} \operatorname{Fun}(i, A)$ to A.

We claim that G is an $\mathbb{N}$-defining function. Let $i \in \mathbb{N}$ and let $f \in \operatorname{Fun}(i)$ be G-defined. Then $f|_{i-1}$ is G-defined and so by induction on i, $f|_{i-1}$ is contained in the domain of G. So $fj \in A$ for all $j < i-1$. Also $f(i-1) = H(f(i-1)) \in A$. Hence $f \in \operatorname{Fun}(i, A)$ and so $f \in \operatorname{Dom}(G)$.

We proved that G is an $\mathbb{N}$-defining function. Thus by A.4.8 there exists unique G-defined $f \in \operatorname{Fun}(\mathbb{N})$. If $i \in \mathbb{Z}^+$, then $fi = G(f|_i) = H(f(i-1)) \in \mathcal{D}$. Also $f0 = G(f|_{\varnothing}) = G(\varnothing) = a$.

Suppose $(b_i)_{i \in \mathbb{N}}$ is another family in A with $a = a_0$ and $Ha_i = a_{i+1}$. Then $b_0 = a = a_0$ and if $a_i = b_i$, then $a_{i+1} = Ha_i = Hb_i = b_{i+1}$. So by induction, $a_i = b_i$ for all $i \in \mathbb{N}$. □

Corollary A.4.10. *Let $(M, \leq)$ be a non-empty partially ordered set and suppose there does not exist a strictly increasing function $h : \mathbb{N} \to M$. Then M has a maximal element.*

Proof. Suppose not. Then for each $m \in M$, $M_m = \{n \in M \mid m < n\}$ is not empty. By the axiom of choice there exists $g \in \times_{m \in M} M_m$. So $g : M \to M$ is a strictly increasing function. Let $m \in M$. So by A.4.8 there exist a function $h : \mathbb{N} \to M$ with $h(0) = m$ and $h(i+1) = g(hi)) < hi$ for all $i \in \mathbb{N}$. Hence h is strictly increasing, contrary to the assumption. □

Corollary A.4.11. *Let $\mathcal{C}$ be a class of sets and $F \in \operatorname{Fun}(\mathcal{C})$ such that $\varnothing \neq F(a) \subseteq \mathcal{C}$ for all $a \in \mathcal{C}$. Let $a \in \mathcal{C}$. Then there exist a family $(a_i)_{i \in \mathbb{N}}$ in $\mathcal{C}$ with $a_0 = a$ and $a_{i+1} \in F(a_i)$ for all $i \in \mathbb{N}$.*

Proof. Let $\mathcal{D}$ be the class of subsets of $\mathcal{C}$. For $A \in \mathcal{D}$ define $H(A) = \bigcup_{a \in A} F(a)$. Then $H(A) \subseteq \mathcal{C}$ for all $A \in \mathcal{D}$ and so $H(A) \in \mathcal{D}$. Thus by A.4.9 there exists a family $(D_i)_{i \in \mathbb{N}}$ in $\mathcal{D}$ with $D_0 = \{a\}$ and $H(D_i) = D_{i+1}$ for all $i \in \mathbb{N}$. Thus $D = \bigcup_{i \in \mathbb{N}} D_i$ is a subset of $\mathcal{D}$ with $a \in D$. By axiom of choice $\bigtimes_{d \in D} F(s) \neq \varnothing$. So there exist function $T \in \operatorname{Fun}(D)$ with $Td \in F(d)$ for all. Let $d \in D$. Then $d \in D_i$ for some $i \in I$ and so $Td \in F(d) \subseteq H(D_i) = D_{i+1}$. So $Td \in D$ for all $d \in D$. Another application of

A.4.9 provides a family $(a_i)_{i\in\mathbb{N}}$ with $a_0 = a$ and $T(a_i) = a_{i+1}$ for all $i \in \mathbb{N}$. Thus $a_{i+1} = T(a_i) \in F(d_i)$ and the corollary is proved. □

Corollary A.4.12. *Let $\mathcal{D}$ be a class of sets, α an ordinal and $D \in \mathcal{D}$. Suppose that $\bigcup_{\gamma\in\beta} D_\gamma \in \mathcal{D}$ for all $\beta \in \alpha$ and all increasing families $(D_\gamma)_{\gamma\in\beta}$ in $\mathcal{D}$. Let $H : \mathcal{D} \to \mathcal{D}$ be an increasing function. Then there exists a unique family $(D_\beta)_{\beta\in\alpha}$ in $\mathcal{D}$ such that*

(a) $D_0 = D$,

(b) $H(D_i) = D_{i+1}$ for all $i \in \alpha$ with $i + 1 < \alpha$.

(c) $D_i = \bigcup_{j<i} D_j$ if $j \in \alpha$ is limit ordinal.

Proof. Let $\gamma \in \alpha$ and $f : \gamma \to \mathcal{D}$ be an increasing function. Define $Gf \in \mathcal{D}$ as follows:

If $\gamma = 0$, define $Gf = D$. If $\gamma = \rho + 1$, define $Gf = H(f\rho)$ and if γ is a non-zero limit ordinal define $Gf = \bigcup_{\delta\in\gamma} f\gamma$.

Note that

1°. *G is a function from $\bigcup_{\gamma\in\alpha} \mathrm{Fun}_{\mathrm{inc}}(\gamma, \mathcal{D})$ to $\mathcal{D}$.*

Next we show:

2°. *Let $\beta \underline{\in} \alpha$ and let $f \in \mathrm{Fun}(\beta)$ G-defined.*

(a) $f(0) = D$.

(b) $f(\gamma + 1) = H(f\gamma)$ for all $\gamma < \beta$ with $\gamma + 1 < \beta$.

(c) $f(\gamma) = \bigcup_{\delta<\gamma} f\delta$ if $\gamma < \beta$ is a limit ordinal.

(d) Then f is an increasing function from β to $\mathcal{D}$.

If $\beta = 0$, this is obvious. So suppose $\beta \neq 0$ and let $\gamma \in \beta$.

Then by definition of a G-defined function, $f\,|_\gamma \in \mathrm{Dom}(G)$ and

$$f\gamma = G(f\,|_\gamma)$$

In particular, $f\gamma \in \mathcal{D}$ and $f\,|_\gamma$ is an increasing function from γ to $\mathcal{D}$. Thus f is a function from β to $\mathcal{D}$.

(a) $f(0) = G(f\,|_0) = G(0) = D$.

(b) Suppose $\gamma + 1 < \beta$. Then

$$f(\gamma + 1) = G(f\,|_{\gamma+1}) = H\big((f\,|_{\gamma+1})\gamma\big) = H(f(\gamma))$$

(c) Suppose γ is a limit ordinal. Then

$$f(\gamma) = G(f\,|_\gamma) = \bigcup_{\delta<\gamma} (f\,|_\gamma)\delta = \bigcup_{\delta<\gamma} f\delta$$

(d) Let $\delta \in \gamma$. If γ is a limit ordinal, (c) shows that $f\delta \subseteq f\gamma$. So suppose $\gamma = \rho + 1$. Since $f\,|_\gamma$ is increasing $f\delta \subseteq f\rho$. By (b) and since H is increasing

$f\rho \subseteq H(f\rho) = f(\rho + 1) = f(\gamma)$ So again $f\delta \subseteq f\gamma$ and f is increasing. Thus also (d) holds.

3°. *G is an α-defining function.*

Let $\beta \in \alpha$, and $f \in \mathrm{Fun}(\beta)$ is G-defined. Then by (d) f is an increasing function from β to $\mathcal{D}$ and so $f \in \mathrm{Dom}(G)$. Hence (3°) holds.

By (3°) and A.4.8 there exists a unique G-defined function $f \in \mathrm{Fun}(\alpha)$. (2°) now shows that the lemma holds for $(fi)_{i\in\alpha}$. □

A.5 Cantor-Bernstein

Lemma A.5.1. *Let A and B be sets and suppose there exist 1-1 functions $f : A \to B$ and $g : B \to A$. Then there exists a bijection $h : A \to B$.*

Proof. Put $C = g(B)$, $D = g(f(A))$ and $\alpha = g \circ f$. Then α is 1-1, $D = \alpha(A)$, $D \subseteq C \subseteq A$. Since g is a bijection from B to C, its suffices to construct a bijection from A to C.

Let $E = \{\alpha^k(a) \mid a \in A \smallsetminus C, k \in \mathbb{N}\}$. Define

$$\beta : A \to A,\ a \to \begin{cases} \alpha(a) & \text{if } a \in E \\ a & \text{of } a \in A \smallsetminus E \end{cases}$$

Let $e \in E$. Then by definition of β, $\beta(e) = \alpha(e)$. By definition of E, $e = \alpha^k(x)$ for some $x \in A \smallsetminus C$ and some $k \in \mathbb{N}$. Thus $\beta(e) = \alpha(e) = \alpha^{k+1}(b) \in E$.

Let $a, b \in A$ with $\beta(a) = \beta(b)$. Suppose first that $a \notin E$. Then $\beta(b) = \beta(a) = a \notin E$. Since $\beta(e) \in E$ for all $e \in E$, this gives $b \notin E$ and so $a = \beta(b) = b$. Suppose that $a \in E$. Then also $b \in E$ and so $\alpha(a) = \beta(a) = \beta(b) = \alpha(b)$. Since α is 1-1, this gives $a = b$.

So β is 1-1. If $a \in E$, then $\beta(a) = \alpha(a) \in D \subseteq C$. Suppose $a \in A \smallsetminus E$. If $x \in A \smallsetminus C$, then $x = \alpha^0(x) \in E$. Thus $a \in C$ and so $\beta(a) = a \in C$. Hence $\beta(A) \subseteq C$.

Now let $c \in C$. If $c \in E$, then $c = \alpha^k(b)$ for some $b \in A \smallsetminus C$ and $k \in \mathbb{N}$. Since $c \in C$, $c \neq b = \alpha^0(b)$ and so $k > 0$. Then $x = \alpha^{k-1}(b) \in E$ and $\beta(x) = \alpha(x) = \alpha^k(b) = c$. So $c \in \beta(A)$.

Suppose that $c \notin E$. Then $\beta(c) = c$ and again ${}^{\in}\beta(A)$. Thus $C \subseteq \beta(A)$. So $\beta(A) = C$ and β is a bijection from A to C. □

A.6 Algebraic Structure

Definition A.6.1. *Let $(S_i)_{i\in I}$ be a family of set. Define*

$$\bigotimes_{i\in I} S_i = \bigtimes_{\substack{i\in I \\ S_i \neq \varnothing}} S_i$$

Definition A.6.2 (Structures)**.** *Let S be set.*

(a) *Let I and K be sets. An I-ary operation on S with constants K is a function f such that $S^I \circledast K$ is contained in the domain of S.*

Such an operation is called closed on S if

$$f(x) \in S$$

for all $x \in S^I \circledast K$.

(b) An operation on S is an I-ary operation on S with constants K for some set I and K.

(c) A structure $\mathcal{G}$ on S is set of triple (I, K, f) such that f is closed I-ary operation with constants K on S.

(d) Let $\mathcal{G}$ be a structure on S. A subset T of S is called $\mathcal{G}$-closed if $\mathcal{G}$ is a structure on T, that is

$$f(x) \in T$$

for all $(I, K, f) \in \mathcal{G}$ and $x \in T^I \circledast K$.

A $\mathcal{G}$-closed subsets of S is also called a $\mathcal{G}$-subset of S.

Example A.6.3. (a) Let G be a group. Let $\mathcal{G}$ be the structure in G consisting of

$$\begin{array}{rrlr}
f_1: & G \times G \circledast \varnothing & \to G & (a,b) \to ab \\
f_2: & G \circledast \varnothing & \to G & a \to a^{-1} \\
f_3: & \varnothing \circledast \{0\} & \to G & 0 \to e_G \\
f_4: & G \circledast G & \to G & (a,b) \to {}^b a
\end{array}$$

Here the set on the right side of $\circledast$ is the set of constants.

Then $T \subseteq G$ is $\mathcal{G}$-closed if and only if

$$\begin{array}{rclcl}
ab & = & f_1(a,b) & \in T & \text{for all } a, b \in T \\
a^{-1} & = & f_2(a) & \in T & \text{for all } a \in T \\
e_G & = & f_3(0) & \in T & \\
{}^b a & = & f_4(a,b) & \in T & \text{for all } a \in T, b \in G
\end{array}$$

So the $\mathcal{G}$-closed subsets of G are the normal subgroups of G. If we remove the function f_4 from $\mathcal{G}$, the $\mathcal{G}$-closed subsets of G is would be subgroups of G.

(b) Consider a group G acting on a set S. Let $\mathcal{G}$ be the structure on S given by

$$f_1: \quad S \circledast G \to S, (s,g) \to gs$$

Let $T \subseteq S$. Then T is $\mathcal{G}$-closed if and only if

$$gt = f_1(t,g) \in T \text{ for all } t \in T, g \in G$$

So T is $\mathcal{G}$-closed if and only if T is G-invariant.

(c) Consider a ring R. Let $\mathcal{G}$ be the structure on R given by

$$\begin{array}{llll} f_1: & R \times R \circledast \varnothing & \to R & (a,b) \to a+b \\ f_2: & R \circledast \varnothing & \to R & a \to -a \\ f_3: & \varnothing \circledast \{0\} & \to R & 0 \to 0_R \\ f_4: & R \circledast R & \to R & (a,b) \to ba \end{array}$$

Let $I \subseteq R$. Then I is $\mathcal{G}$-closed if and only if

$$\begin{array}{rcccl} a+b & = & f_1(a,b) & \in T & \text{for all } a,b \in T \\ -a & = & f_2(a) & \in T & \text{for all } a \in T \\ 0_R & = & f_3(0) & \in T & \\ ba & = & f_4(a,b) & \in T & \text{for all } a \in T, b \in R \end{array}$$

So the $\mathcal{G}$- subsets of R are just the left ideals in R.

If we replace f_4 by

$$f_5: \quad R \times R \circledast \varnothing \to R, \quad (a,b) \to ab$$

the closed subsets will be the subrings.

If we replace f_4 by

$$f_6: \quad R \circledast R \to R, \quad (a,b) \to ab$$

the $\mathcal{G}$-subsets will be the right ideals in R. If we use f_4 and f_6, the $\mathcal{G}$-closed subsets will be the ideals

Proposition A.6.4. *$\mathcal{G}$ be a structure on the set S and $(T_q)_{q \in Q}$ a non-empty family of $\mathcal{G}$-closed subsets of S. Then $\bigcap_{q \in Q} T_q$ is $\mathcal{G}$-closed.*

Proof. Put $T = \bigcap_{q \in Q} T_q$. Let $(I,K,f) \in \mathcal{G}$ and $x = (y,k) \in T^I \circledast K$. Let $q \in Q$ and note that $y_i \in T_q$ for all $i \in I$. Thus $x \in T_q^I \circledast K$ and since T_q is $\mathcal{G}$-closed we get $f(x) \in T_q$. Since this holds for all $q \in Q$, $f(x) \in T$. Thus T is $\mathcal{G}$-closed. □

Definition A.6.5. *A family $(T_q)_{q \in Q}$ of sets is called directed if for each $q, p \in Q$ there exists $r \in Q$ with $T_q \cup T_p \subseteq T_r$.*

Proposition A.6.6. *Let $\mathcal{G}$ be a structure on the set S and $(T_q)_{q\in Q}$ a non-empty family of $\mathcal{G}$-closed subsets of S. Suppose that*

(i) $(T_q)_{q\in Q}$ *is directed.*

(ii) I *is finite for all* $(I,K,f)\in\mathcal{G}$.

Then $\bigcup_{q\in Q} T_q$ *is* $\mathcal{G}$*-subset of* S.

Proof. Put $T=\bigcup_{q\in Q}T_q$. Fix $(I,K,f)\in\mathcal{G}$ and let $x=(y,k)\in T^I\circledast K$. Then for each $i\in I$ there exists $q_i\in Q$ with $y_i\in T_{q_i}$. Since I is finite and $(T_q)_{q\in Q}$ is directed we can choose $q\in Q$ with $T_{q_i}\subseteq T_q$ for all $i\in I$. Thus $y_i\in T_q$ for all $i\in I$ and so $x\in T_q^I\circledast K$. Since T_q is $\mathcal{G}$-closed we get $f(x)\in T_q\subseteq T$. Thus T is $\mathcal{G}$-closed . □

Corollary A.6.7. *(a) Let G be a group and* $(G_q)_{q\in Q}$ *a non-empty family of (normal,) subgroups of G. Then* $\bigcap_{q\in Q}T_q$ *is a (normal,)subgroup of G.*

(b) Let G be a group and $(G_q)_{q\in Q}$ *a non-empty directed family of (normal,)subgroups of G. Then* $\bigcup_{q\in Q}T_q$ *is a (normal,) subgroup of G.*

(c) Let R be a ring and $(I_q)_{q\in Q}$ *a non-empty family of (left,right,) ideals in R. Then* $\bigcap_{q\in Q}I_q$ *is an (left,right,) ideal in R.*

(d) Let R be a ring and $(I_q)_{q\in Q}$ *a non-empty direct family of (left,right,) ideals in R. Then* $\bigcup_{q\in Q}I_q$ *is an (left,right,)ideal in R.*

Definition A.6.8. *Let* $\mathcal{G}$*-be a structure of the set* S *and* T *a subset of* G*. The set*

$$\langle T\rangle_{\mathcal{G}}:=\bigcap\{H\mid T\subseteq H\subseteq S, H \text{ is } \mathcal{G}\text{-closed}\}$$

is called the $\mathcal{G}$*-subset generated by* T*, or the* $\mathcal{G}$*-closure of* T.

Appendix B

Categories

B.1 Definition and Examples

In this chapter we give a brief introduction to categories.

Definition B.1.1. *A* category Cat *is a triple of* $(\mathcal{C}, \mathrm{Hom}, \mathrm{Com})$ *such that*

(i) *$\mathcal{C}$ is class;*

(ii) Hom *is a function from $\mathcal{C} \times \mathcal{C}$ to the class of sets;*

(iii) Com *is a function with domain $\mathcal{C} \times \mathcal{C} \times \mathcal{C}$ such that for each $A, B, C \in \mathcal{C}$,* $\mathrm{Com}(A, B, C)$ *is a function*

$$\mathrm{Com}(A, B, C) : \mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$$

(iv) *the elements of $\mathcal{C}$ are called the objects of* Cat.

(v) *If A and B are objects and $f \in$* $\mathrm{Hom}(A, B)$ *are then the triple (f, A, B) id called a morphism from A to B and is denoted by $f : A \to B$. (Note here that f does not have to be a function from A to B.*

(vi) *For objects A, B, C and morphisms $f : A \to B$ and $g : B \to C$ we denote* $\mathrm{Com}(A, B, C)(g, f)$ *by $g \circ f$. (Note that this is a bit ambiguous, since $g \circ f$ also depends on A, B and C, but this should not lead to confusion). $g \circ f$ is called the composition of g and f. If $\mathbb{f} = (f, A, B)$ and $\mathbb{g} = (g, B, C)$ we write $\mathbb{g} \circ \mathbb{f}$ for $(g \circ f, A, C)$. Note that the notation $\mathbb{g} \circ \mathbb{f}$ is unambiguous.*

(vii) *If $f : A \to B$, $g : B \to C$ and $h : C \to D$ are morphisms then*

$$h \circ (g \circ f) = (h \circ g) \circ f$$

(viii) *For each object A there exists a morphism from A to A, denoted by* id_A*, such that for all morphism $f : A \to B$ and $g : B \to A$*

$$f \circ \mathrm{id}_A = f \qquad \textit{and} \qquad \mathrm{id}_A \circ g = g$$

Definition B.1.2. *Let* Cat *be a category..*

(a) A morphism $f : A \to B$ is called an equivalence *if there exists a morphism $g : B \to A$ with*

$$f \circ g = \mathrm{id}_B \qquad \textit{and} \qquad g \circ f = id_A$$

(b) Two objects A and B are called equivalent *if there exists an equivalence $f : A \to B$.*

Remark B.1.3. *Let* Cat *be a category.*

(a) The composition of two equivalences in a category is an equivalence.

(b) Let A be an object. Then $(\mathrm{Hom}(A,A), \mathrm{Com}(A,A,A))$ is a monoid. $f : A \to A$ is an equivalence if an only if f is invertible in $\mathrm{Hom}(A,A)$. So the set of equivalences from A to A form a group.

Proof. Straightforward. □

Example B.1.4. *1. Let $\mathcal{S}$ be the class of all sets. Let $\mathrm{Hom}(A,B) = \mathrm{Fun}(A,B)$ be the set of all functions from $A \to B$. Let $\mathrm{Com}(A,B,C)$ be regular composition. Then $(\mathcal{S}, \mathrm{Hom}, \mathrm{Com})$ is a category called the category of sets. A morphism in this category is an equivalence if an only if it is a bijection.*

2. The class of all groups with morphisms the group homomorphisms and the regular composition is a category called the category of groups.

3. By Remark B.1.3 a category with one objects is essentially the same thing as a monoid.

4. Let G be a monoid. Let $\mathcal{C} = G$. For $a, b \in G$ define $\mathrm{Hom}(a,b) = \{x \mid xa = b\}$. So $x : a \to b$ means $xa = b$. Define composition by multiplication. If $x : a \to b$ and $y : b \to c$ are morphisms then

$$(yx)a = y(xa) = yb = c$$

and so yx is indeed morphism from a to c. Note that e_G is the identity in $\mathrm{Hom}(a,a)$ for all $a \in G$. So $(\mathcal{C}, \mathrm{Hom}, \mathrm{Com})$ is category.

5. The class of all partially ordered sets with morphisms the increasing functions and regular composition is category.

6. Let $(I, \leq)$ be a partially ordered set. Let $a, b \in I$. If $a > b$ define $\mathrm{Hom}(a,b) = \varnothing$. If $a \leq b$ let $\mathrm{Hom}(a,b)$ have a single element, which we denote by "$a \to b$". Define composition by

$$(b \to c) \circ (a \to b) = (a \to c).$$

this is well defined as partial orderings are transitive. Associativity is obvious. Since $\leq q$ is reflexive $a \to a$ is an identity for A. So (I, Hom, Com) is a category.

Conversely, suppose Cat *is a category such that $\mathcal{C}$ is a set and $|\mathrm{Hom}(A,B)| \leq 1$ for all $A, B \in \mathcal{C}$. Define $A \leq B$ if $|\mathrm{Hom}(A,B)| = 1$. Then $(\mathcal{C}, \leq)$ is a partially ordered set.*

7. *Let* Cat *be any category. Let $\mathcal{D}$ be the class of morphisms in* Cat. *Given morphisms $f : A \to B$ and $g : C \to D$ in $\mathcal{C}$ define* Hom$(\mathbb{f}, \mathbb{g})$ *to be the sets of all pairs* $(\mathbb{a}, \mathbb{b})$ *where $a : A \to C$ and $b : B \to D$ are morphism such that $g \circ a = b \circ f$, that is the diagram:*

$$\begin{tikzcd}
A \arrow[r, "a"] \arrow[d, "f"'] & C \arrow[d, "g"] \\
B \arrow[r, "b"] & D
\end{tikzcd}$$

commutes.

If $h : E \to F$ is a further morphism and $(\mathbb{c}, \mathbb{d}) \in$ Hom$(\mathbb{g}, \mathbb{h})$ *define* $(\mathbb{a}, \mathbb{b}) \circ (\mathbb{c}, \mathbb{d}) = (\mathbb{a} \circ \mathbb{c}, \mathbb{b} \circ \mathbb{d})$. *Then* $(\mathbb{a}, \mathbb{b}) \circ (\mathbb{c}, \mathbb{d}) \in$ Hom$(\mathbb{f}, \mathbb{h})$*:*

$$\begin{tikzcd}
A \arrow[r, "a"] \arrow[d, "f"'] & C \arrow[r, "c"] \arrow[d, "g"] & E \arrow[d, "h"] \\
B \arrow[r, "b"] & D \arrow[r, "d"] & F
\end{tikzcd}$$

The resulting category is called the category of morphisms for Cat.

8. *Let* Cat *be a category. The* opposite *category* Cat$^{\mathrm{op}}$ *is defined as follows: The objects of* Cat$^{\mathrm{op}}$ *are the objects of* Cat.

Hom$^{\mathrm{op}}(A, B) =$ Hom(B, A) *for all objects A, B.*

$f \in$ Hom$^{\mathrm{op}}(A, B)$ *will be denoted by*

$$f : A \overset{op}{\to} B \quad or \quad f : A \leftarrow B.$$

$$f \overset{op}{\circ} g = g \circ f.$$

The opposite category is often also called the dual *or* arrow reversing *category. Note that two objects are equivalent in $\mathcal{C}$ if and only if they are equivalent in $\mathcal{C}^{\mathrm{op}}$.*

B.2 Universal Objects and Products

Definition B.2.1. *(a) An object I in a category is called* universal *(or* initial*) if for each object C of $\mathcal{C}$ there exists a unique morphism $I \to C$.*

(b) An object I in a category is called couniversal *(or* terminal*) if for each object C of $\mathcal{C}$ there exists a unique morphism $C \to I$.*

Note that I is initial in $\mathcal{C}$ if and only if its terminal in $\mathcal{C}^{\mathrm{op}}$.

The initial and the terminal objects in the category of groups are the trivial groups.

Let I be a partially ordered set. A object in $\mathcal{C}_I$ is initial if an only if its a least element. Its terminal if and only if its a greatest element.

Let G be a monoid and consider the category $\mathcal{C}(G)$. Since $g : e \to g$ is the unique morphism form e to G, e is a initial object. e is a terminal object if and only if G is a group.

Theorem B.2.2. [**uniuni**] *Any two initial (resp. terminal) objects in a category I are equivalent.*

Proof. Let A and B be initial objects. In particular, there exists $f : A \to B$ and $g : B \to A$. Then id_A and $g \circ f$ both are morphisms $A \to A$. So by the uniqueness claim in the definition of an initial object, $\mathrm{id}_A = g \circ f$, by symmetry $\mathrm{id}_B = f \circ g$.

Let A and B be terminal objects. Then A and B are initial objects in $\mathcal{C}^{\mathrm{op}}$ and so equivalent in $\mathcal{C}^{\mathrm{op}}$. Hence also in $\mathcal{C}$. □

Definition B.2.3. *Let $\mathcal{C}$ be a category and $(A_i, i \in I)$ a family of objects in $\mathcal{C}$. A* product *for $(A_i, i \in I)$ is an object P in $\mathcal{C}$ together with a family of morphisms $\pi_i : P \to A_i$ such that any object B and family of homomorphisms $(\phi_i : B \to A_i, i \in I)$ there exists a unique morphism $\phi : B \to P$ so that $\pi_i \circ \phi = \phi_i$ for all $i \in I$. That is the diagram commutes:*

$$\begin{tikzcd}
P \arrow[rr, "\phi"] \arrow[dr, "\pi_i"'] & & B \arrow[dl, "\phi_i"] \\
& A_i &
\end{tikzcd}$$

commutes for all $i \in I$.

Any two products of $(G_i, i \in I)$ are equivalent in $\mathcal{C}$. Indeed they are the terminal object in the following category $\mathcal{E}$

The objects in $\mathcal{E}$ are pairs $(B, (\phi_i, i \in I))$ there B is an object and $(\phi_i : B \to A_i, i \in I)$ is a family of morphism. A morphism in $\mathcal{E}$ from $(B, (\phi_i, i \in I))$ to $(D, (\psi_i, i \in I)$ is a morphism $\phi : B \to D$ with $\phi_i = \psi_i \circ \phi$ for all $i \in I$.

A *coproduct* of a family of objects $(G_i, i \in I)$ in a category $\mathcal{C}$ is its product in $\mathcal{C}^{\mathrm{op}}$. So it is an initial object in the category $\mathcal{E}$. This spells out to:

Definition B.2.4. *Let $\mathcal{C}$ be a category and $(A_i, i \in I)$ a family of objects in $\mathcal{C}$. A* coproduct *for $(A_i, i \in I)$ is an object P in $\mathcal{C}$ together with a family of morphisms $\pi_i : A_i \to B$ such that for any object B and family of homomorphisms $(\phi_i : A_i \to B, i \in I)$ there exists a unique morphism $\phi : P \to B$ so that $\phi \circ \pi_i = \phi_i$ for all $i \in I$.*

Bibliography

[Gro] Larry C. Grove, *Algebra* Pure and Applied Mathematics 110, Academic Press, (1983) New Work.

[Hun] Thomas W. Hungerford, *Algebra* Graduate Text in Mathematics 73, Springer-Verlag (1974) New York.

[Lan] Serge Lang, *Algebra* Addison-Wesley Publishing Company, (1965) New York.