Honors Algebra II
Lecture Notes for MTH 418/419
Fall 2006/Spring 2007

Ulrich Meierfrankenfeld

September 1, 2009

Chapter 1

Preface

These are the lecture notes for the class MTH 418/419 which taught in F06/S07 at Michigan State University.

Contents

1.1 Sets

Naively a set S is collection of objects such that for each object x either x is *contained* in S or x is not contained in S. We use the symbol '$\in$' to express containment. So $x \in S$ means that x is contained in S and $x \notin S$ means that x is not contained in S. Thus we have

$$\text{For all objects } x: \quad x \in S \quad \text{or} \quad x \notin S.$$

You might think that every collection of objects is a set. But we will now see that this cannot be true. For this let A be the collection of all sets. Suppose that A is a set. Then A is contained in A. This already seems like a contradiction . But a set may be contained in itself. So we need to refine our argument. We say that a set S is nice if S is not contained in S. Now let B be the collection of all nice sets. Suppose that B is a set. Then either B is contained in B or B is not contained in B.

Suppose that B is contained in B. Since B is the collection of all nice sets we conclude that B is nice. The definition of nice now implies that B is not contained in B, a contradiction.

Suppose that B is not contained in B. Then by definition of 'nice', B is a nice set. But B is the collection of all nice sets and so B is contained in B, again a contradiction.

This shows that B cannot be a set. Therefore B is a collection of objects, but is not a set.

What kind of collections of objects are sets is studied in Set Theory.

The easiest of all sets is the *empty set* denoted by $\{\}$ or $\emptyset$. The empty set is defined by

$$\text{For all objects } x: \quad x \notin \emptyset.$$

So the empty set has no members.

Given an object s we can form the *singleton* $\{s\}$, the set whose only member is s:

$$\text{For all objects } x: \quad x \in \{s\} \text{ if and only if } x = s$$

If A and B is a set then also its union $A \cup B$ is a set. $A \cup B$ is defined by

$$\text{For all objects } x: x \in A \cup B \text{ if and only if } x \in A \text{ or } x \in B.$$

The *natural numbers* are defined as follows:

$$\begin{array}{rcrcrcr}
0 & := & & & & & \emptyset \\
1 & := & 0 \cup \{0\} & = & \{0\} & = & \{\emptyset\} \\
2 & := & 1 \cup \{1\} & = & \{0,1\} & = & \{\emptyset, \{\emptyset\}\} \\
3 & := & 2 \cup \{2\} & = & \{0,1,2\} & = & \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 & := & 4 \cup \{4\} & = & \{0,1,2,3\} & = & \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
n+1 & := & n \cup \{n\} & = & \{0,1,2,3,\ldots n\} & &
\end{array}$$

One of the axioms of set theory says that the collection of all the natural numbers

$$\{0,1,2,3,4,\ldots\}$$

is a set. We denote this set by $\mathbb{N}$.

Addition on $\mathbb{N}$ is defined as follows: $n + 0 := n$, $n + 1 := n \cup \{n\}$ and inductively

$$n + (m+1) := (n+m) + 1.$$

Multiplication on $\mathbb{N}$ is defined as follows: $n \cdot 0 := n$, $n \cdot 1 := n$ and inductively

$$n \cdot (m+1) := (n \cdot m) + n.$$

1.2 Functions and Relations

We now introduce two important notations which we will use frequently to construct new sets from old ones. Let $I_1, I_2, \ldots I_n$ be sets and let Φ be some formula which for given elements $i_1 \in I_1, i_2 \in I_2, \ldots, i_n \in I_n$ allows you to compute a new object $\Phi(i_1, i_2, \ldots, i_n)$. Then

$$\{\Phi(i_1, i_2, \ldots, i_n) \mid i_1 \in I_1, \ldots, i_n \in I_n\}$$

is the set defined by

$$x \in \{\Phi(i_1, i_2, \ldots, i_n) \mid i_1 \in I_1, \ldots, i_n \in I_n\}$$

$$\text{if and only}$$

$$\text{there exist objects } i_1, i_2, \ldots, i_n \text{ with } i_1 \in I_1, i_2 \in I_2, \ldots, i_n \in I_n \text{ and } x = \Phi(i_1, i_2, \ldots, i_n) \ .$$

In Set Theory it is shown that $\{\Phi(i_1, i_2, \ldots, i_n) \mid i_1 \in I_1, \ldots, i_n \in I_n\}$ is indeed a set.

Let P be a statement involving a variable t. Let I be set. Then

$$\{i \in I \mid P(i)\}$$

is the set defined by

$$x \in \{i \in I \mid P(i)\} \quad \text{if and only if} \quad x \in I \text{ and } P \text{ is true for } t = x.$$

Under appropriate conditions it is shown in Set Theory that $\{i \in I \mid P(i)\}$ is a set.

Let a and b be objects. Then the *ordered pair* (a, b) is defined as $(a, b) := \{\{a\}, \{a, b\}\}$. We will prove that

$$(a, b) = (c, d) \text{ if and only if } a = c \text{ and } b = d.$$

For this we first establish a simple lemma:

Lemma 1.2.1. [**a=b**] *Let u, a, b be objects with $\{u, a\} = \{u, b\}$. Then $a = b$.*

Proof. We consider the two cases $a = u$ and $a \neq u$.

Suppose first that $a = u$. Then $b \in \{u, b\} = \{u, a\} = \{a\}$ and so $a = b$.

Suppose next that $a \neq u$. Since $a \in \{u, a\} = \{u, b\}$, $a = u$ or $a = b$. But $a \neq u$ and so $a = b$. □

Proposition 1.2.2. [**ordered pairs**] *Let a, b, c, d be objects. Then*

$$(a, b) = (c, d) \textit{ if and only if } a = c \textit{ and } b = d.$$

Proof. Suppose $(a, b) = (c, d)$. We need to show that $a = c$.

We will first show that $a = b$. Since

$$\{a\} \in \{\{a\}, \{a, b\}\} = (a, b) = (c, d) = \{\{c\}, \{c, d\}\},$$

we have

$$\{a\} = \{c\} \quad \text{or} \quad \{a\} = \{c, d\}.$$

In the first case $a = c$ and in the second $c = d$ and again $a = c$.

From $a = c$ we get $\{\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\} = \{\{a\}, \{a, d\}$. So by 1.2.1 $\{a, b\} = \{a, d\}$ and applying 1.2.1 again, $b = d$. □

If I and J are sets we define $I \times J := \{(i, j) \mid i \in I, j \in J\}$.

A *relation* on I and J is a triple $r = (I, J, R)$ where R is a subset $I \times J$. If $i \in I$ and $j \in J$ we write irj if $(i, j) \in R$.

For example let $R := \{(n, m) \mid n, m \in \mathbb{N}, n \in m\}$ and let $<$ be the triple $(\mathbb{N}, \mathbb{N}, R)$. Let $n, m \in \mathbb{N}$. Then $n < m$ if and only if $n \in m$. Since $m = \{0, 1, 2, \ldots, m - 1\}$ we see that $n < m$ if and only if n is one of $0, 1, 2, 3, \ldots, m - 1$.

A *function* from I to J is a relation $f = (I, J, R)$ on I and J such that for each $i \in I$ there exists a unique $j \in J$ with $(i, j) \in R$. We denote this unique j by $f(i)$. So for $i \in I$ and $j \in J$ the following three statements are equivalent:

$$ifj \iff (i,j) \in R \iff j = f(i).$$

We denote the function $f = (I, J, R)$ by

$$f : I \to J, \quad i \to f(i).$$

So $R = \{(i, f(i)) \mid i \in I\}$.

For example

$$f : \mathbb{N} \to \mathbb{N}, \quad m \to m^2$$

denotes the function $(\mathbb{N}, \mathbb{N}, \{(m, m^2) \mid n \in \mathbb{N}\})$

Informally, a function f from I to J is a rule which assigns to each element i of I a unique element $f(i)$ in J.

A function $f : I \to J$ is called *1-1* or *injective* if $i = k$ whenever $i, k \in I$ with $f(i) = f(k)$.

f is called *onto* or *surjective* if for each $j \in I$ there exists $i \in I$ with $f(i) = j$. Observe that f is 1-1 and onto if and only if for each $j \in J$ there exists a unique $i \in I$ with $f(i) = j$.

If $f : I \to J$ and $g : J \to K$ are functions, then the *composition* $g \circ f$ of g and f is the function from I to K defined by $(g \circ f)(i) = g(f(i))$ for all $i \in I$.

id_I denotes the function $\mathrm{id}_I, I \to T, i \to i$. id_I is called the *identity function* on I.

A function $f : I \to J$ is called *bijective* if there exists a function $g : J \to I$ with $f \circ g = \mathrm{id}_J$ and $g \circ f = \mathrm{id}_I$.

Lemma 1.2.3. [**char bijective**] *A function $f : A \to B$ is bijective if and only if it's $1 - 1$ and onto.*

Proof. $\Longrightarrow$: Suppose first that f is bijective. Then by definition there exists a function $g : B \to A$ with $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. To show that f is 1-1, let $a, d \in A$ with $f(a) = f(d)$. Then

$$a = \mathrm{id}_I(a) = (g \circ f)(a) = g(f(a)) = g(f(d)) = (g \circ f)(d) = \mathrm{id}_A(d) = d$$

and so f is 1-1.

To show that f is onto, let $b \in B$. Put $a = g(b)$. Then $a \in A$ and

$$f(a) = f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b$$

and so f is onto.

$\Longleftarrow$: Suppose that f is $1 - 1$ and onto. Let $b \in B$. Since f is onto, there exists $b' \in A$ such that

$$f(b') = b$$

Since f is 1-1, b' is unique. Thus we can define

$$g : B \to A, b \to b'$$

Let $b \in B$. Then

$$(f \circ g)(b) = f(g(b)) = f(b') = b = \mathrm{id}_B(b)$$

and so

$$f \circ g = \mathrm{id}_B$$

Let $a \in A$ and put $b = f(a)$. Since $f(a) = b$ we have $a = b'$ and so

$$(g \circ f)(a) = g(f(a)) = g(b) = b' = a = \mathrm{id}_A(a)$$

Thus $g \circ f = \mathrm{id}_A$. Hence f is bijective. □

1.2.4 (Well-Defined Functions)**.** [**well-defined**]

We will often define a function from A to B as follows

$$(*) \qquad f : A \to B, \mathrm{P}(i) \to \mathrm{Q}(i)$$

where $\mathrm{P}(i)$ and $Q(i)$ are formulas involving a variable i which runs through some index set I. So a better version of (*) is

$$(**) \qquad f : A \to B, \mathrm{P}(i) \to \mathrm{Q}(i) \text{ for } i \in I$$

(**) can be turned into a precise definition:

$$(***) \qquad f = (A, B, R) \text{ where } R = \{(\mathrm{P}(i), \mathrm{Q}(i)) \mid i \in I\}$$

We see now that in order for (*) to really define a function from A to B the following conditions must be met

(i) [**i**] It must be clear from the context what the index set I is, or I must be explicitly stated as in (**).

(ii) [**ii**] For each $i \in I$, $\mathrm{P}(i)$ is an element of A. In particular, it must the possible to evaluate $\mathrm{P}(i)$ for each i in I.

(iii) [**iii**] For each $i \in I$, $\mathrm{Q}(i)$ is an element of B. In particular, it must the possible to evaluate $\mathrm{Q}(i)$ for each i in I.

(iv) [**iv**] For each $a \in A$ there exists $i \in I$ with $\mathrm{P}(i) = a$.

(v) [**v**] If $i, j \in I$ with $\mathrm{P}(i) = \mathrm{P}(j)$, then $\mathrm{Q}(i) = \mathrm{Q}(j)$.

If all of the above five conditions are met we say that f as in (*) is a *well-defined* function. The following examples might help to understand the concept 'well-defined': Consider

$$f : \mathbb{R} \to \mathbb{R}, x^2 \to \frac{1}{x}$$

Already Condition (i) is not quite fulfilled. But let's assume that $I = \mathbb{R}$. Then (ii) is fulfilled, but (iii) is not, since $\frac{1}{0}$ is not defined. We fix this problem by choosing $I = \mathbb{R} \setminus 0$. Then (i)-(iii) are fulfilled, but (iv) is not, since a negative number is not the square of a real number. So let's consider

$$g : \mathbb{R}^+ \to \mathbb{R}, x^2 \to \frac{1}{x} \text{ for } x \in \mathbb{R} \setminus \{0\},$$

where $\mathbb{R}^+$ is the set of positive real numbers.

Now (i)-(iv) holds, but (v) fails since $1^2 = (-1)^2$ but $\frac{1}{1} \neq \frac{1}{-1}$. Also this problem can be overcome:

$$h : \mathbb{R}^+ \to \mathbb{R}, x^2 \to \frac{1}{x} \text{ for } x \in \mathbb{R}^+$$

Now all five conditions are met and h is a well-defined function.

Chapter 2

Groups

2.1 Definition and Examples

Definition 2.1.1. [**def:binary op**] *Let G be a set. A* binary operation *on G is a function $* : G \times G \to A$, where A is some set. We denote the image of (s,t) under $*$ by $s * t$. A binary operation $*$ is called* closed *if*

$$a * b \in G \textit{ for all } a, b \in G$$

$\mathbb{Z}$ denotes the set of *integers*, so $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$. $\mathbb{Q}$ denotes the set of *rational numbers*, so $\mathbb{Q} = \{\frac{n}{m} \mid n, m \in \mathbb{Z}, m \neq 0\}$. $\mathbb{R}$ is the set of *real numbers* and $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ is the set of *complex numbers.* We assume that the reader is familiar with the basic properties of integers and rational, real and complex numbers.

Example 2.1.2. [**ex:binary op**]

(a) [**1**] $+ : \mathbb{Z} \times \mathbb{Z}, (n, m) \to n + m$ is a closed binary operation.

(b) [**2**] $\Box : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \to \mathbb{Q}, (n, m) \to \frac{n}{m}$ is a binary operation on $\mathbb{Z}$, but is not closed, since for example $1 \Box 2 = \frac{1}{2}$ is not contained in $\mathbb{Z}$.

Definition 2.1.3. [**def:group**] *Let $*$ be a binary operation on a set G. Then $(G, *)$ is a* group*provided that*

(i) [**i**] *$a * b \in G$ for all $a, b \in G$, that is $*$ is closed.*

(ii) [**ii**] *$(a*b)*c = a*(b*c)$ for all $a, b, c \in G$ (such a binary operation is called* associative*).*

(iii) [**iii**] *There exists $e \in G$ with $a * e = a = e * a$ for all $a \in G$. Such e is called an* identity *an identity in G with respect to $*$.*

(iv) [**iv**] *For all $a \in G$ there exists $b \in G$ with $a * b = e = b * a$. Such b is called an inverse of a in G with respect to $*$.*

Example 2.1.4. [**ex:groups**]

(a) [**a**] $(\mathbb{Z}, +)$ is a group.

(b) [**b**] $(\mathbb{N}, +)$ is not a group since the positive integers have no inverses.

(c) [**c**] $(\mathbb{R}, +)$ is a group.

(d) [**d**] $(\mathbb{R}, \cdot)$ is not a group, since 0 does not have an inverse.

(e) [**e**] Let $S = \{x \in \mathbb{C} \mid ||x|| = 1\}$ where $||a + ib|| = \sqrt{a^2 + b^2}$. Then $(S, \cdot)$ is a group. Indeed, let $x, y \in S$. Then $||xy|| = ||x|| \cdot ||y|| = 1 \cdot 1$ and so S is closed under multiplication. Multiplication of complex numbers is associative. $||1|| = 1$ and so $1 \in S$ and $(S, \cdot)$ has an identity. For $x = a + ib$ define $\overline{x} = a - ib$. Then $x\overline{x} = a^2 + b^2 = ||x||^2$. So if $x \in S$, then $\overline{x}$ is an inverse of x in S.

Lemma 2.1.5. [**symmetric group**] *Let I be a set and define*

$$\mathrm{Sym}(I) := \{f : I \to I \mid f \textit{ is bijective } \}$$

Then $(\mathrm{Sym}(I), \circ)$ *is a group.* $\mathrm{Sym}(I)$ *is called the* symmetric group *on I*

Proof. We need to verify the four axioms of a group.

(i): To show that $\circ$ is closed on $\mathrm{Sym}(I)$, let $f, g \in \mathrm{Sym}(I)$. Then f and g are bijective and so by 1.2.3 f and g are 1-1 and onto. We will show that also $f \circ g$ is 1-1 and onto. Let $i, j \in I$ with $(f \circ g)(i) = (f \circ g)(j)$. Then

$$f(g(i)) = f(g(j))$$

Since f is 1-1 this implies, $g(i) = g(j)$. As g is 1-1, we conclude that $i = j$ and so $f \circ g$ is 1-1.

Let $k \in I$. Since f is onto there exists $j \in I$ with $f(j) = k$. Since g is onto, there exists $i \in I$ with $g(i) = j$. Thus

$$(f \circ g)(i) = f(g(i)) = f(j) = k$$

and so $f \circ g$ is onto. We proved that $f \circ g$ is 1-1 and onto. Hence by 1.2.3, $f \circ g$ is bijective. It follows that $f \circ g \in \mathrm{Sym}(I)$ and so $\circ$ is closed on $\mathrm{Sym}(i)$.

(ii): To show that $\circ$ is associative, let $f, g, h \in \mathrm{Sym}(I)$. let $i \in I$. Then

$$(f \circ (g \circ h))(i) = f((g \circ h)(i)) = f(g(h(i)))$$

and

$$((f \circ g) \circ h)(i) = (f \circ g)(h(i)) = f(g(h(i)))$$

$$(f \circ (g \circ h))(i) = ((f \circ g) \circ h)(i)$$

for all $i \in I$. This just means that $f \circ (g \circ h) = (f \circ g) \circ h$ and so $\circ$ is associative.

(iii): We have

$$(f \circ \mathrm{id}_I)(i) = f(\mathrm{id}_I(i)) = f(i)$$

and so $f = f \circ \mathrm{id}_I$. Similarly, $\mathrm{id}_I \circ f = f$ and so id_I is an identity element in $\mathrm{Sym}(I)$ with respect to $\circ$.

(iv): Let $f \in \mathrm{Sym}(I)$. Then f is bijective and so by definition there exists $g : I \to I$ with $f \circ g = \mathrm{id}_I = \gamma \circ f$.

If follows that g is bijective, $g \in \mathrm{Sym}(I)$ and g is an inverse of f in $\mathrm{Sym}(I)$ with respect to $\circ$.

We verified the four axioms of a group and so $(\mathrm{Sym}(I), \circ)$ is a group. □

If n is a positive integer, then $\mathrm{Sym}(n) := \mathrm{Sym}(\{1, 2, 3, \ldots, n\})$. Elements of $\mathrm{Sym}(I)$ are also called *permutations* of I. So a permutation of I is just a 1-1 and onto function from I to itself.

Let $\pi \in \mathrm{Sym}(n)$. Then we denote π by

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n-1) & \pi(n) \\ & & & & & \end{pmatrix}.$$

For example

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

denotes the permutation of π of $[1 \ldots 5]$ with $\pi(1) = 2, \pi(2) = 1, \pi(3) = 4, \pi(4) = 5$ and $\pi(5) = 3$.

Almost always we will use the more convenient *cycle* notation:

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

denotes the permutation π with $\pi(a_{i,j}) = a_{i+1,j}$ and $\pi(a_{k_j,j}) = a_{1,j}$ for all $1 \leq i < k_j$ and $1 \leq j \leq l$. For example

$$(1, 3)(2, 4)$$

denotes the permutation with $\pi(1) = 3$, $\pi(3) = 1$, $\pi(2) = 4$ and $\pi(4) = 2$ and

$$(1, 3, 5)(2, 4)(6)$$

denotes the permutation with

$\pi(1) = 3$, $\pi(3) = 5$, $\pi(5) = 1$, $\pi(2) = 4$, $\pi(4) = 2$ and $\pi(6) = 6$.

Usually we skip cycles of length 1 in the cycle notation. So $(1,3,4) = (1,3,4)(2)$. Note that the cycle notation is not unique, for example

$$(1,2,4)(3,5) = (2,4,1)(3,5) = (4,1,2)(5,3)$$

As a further example we compute $(1,2) \circ (1,3)$ and $(1,3) \circ (1,2)$. In the following

$$i \xrightarrow{\pi} j$$

means that $\pi(i) = j$. We have

$$\begin{array}{ccccc} 1 & \xrightarrow{(1,3)} & 3 & \xrightarrow{(1,2)} & 3 \\ 3 & \xrightarrow{(1,3)} & 1 & \xrightarrow{(1,2)} & 2 \\ 2 & \xrightarrow{(1,3)} & 2 & \xrightarrow{(1,2)} & 1 \end{array}$$

and so

$$(1,2) \circ (1,3) = (1,3,2)$$

Also

$$\begin{array}{ccccc} 1 & \xrightarrow{(1,2)} & 2 & \xrightarrow{(1,3)} & 2 \\ 2 & \xrightarrow{(1,2)} & 1 & \xrightarrow{(1,3)} & 3 \\ 3 & \xrightarrow{(1,2)} & 3 & \xrightarrow{(1,3)} & 1 \end{array}$$

and so

$$(1,3) \circ (1,2) = (1,2,3)$$

In particular, we see that $(1,2) \circ (2,3) \neq (2,3) \circ (1,3)$. We call a group *abelian* if $a * b = b * a$ for all $a, b \in G$. $\mathrm{Sym}(n)$ for $n \geq 3$ is an example of a non-abelian group.

2.2 Elementary Properties of Groups

The remaining assertions are proved similarly.

Lemma 2.2.1 (Cancellation Law)**.** [**cancellation**] *Let G be a group and $a, b, c \in G$. Then*

$$\begin{aligned} & ab = ac \\ \Longleftrightarrow \quad & b = c \\ \Longleftrightarrow \quad & ba = ca \ . \end{aligned}$$

Proof. Suppose first that

$$ab = ac \tag{1}$$

Since G is a group there exists an inverse d of a in G. So

$$da = e \tag{2}$$

Multiplying (1) from the left with d gives:

$$d(ab) = d(ac)$$

Since multiplication is associative we conclude

$$(da)b = (da)c$$

Using (2) this implies

$$eb = ec$$

and since e is an identity

$$b = c$$

If $b = c$, then clearly $ab = ac$. So the first two statements are equivalent. Similarly the last two statements are equivalent. □

Lemma 2.2.2. [**a-1a**] *Let $(G, *)$ be a group.*

(a) [**a**] *G has a unique identity.*

(b) [**b**] *Each $a \in G$ has a unique inverse a^{-1}.*

(c) [**c**] *$(a^{-1})^{-1} = a$ for all $a \in G$.*

(d) [**d**] *$(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in G$.*

Proof. (a) Let e and f be identities of G with respect to $*$. We need to show that $e = f$. Consider hf. Since e is an identity $hf = e$. Since f is an identity, $ef = f$. Hence $e = f$.

(b) Let b and c be inverse of a. Then $ab = e$ and $ac = e$. So $ab = ac$ and by the Cancellation Law 2.2.1, $b = c$. So a has a unique inverse.

(c) By definition of a^{-1} we have $aa^{-1} = e = a^{-1}a$. Hence a is an inverse of a^{-1} and so $(a^{-1})^{-1} = a$.

(d) We compute:

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)(a^{-1}) = aa^{-1} = e$$

and similarly

$$(b^{-1}a^{-1})(ab) = e$$

So $b^{-1}a^{-1}$ is an inverse of ab, that is $(ab)^{-1} = b^{-1}a^{-1}$. □

2.3 Subgroups

Definition 2.3.1. [**defsubgroup**] *Let $(G, *)$ and $(H, \cdot)$ be groups. Then $(H, \cdot)$ is called a* subgroup *of $(G, *)$ provided that:*

(i) [**i**] $H \subseteq G$.

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

Lemma 2.3.2. [**properties subgroup**] *Let $(G, *)$ be a group and $(H, \cdot)$ a subgroup of $(G, *)$. Then*

(a) [**a**] $e_H = e_G$ *where e_H is the identity of H with respect to $\cdot$ and e_G is the identity of G with respect to $*$. In particular, $e_G \in H$.*

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

(c) [**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)

$$e_H * e_H = e_H \cdot e_H = e_H = e_H * e_G$$

So the Cancellation law 2.2.1 implies that $e_H = e_G$.

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

(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

$$a * b = a \cdot b = e_H = e_H = a * c$$

So by the Cancellation Law 2.2.1 $b = c$. □

Lemma 2.3.3. [**char subgroup**] *Let $(G, *)$ be a group and $H \subseteq G$. Suppose that*

(i) [**a**] $e \in H$

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

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

Define $\cdot : H \times H \to G, (a, b) \to a * b$. Then $(H, \cdot)$ is a subgroup of $(G, *)$.

Proof. We will first verify that $(H, \cdot)$ is a group.

By (ii), $\cdot$ is closed.

Let $a, b, c \in H$. Then since $H \subseteq G$, a, b, c are in H. Thus since $*$ is associative,

$$(a \cdot b) \cdot c = (a * b) * c = a * (b * c) = a \cdot (b \cdot c)$$

and so $\cdot$ is associative.

By (i), $e \in H$. Let $h \in H$. Then $e \cdot h = e * h = h$ and similarly $h \cdot e = h$ for all $h \in h$. So e is an identity of H with respect to $\cdot$.

Let $h \in H$. Then by (iii), $h^{-1} \in H$. Thus $h \cdot h^{-1} = h * h^{-1} = e$ and similarly $h^{-1} \cdot h = e$. Thus h^{-1} is an inverse of h with respect to $\cdot$.

So $(H, \cdot)$ is a group. By assumption H is a subset of G and by definition of $\cdot$, $a \cdot b = a * b$ for all $a, b \in H$. So $(H, \cdot)$ is a subgroup of $(G, *)$. □

Let $(G, *)$ be a group and H be a subset of G. We denote the binary operation, $H \times H \to G, (a, b) \to a * b$ by $* \mid_H$. So if H fulfills the three conditions in 2.3.3 then $(H, * \mid_H)$ is a subgroup of $(G, *)$. Slightly abusing notation, we will often say that $(H, *)$ is a subgroup of $(G, *)$ or even sloppier that H is a subgroup of G.

Example 2.3.4. [**ex:subgroup**]

1. [**1**] The even integers under addition form a subgroup of the integers under addition. Indeed we have

   (i) [**1i**] 0 is an even integer.

   (ii) [**1ii**] The sum of two even integers is an even integer.

   (iii) [**1iii**] The negative of an even integer is an even integer.

   So we see that the three conditions of 2.3.3 are fulfilled.

2. [**2**] Let n be an integer and put $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. So $n\mathbb{Z}$ consists of all the multiples of n. Then $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$. Indeed for $k, l \in n\mathbb{Z}$ we have

   (i) [**2i**] $0 = n \cdot 0 \in n\mathbb{Z}$.

   (ii) [**2ii**] $nk + nl = n(k + l) \in n\mathbb{Z}$.

   (iii) [**2iii**] $-nk = n(-k) \in n\mathbb{Z}$

   So again the three conditions of 2.3.3 are fulfilled.

3. [**3**] Let $(G, *)$ be any group. Then $(G, *)$ is a subgroup of G and also $(\{e\}, *)$ is a subgroup of $(G, *)$.

4. [**4**] Let $S = \{x \in \mathbb{C} \mid ||x|| = 1\}$. By 2.1.4(e), $(S, \cdot)$ is a group and so by definition of a subgroup, $(S, \cdot)$ is a subgroup of $(\mathbb{C} \setminus \{0\}, \cdot)$.

5. [**5**] Let I be a set and J a subset of I. Define

$$\mathrm{Stab}_{\mathrm{Sym}(I)}(J) := \{\alpha \in \mathrm{Sym}(I) \mid \alpha(j) = j \text{ for all } j \in J\}$$

$\mathrm{Stab}_{\mathrm{Sym}(I)}(J)$ called the *stabilizer* of J in $\mathrm{Sym}(I)$. We claim that $\mathrm{Stab}_{\mathrm{Sym}(I)}(J)$ is a subgroup of $\mathrm{Sym}(I)$. To verify this put $H := \mathrm{Stab}_{\mathrm{Sym}(I)}(J)$. Let $\delta \in \mathrm{Sym}(I)$. The definition of H implies that

$$\delta \in H \iff \delta(j) = j \text{ for all } j \in J.$$

Let $\alpha, \beta \in H$ and $j \in J$. Then

$$\alpha(j) = j \text{ and } \beta(j) = j$$

We compute

(i) [**5i**] $\mathrm{id}_I(j) = j$ and so $\mathrm{id}_I \in H$.

(ii) [**5ii**] $(\alpha \circ \beta)(j) = \alpha(\beta(j)) = \alpha(j) = j$ and so $\alpha \circ \beta \in H$.

(iii) [**5iii**] Applying α^{-1} to both sides of $\alpha(j) = j$ we get $\alpha^{-1}(\alpha(j)) = \alpha^{-1}(j)$. Since $\alpha \circ \alpha^{-1} = \mathrm{id}_I$ this gives $j = \alpha^{-1}(j)$ and so $\alpha^{-1} \in H$.

Thus by 2.3.3 H is a subgroup of $\mathrm{Sym}(I)$.

6. [**6**] Let G be a group and I a subset of G. Define

$$\mathrm{C}_G(I) := \{g \in G \mid g * i = i * g \text{ for all } i \in I\}$$

$\mathrm{C}_G(I)$ is called the *centralizer* of I in G. We will use 2.3.3 to show that $\mathrm{C}_G(I)$ is a subgroup of G. let $i \in I$.

(i) [**6i**] $e * i = i = i * e$ and so $e \in \mathrm{C}_G(I)$.

(ii) [**6ii**] Let $a, b \in \mathrm{C}_G(I)$. Then $a * i = i * a$ and $b * i = i * b$ and so

$$(a * b) * i = a * (b * i) = a * (i * b) = (a * i) * b = (i * a) * b = i * (a * b)$$

Hence $a * b \in \mathrm{C}_G(I)$.

(iii) [**6iii**] Let $a \in \mathrm{C}_G(I)$. Then $a * i = i * a$. Multiplication with a^{-1} from the left and then from the right gives

$$(a^{-1} * (a * i)) * a^{-1} = (a^{-1} * (i * a)) * a^{-1}$$

Using the associative law a few times we get

$$((a^{-1} * a) * i) * a^{-1} = a^{-1} * (i * (a * a^{-1}))$$

and so

$$(e * i) * a^{-1} = a^{-} * (i * e)$$

and

$$i * a^{-1} = a^{-1} * i$$

Hence $a^{-1} \in \mathrm{C}_G(I)$.

Thus by 2.3.3 $\mathrm{C}_G(I)$ is a subgroup of G.

Since the last two example have been rather abstract we now work out a couple of special cases.

7. [**7**] What is $H := C_{\mathrm{Sym}(5)}(\{2,5\})$? By definition H consists of all permutations α of $\{1,2,3,4,5\}$ which fix 2 and 5, (that is $\alpha(2) = 2$ and $\alpha(5) = 5$).

$$\begin{aligned} H \quad = \quad \{ \quad (1)(2)(3)(4)(5) \quad , \quad (1,3)(2)(4)(5) \quad , \quad (1,5)(2)(3)(4) \quad , \quad (1,4)(2)(3)(5) \quad , \\ (1,3,4)(2)(5) \quad , \quad (1,4,3)(2)(5) \quad \} \end{aligned}$$

Note that H is essentially the same as $\mathrm{Sym}(\{1,3,4\})$.

8. [**8**] Let G be the set of invertible 2×2 matrices over $\mathbb{R}$. Then G is a group under matrix multiplication. Let $A := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. What is $\mathrm{C}_G(\{A\})$? Let $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We have

$$B \in C_G(A) \iff AB = BA$$

Since

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ -c & -d \end{pmatrix}$$

and

$$BA = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} a & -b \\ c & -d \end{pmatrix}$$

So

$$AB = BA \iff a = a, b = -b, -c = c, d = d \iff b = c = 0$$

Thus

$$\mathrm{C}_G(\{A\}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| \, a, d \in \mathbb{R} \setminus \{0\} \right\}$$

Lemma 2.3.5. [**intersection**] *Let $(H_i \mid i \in I)$ be a family of subgroups of G. Then $\bigcap\limits_{i\in I} H_i$ is a subgroup of G.*

Proof. Recall first that by definition of the intersection of subsets:

$$a \in \bigcap_{i\in I} H_i \iff a \in H_i \text{ for all } i \in I$$

Since $e \in H_i$ for all $i \in I$, $e \in \bigcap_{i\in I} H_i$.

Let $a, b \in \bigcap_{i\in I} H_i$. Then $a, b \in H_i$ for all $i \in I$ and so since H is a subgroup of G, $ab \in H_i$ and $a^{-1} \in H_i$ for all i. Hence $ab \in \bigcap_{i\in I} H_i$ and $a^{-1} \in \bigcap_{i\in I} H_i$. Thus $\bigcap_{i\in I} H_i$ is a subgroup of G. □

Definition 2.3.6. [**def:generated**] *Let G be a group.*

(a) [**a**] *$H \leq G$ means that H is a subgroup of G.*

(b) [**b**] *Let $A \subseteq G$. Then*

$$\langle A\rangle := \bigcap\{H \mid A \subseteq H \leq G\}$$

$\langle A\rangle$ is called the subgroup of G generated *by A.*

Lemma 2.3.7. [**generated**] *Let G be a group and A be a subset of I. Then*

$$\langle A\rangle = \{a_1a_2\dots a_n \mid n \in \mathbb{N}, a_i \in A \cup A^{-1}\}$$

where $A^{-1} := \{a^{-1} \mid a \in A\}$, and if $n = 0$, $a_1 \dots a_n$ is defined to be e.

Proof. Let $B := \{a_1a_2\dots a_n \mid n \in \mathbb{N}, a_i \in A \cup A^{-1}\}$. We will first show that $B \subseteq \langle A\rangle$. For this let $A \subseteq H \leq G$, $n \in \mathbb{N}$ and $a_i \in A \cup A^{-1}$ for $1 \leq i \leq n$. Since H is closed under inverses, $a_i \in H$. Since H is closed under multiplication, $a_1 \dots a_n \in H$ (note that this is also true for $n = 0$ since $e \in H$. Thus $B \leq H$ for any such H. Since $\langle I\rangle$ is the intersection of all such H's, $B \subseteq \langle I\rangle$.

Next we will show that B is a subgroup of G. Choose $n = 0$ we see that $e \in B$. If $b = a_1a_2\dots a_n \in B$, then

$$b^{-1} = a_n^{-1} \dots a_1^{-1}$$

Moreover $a_i^{-1} \in A \cup A^{-1}$ and so $b^{-1} \in B$. So B is closed under inverses. Clearly B is closed under multiplication and so B is a subgroup of G. Taking $n = 1$ we see that $A \subseteq \langle A\rangle$. Hence B is a subgroup of G containing A. Since $\langle I\rangle$ is the intersection of such subgroups, $\langle I\rangle \subseteq B$.

From $\langle I\rangle \subseteq B$ and $B \subseteq \langle I\rangle$ we have $\langle I\rangle = B$ □

Example 2.3.8. [**ex:generated**]

1. [**1**] Let G be a group and $g \in G$. Define $\langle g \rangle := \langle \{g\} \rangle$. We can apply 2.3.7 to $A = \{g\}$. Then $A \cup A^{-1} = \{g, g^{-1}\}$. Hence each element of $\langle g \rangle$ has the form

$$\underbrace{gg\dots g}_{n_1\text{-times}}\underbrace{g^{-1}g^{-1}\dots g^{-1}}_{n_2\text{-times}}\underbrace{gg\dots g}_{n_3\text{-times}}\underbrace{g^{-1}g^{-1}\dots g^{-1}}_{n_4\text{-times}}\dots$$

After cancelling adjacent g and g^{-1} we see that this equals

$$\underbrace{gg\dots g}_{n\text{-times}} \text{ or } \underbrace{g^{-1}g^{-1}\dots g^{-1}}_{m\text{-times}},$$

depending on whether there are more g or g^{-1}-terms. We denote this element by g^n and g^{-m} respectively. Hence

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

2. [**2**] Let $g = (12345) \in \mathrm{Sym}(5)$. We compute

$$\begin{array}{llll}
g^0 & = & (1) & \\
g^1 & = & (12345) & \\
g^2 & = & (13524) & \\
g^3 & = & (14253) & \\
g^4 & = & (15432) & \\
g^5 & = & (1) & = & g^0 \\
g^6 & = & (12345) & = & g \\
\vdots & & & \\
g^{-1} & = & (15432) & = & g^4 \\
g^{-2} & = & (14253) & = & g^3 \\
g^{-3} & = & (13524) & = & g^2 \\
g^{-4} & = & (12345) & = & g \\
g^{-5} & = & (1) & = & g^0 \\
g^{-6} & = & (15432) & = & g^4 \\
\vdots & & &
\end{array}$$

Thus

$$\langle (12345) = \{(1), (12345), (13524), (14253), (15432)\}$$

2.4 Lagrange's Theorem

Definition 2.4.1. [**def:equiv rel**] *A relation $\sim$ on a set I is called an* equivalence relation *provided that*

(i) [**i**] *$\sim$ is* reflexive*, that is $a \sim a$ for all $a \in I$.*

(ii) [**ii**] *$\sim$ is* symmetric*, that is if $a, b \in I$ with $a \sim b$, then $b \sim a$.*

(iii) [**iii**] *$\sim$ is* transitive*, that is if $a, b, c \in I$ with $a \sim b$ and $b \sim c$, then $a \sim b$.*

Example 2.4.2. [**ex:equiv rel**]

1. [**1**] $\leq$ is reflexive and transitive but not symmetric on $\mathbb{N}$. Hence $\leq$ is not an equivalence relation.

2. [**2**] Let $f : I \to J$ be a function and for $i, k \in I$ define the relation $\sim$ on I by $i \sim k$ if $f(i) = f(k)$. Then $\sim$ is an equivalence relation on I.

3. [**3**] Let G be a group and H a subgroup of G. Define the relation $\sim_H$ on I by $a \sim_H b$ if $a^{-1}b \in H$. We will verify that $\sim$ is an equivalence relation. For this let $a, b, c \in G$.

   (i) [**3i**] $a^{-1}a = e \in H$. So $a \sim_H a$ and $\sim_H$ is reflexive.

   (ii) [**3ii**] Suppose $a \sim_H b$. Then $a^{-1}b \in H$ and so also $(a^{-1}b)^{-1} \in H$. Thus $b^{-1}a \in H$ and $b \sim_H a$. So $\sim$ is symmetric.

   (iii) [**3iii**] Suppose $a \sim_H b$ and $b \sim_H c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$. Hence also $(a^{-1}b)(b^{-1}c) \in H$ and $a^{-1}c \in H$. Thus $a \sim_H c$ and $\sim_H$ is transitive.

   Thus $\sim$ is an equivalence relation.

Lemma 2.4.3. [**equiv rel**] *Let $\sim$ be an equivalence relation on the set I. For $a \in I$ put $[i] := \{j \in I \mid i \sim j\}$. $[i]$ is called the* equivalence class *of $\sim$ determined i. Let $I/\sim$ be the set of equivalence classes of I. So*

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

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

(b) [**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 an 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 2.4.4. [**def:coset**] *Let H be a subgroup of the group G and $g \in G$. Then*

$$gH := \{gh \mid h \in H\}$$

gH is called the (left) coset *of H in G determined by g.*

G/H is the set of cosets of H in H. So

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

Proposition 2.4.5. [**prep lagrange**] *Let H be a subgroup of G and $g \in G$.*

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

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

(c) [**c**] *$|gH| = |H|$.*

Proof. (a) We have

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

So $gH = [g]$.

(b) This follows from (a) and 2.4.3

(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 $h = h'$ by the Cancellation Law 2.2.1. Hence f is 1-1. This gives (c). □

Theorem 2.4.6 (Lagrange)**.** [**lagrange**] *Let H be a subgroup of the group G. Then*

$$|G| = |G/H| \cdot |H|$$

In particular, if G is finite, then the order of any subgroup of G divides the order of G.

By 2.4.5 $|C| = |H|$ for all $C \in G/H$. By 2.4.3(b) applied to the equivalence relation $\sim_H$ we have

$$|G| = \sum_{C \in G/H} |C| = \sum_{C \in G/H} |H| = |G/H| \cdot |H|$$

□

Example 2.4.7. [**ex:lagrange**] Let $G = \mathrm{Sym}(3)$ and $H = \langle (1,2) \rangle = \{(1), (1,2)\}$. Then

$$\begin{gathered} (1) \circ H = H = \{(1), (1,2)\} \\ (1,2,3) \circ H = \{(1,2,3) \circ (1), (1,2,3) \circ (1,2)\} = \{(1,2,3), (1,3)\} \\ (1,3,2) \circ H = \{((1,3,2) \circ (1), (1,3,2) \circ (1,2)\} = \{(1,3,2), (2,3)\} \end{gathered}$$

Each element of Sym(3) lies in one of these three cosets, so this must be all the cosets. It might also be worthwhile to point out that

$$H = (1,2) \circ H$$

since H is a coset of H containing H. Similarly

$$(1,2,3) \circ H = (1,3) \circ H \text{ and } (2,3) \circ H = (1,3,2) \circ H$$

Hence

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

So by Lagrange's

$$6 = 3 \cdot 2$$

Definition 2.4.8. [**def:order**] *Let G be a group.*

(a) [**a**] *G is called cyclic if there exists $g \in G$ with $G = \langle g \rangle$.*

(b) [**b**] *Let $g \in G$. Then $|g| := |\langle g \rangle|$. $|g|$ is called the* order *of g.*

Lemma 2.4.9. [**order**] *Let G be a group, $g \in G$ and put $n := |g|$.*

(a) [**a**] *If n is infinite, then $g^m \neq e$ for all $0 \neq m \in \mathbb{Z}$. Moreover, $g^i \neq g^j$ for all $i \neq j \in \mathbb{Z}$.*

(b) [**b**] *Suppose n is finite.*

- *(a)* [**a**] *n is the smallest positive integer with $g^n = e$.*
- *(b)* [**b**] *Let $m \in \mathbb{Z}$ and let d be the remainder of m when divided by n. Then $g^m = g^d$.*
- *(c)* [**c**] *$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ and $g^i \neq g^j$ for all $0 \leq i < j < n$.*
- *(d)* [**d**] *Let $m \in \mathbb{Z}$. Then $g^m = e$ if and only if n divides m.*

(c) [**c**] *Suppose G is finite. Then*

- *(a)* [**a**] *n is finite.*
- *(b)* [**b**] *n divides $|G|$.*
- *(c)* [**c**] *$g^{|G|} = e$.*

Proof. Suppose there exists a positive integer with $g^k = e$. We will show that

$$\langle g \rangle = \{e, g, \ldots, g^{k-1}\} \tag{1}$$

For this let $h \in \langle g \rangle$. Then by 2.3.8(1), $h = g^m$ for some $m \in \mathbb{Z}$. let $m = kl + d$ with $l, d \in \mathbb{Z}$ and $0 \leq d < k$. Then

$$g^m = g^{kl+d} = g^{kl}g^d = (g^k)^l g^d = e^l g^d = g^d \tag{2}$$

Thus (1) holds. It follows that

$$n = |\langle g\rangle| \leq k \tag{3}$$

(a) Suppose that n is infinite. Then (3) shows that there does not exist a positive integer k with $g^k = e$. In other words, $g^k \neq e$ for all $k \in \mathbb{Z}^+$. Then also $g^{-k} = (g^k)^{-1} \neq e$. if $i, j \in \mathbb{Z}$ with $g^i = g^j$, then $g^{i-j} = g^i(g^j)^{-1} = e$ and so $i - j = 0$ and $i = j$. Thus (a) holds.

(b) Suppose now that n is finite. Then the elements

$$e, g, g^2, \dots, g^n$$

cannot be pairwise distinct (since otherwise $\langle g\rangle$ would contain $n+1$ distinct elements) and so there exists $0 \leq s < t \leq n$ with $g^s = g^t$. Then $g^{t-s} = g^t(g^s)^{-1} = e$. So by (3) applied to $k = t - s$, $n \leq t - s$. Since $0 \leq s < t \leq n$ this implies $s = 0$, $t = n$. In particular $g^i \neq g^j$ for all $0 \leq i < j < n$. Moreover, $g^n = e$. Together with (3) we conclude that n is the smallest positive integer with $g^n = e$. From (1) and (2) applied with $n = k$ we see that (b) holds.

(c) Suppose that G is finite. Since $\langle g\rangle \leq G$ also $\langle g\rangle$ is finite. So n is finite. Since $\langle g\rangle$ is a subgroup of G, Lagrange's Theorem says that $n = |\langle g\rangle|$ divides $|G|$. Hence the remainder of $|G|$ when divided by n is 0. Thus by (b:b), $g^{|G|} = g^0 = e$. So also (c) is proved. □

Example 2.4.10. [**ex:cyclic**] Let $G = \mathrm{Sym}(4)$. Let $g \in \mathrm{Sym}(4)$. Then by 2.4.9, $|g|$ is the smallest positive integer n with $g^n = e = (1)$. Moreover n divides $|G| = 4! = 24$ and $\langle g\rangle = \{(1), g, g^2, \dots, g^{n-1}\}$. We verify this for a few particular choices of g.

(a) [**a**] $g = (1)$. Then $g^1 = (1)$, $|g| = 1$, 1 indeed divides 24 and $\langle(1)\rangle = \{(1)\}$.

(b) [**b**] $g = (12)$. Then $g^1 \neq (1)$ but $g^2 = (1)$. So $|g| = 2$. 2 does indeed divide 24 and $\langle(12)\rangle = \{(1), (12)\}$.

(c) [**c**] $g = (123)$. Then $g^2 = (132)$ and $g^3 = (1)$. So $|g| = 3$. 2 does indeed divide 24 and $\langle(123)\rangle = \{(1), (123), (132)\}$.

(d) [**d**] $g = (1234)$. Then $g^2 = (13)(24)$, $g^3 = (1432)$ and $g^4 = (1)$. So $|g| = 4$. 4 does indeed divide 24 and $\langle(1234)\rangle = \{(1), (1234), (13)(24)), (1423)\}$.

(e) [**e**] $g = (12)(34)$. Then $g^2 = (1)$. So $|g| = 2$. 2 does indeed divide 24 and $\langle(12)(34)\} = \{(1), (12)(34)\}$.

We will later see that the above example in some sense represents all the possible elements of Sym(4). In particular Sym(4) has elements of order $1, 2, 3$ and 4, but of no other order. So even though 6, 8, 12 and 24 are divisors of |Sym(4)|, Sym(4) does not have elements of order 6, 8, 12 or 24.

Definition 2.4.11. [**def:product**] *Let G be a group, $I, J \subseteq G$ and $g \in G$.*

(a) [**a**] $IJ := \{ij \mid i \in I, j \in J\}$.

(b) [**b**] $gI := \{gi \mid i \in I\}$ *and* $Ig = \{ig \mid i \in I\}$.

(c) [**c**] *If $K \leq G$ and H is a union of cosets of K, then* $H/K := \{C \in G/K \mid C \subseteq H\} = \{hK \mid h \in H\}$

Lemma 2.4.12. [**ab**] *Let G be a group, A, B, C subsets of G and $g, h \in G$. Then*

(a) [**a**] $A(BC) = \{abc \mid a \in A, b \in B, c \in C\} = (AB)C$.

(b) [**b**] $A(gh) = (Ag)h$, $(gB)h = g(Bh)$ *and* $(gh)C = g(hC)$.

(c) [**c**] $Ae = A = Ae = (Ag)g^{-1} = g^{-1}(gA)$.

(d) [**d**] $A = B$ *if and only if* $Ag = Bg$ *and if and only if* $gA = gB$.

(e) [**e**] $A \subseteq B$ *if and only if* $Ag \subseteq Bg$ *and if and only if* $gA \subseteq gB$.

(f) [**f**] *If A is subgroup of G, then $AA = A$ and $A^{-1} = A$.*

(g) [**g**] $(AB)^{-1} = B^{-1}A^{-1}$.

(h) [**h**] $(gB)^{-1} = B^{-1}g^{-1}$ *and* $(Ag)^{-1} = g^{-1}A^{-1}$.

Proof. (a)

$$\begin{array}{rclclcl} A(BC) & = & \{ad \mid a \in A, d \in BC\} & = & \{a(bc) \mid a \in A, b \in B, c \in C\} & & \\ & = & \{(ab)c \mid a \in A, b \in B, c \in C\} & = & \{fc \mid f \in AB, c \in C\} & = & (AB)C \ . \end{array}$$

(b) Observe first that

$$A\{g\} = \big\{ab \mid a \in A, b \in \{g\}\big\} = \big\{ag \mid a \in A\big\} = Ag,$$

and $\{g\}\{h\} = \{gh\}$. So the first statement in (b) follows from (a) applied with $B = \{g\}$ and $C = \{h\}$. The other two statements are proved similarly.

(c) $Ae = \{ae \mid a \in A\} = \{a \mid a \in A\} = A$. Similarly $Ae = A$. By (b) $(Ag)g^{-1} = A(gg^{-1}) = Ae = A$. Similarly $g(g^{-1}A) = A$.

(d) Clearly $A = B$ implies that $Ag = Bg$. If $Ag = Bg$, then by (b)

$$A = (Ag)g^{-1} = (Bg)g^{-1} = B.$$

So $A = B$ if and only if $Ag = Bg$ and (similarly) if and only if $gA = gB$.

(e) Suppose that $A \subseteq B$ and let $a \in A$. Then $a \in B$ and so $ag \in Bg$. Hence $Ag \subseteq Bg$. If $Ag \subseteq Bg$ we conclude that $(Ag)g^{-1} \subseteq (Bg)g^{-1}$ and by (c), $A \subseteq B$. Hence $A \subseteq B$ if and only if $Ag \subseteq Bg$. Similarly, $A \subseteq B$ if and only if $gA \subseteq gB$

(f) Since a subgroup is closed under multiplication, $ab \in A$ for all $a, b \in A$. So $AA \subseteq A$. Also $e \in A$ and so $A = eA \subseteq AA$. Thus $AA = A$.

Since A is closed under inverses, $A^{-1} = \{a^{-1} \mid a \in A\} \subseteq A$. Let $a \in A$, then $a^{-1} \in A$ and $a = (a^{-1})^{-1}$. So $a \in A^{-1}$ and $A \subseteq A^{-1}$. Thus $A = A^{-1}$.

$$(g)\qquad \begin{aligned} (AB)^{-1} &= \{d^{-1} \mid d \in AB\} &&= \{(ab)^{-1} \mid a \in A, b \in B\} \\ &= \{b^{-1}a^{-1} \mid a \in A, b \in B\} &&= \{cd \mid c \in B^{-1}, d \in A^{-1}\} \\ &= B^{-1}A^{-1} \end{aligned}$$

(h) By (g) applies with $A = \{g\}$:

$$(gB)^{-1} = \big(\{g\}B\big)^{-1} = B^{-1}\{g\}^{-1} = B^{-1}\{g^{-1}\} = B^{-1}g^{-1}$$

Similarly, $(Ag)^{-1} = g^{-1}A^{-1}$. □

Lemma 2.4.13. [**order formula**] *Let G be a group and H and K subgroups of G. Then*

(a) [**a**] *The map $\alpha : H/H \cap K \to HK/K, h(H \cap K) \to hK$ is a well-defined bijection.*

(b) [**b**] *$|HK| = |HK/K| \cdot |K| = |H/H \cap K| \cdot |K|$.*

(c) [**c**] *If G is finite, then $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.*

Proof. (a) Let $h, l \in H$. Then also $h^{-1}l \in H$. We have

$$\begin{aligned} & hK = lK \\ \iff\quad & h^{-1}l \in K && - \quad 2.4.5 \\ \iff\quad & h^{-1}l \in K \cap H && - \quad \text{since } h^{-1}d \in H \\ \iff\quad & h(H \cap K) = l(H \cap K) && - \quad 2.4.5 \end{aligned}$$

If $h(H \cap K) = l(H \cap K)$ this shows that $hK = lH$ and so α is well defined. If $\alpha(h(H \cap K)) = \alpha(l(H \cap K)$ we have $hK = lK$ and so we get $h(H \cap K) = l(H \cap K)$. Thus α is 1-1.

Note that $H = \{hk \mid h \in H, k \in K\} = \bigcup_{h \in H} hK$ is a union of cosets of K and so HK/K is defined. Moreover, $HK/K = \{hK \mid h \in H\} = \{\alpha(h(H \cap K)) \mid h \in H\}$. So α is onto and (a) holds.

(b)

$$|HK/K| = \bigcup_{C \in HK/K} |C| = |HK/K| \cdot |K| = |H/H \cap K| \cdot |K|$$

(c) By Lagrange's $|H| = |H/H \cap K| \cdot |H \cap K|$. So $|H/H \cap K| = \frac{|H|}{|H \cap K|}$ and (c) follows from (b). □

2.5 Normal subgroups

Just as we have defined (left) cosets one can define right cosets:

Definition 2.5.1. [**def:right coset**] *Let G be a group and $H \leq G$ and $g \in G$. Then $Hg = \{hg \mid h \in H\}$ is called a right coset of H in G.*

In general a right coset of H is not a left coset as the following example shows:

Example 2.5.2. [**ex:left right**] Let $G = \mathrm{Sym}(3)$ and $H = \{(1),(12)\}$ Then

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

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

Suppose now that $H \circ (23)$ is a left coset of H. Note that by 2.4.5(b), (23) is contained in a unique left coset of H, namely $(23) \circ H$. Since $(23) \in H \circ (23)$ we conclude $H \circ (23) = (23) \circ H$. This contradiction shows that $H \circ (23)$ is not a left coset.

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

Definition 2.5.3. [**def:conjugation**] *Let G be a group. For $a, b \in G$ put*

$$^{a}b := aba^{-1}$$

and for $I \subseteq G$ put

$$^{a}I := aIa^{-1} = \{^{a}i \mid i \in I\}.$$

The map

$$i_h : G \to G, b \to {}^{a}b$$

is called conjugation *by a and ^{a}b is called the* conjugate *of b under a.*

Lemma 2.5.4. [**basicnormal**] *Let $N \leq G$. Then the following statements are equivalent:*

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

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

(c) [**c**] *Every left coset is a right coset*

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

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

(f) [**z**] *$^{g}n \in N$ 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 coset 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 2.4.5(b), Ng is the unique right coset of N containing g and so $Ng = Nh$ Thus $gN \subseteq Ng$. Multiplying with g^{-1} from the right we get $gNg^{-1} \subseteq N$. Hence (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 $N \subseteq {}^gN$ and ${}^gN \subseteq N$. So $N = {}^gN$ and (a) holds. □

Definition 2.5.5. [**def:normal**] *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 2.5.4*

Example 2.5.6. [**ex:normal**]

1. [**1**] Let $H = \{(1), (12)\} \leq \mathrm{Sym}(3)$. From 2.5.2 we have $(2,3) \circ H \neq H \circ (2,3)$ and so Sym(2) is not a normal subgroup of Sym(3).

2. [**2**] Let $H = \langle (123) \rangle = \{(1), (123), (132)\}$. 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

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

   Since each element of 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 Sym(3). Thus every coset is a right coset and so H is normal in Sym(3).

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 normal subgroup of $\mathrm{GL}_n(\mathbb{R})$.

4. [**4**] Let G be any abelian group and $H \leq G$. Let $h \in H$ and $g \in G$. Then

$$ghg^{-1} = gg^{-1}h = eh = h \in H$$

and so $H \trianglelefteq G$. Hence every subgroup of an abelian group is normal.

2.6 Homomorphisms and the Isomorphism Theorems

Definition 2.6.1. [**def:hom**] *Let $(G, *)$ and $(H, \cdot)$ be groups and $\phi : G \to H$ a function.*

(a) [**a**] *ϕ is called a* homomorphism *of groups if*

$$\phi(a * b) = \phi(a) \cdot \phi(b) \quad \textit{for all }, a, b \in G$$

(b) [**b**] *ϕ is called an* isomorphism *if ϕ is a bijective isomorphism.*

(c) [**c**] *We say that G and H are* isomorphic *and write $G \cong H$ if there exists an isomorphism $\psi : G \to H$.*

(d) [**d**] *If $\phi : G \to H$ is a homomorphism, then* $\ker \phi = \{a \in G \mid \phi(a)\} = e_H$. $\ker \phi$ *is called the* kernel *of ϕ.*

Example 2.6.2. [**ex:hom**]

1. [**5**] Define $\phi : (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot)$, $r \to e^r$. (Here $e = 2.718...$ is the Euler constant). Since $e^{r+s} = e^r e^s$, ϕ is a homomorphism.

2. [**2**] Define $\alpha : (\mathbb{C} \setminus \{0\}, \cdot) \to (\mathbb{R}^+, \cdot), a + ib \to a^2 + b^2$. A direct calculation shows that $\alpha(xy) = \alpha(x)\alpha(y)$ for all $x, y \in \mathbb{C} \setminus \{0\}$.

3. [**3**] Define $\beta : (\mathbb{Z}, +) \to (\{1, -1\}, \cdot)$, $n \to \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases}$

   We will show that β is a homomorphism. Let $n, m \in \mathbb{Z}$.

   If n and m is even, then also $n + m$ is even. Thus $\beta(n) = \beta(m) = \beta(n + m) = 1$ and so $\beta(n + m) = 1 = 1 \cdot 1 = \beta(n)\beta(m)$.

   If n is even and m is odd , then $n + m$ is odd. Thus $\beta(n) = 1$, $\beta(m) = \beta(n + m) = -1$ and so $\beta(n + m) = -1 = 1 \cdot (-1) = \beta(n)\beta(m)$.

   If n is odd and m is even , then $n + m$ is odd. Thus $\beta(m) = 1$, $\beta(n) = \beta(n + m) = -1$ and so $\beta(n + m) = -1 = -1 \cdot 1 = \beta(n)\beta(m)$.

   If n is odd and m is odd , then $n + m$ is even. Thus $\beta(n) = \beta(b) = -1$, $\beta(n + m) = -1$ and so $\beta(n + m) = 1 = -1 \cdot (-1) = \beta(n)\beta(m)$.

   Thus β is a homomorphism. (A second way to show that β is a homomorphism is to realize that $\beta(n) = (-1)^n$.

4. [**4**] Define $\gamma : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$, $A \to \det(A)$. Since $\det(AB) = \det(A)\det(B)$, γ is a homomorphism.

5. [**1**] Let G be a group and $g \in G$. Define $\alpha : (\mathbb{Z}, +) \to G, n \to g^n$. Then α is a homomorphism. Rather than giving a formal proof by induction we contend ourselves with an informal argument. We have

$$g^n g^m = \underbrace{g \cdot g \cdot g \ldots g}_{n-\text{times}} \cdot \underbrace{g \cdot g \cdot g \ldots g}_{m-\text{times}} = \underbrace{g \cdot g \cdot g \ldots g}_{(n+m)-\text{times}} = g^{n+m}$$

so $\alpha(n)\alpha(m) = g^n g^m = g^{n+m} = \alpha(n+m)$.

Lemma 2.6.3. [**basichom**] *Let $\phi : G \to H$ be a group homomorphism.*

(a) [**a**] $\phi(e_G) = e_H$.

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

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

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

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

(f) [**g**] *ϕ is 1-1 if and only if* $\ker \phi = \{e_G\}$.

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

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

(i) [**f**] $\ker \phi$ *is a normal subgroup of G.*

Proof. (a) We have $e_H\phi(e_G) = \phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_H)$. So by the Cancellation Law $e_H = \phi(e_G)$.

(b) $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_G) = e_H = \phi(a)\phi(a)^{-1}$. So by the Cancellation Law, $\phi(a^{-1}) = \phi(a)^{-1}$.

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

(d) Since $e_G \in A$, $e_H = \phi(e_H) \in \phi(A)$. Let $x, y \in \phi(A)$. Then $x = \phi(a)$ and $y = \phi(b)$ for some $a, b \in A$. Since A is a subgroup of G, $ab \in A$ and $a^{-1} \in A$. Thus

$$xy = \phi(a)\phi(b) = \phi(ab) \in \phi(A)$$

and

$$x^{-1} = \phi(a)^{-1} = \phi(a^{-1}) \in \phi(A)$$

So $\phi(A)$ is a subgroup of H.

(e) Since $e_H \in B$ we have $\phi(e_G) = e_H \in B$ and so $e_G \in \phi^{-1}(B)$. Let $a, c \in \phi^{-1}(B)$. Then $\phi(a), \phi(c) \in B$. Thus

$$\phi(ac) = \phi(a)\phi(c) \in B$$

and

$$\phi(a^{-1}) = \phi(a)^{-1} \in B$$

So $ac \in \phi^{-1}(B)$ and $a^{-1} \in \phi^{-1}(B)$.

(f) Suppose first that ϕ is 1-1 and let $a \in \ker\phi$. Then

$$\phi(a) = e_H = \phi(e_G)$$

and since ϕ is 1-1, $a = e_G$. So $\ker\phi = \{e_G\}$.

Suppose next that $\ker\phi = \{e_G\}$ and let $a, b \in G$ with $\phi(a) = \phi(b)$. Then

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

Hence $a^{-1}b \in \ker\phi = \{e_G\}$, $a^{-1}b = e_G$ and so $a = b$. Thus ϕ is 1-1.

(g) By (d), $\phi(N)$ is a subgroup of H. Let $m \in \phi(N)$ and $h \in H$. Then $m = \phi(n)$ for some $n \in N$ and since ϕ is onto, $h = \phi(g)$ for some $g \in G$. Since N is normal in G, ${}^{g}n \in N$. Hence

$${}^{h}m = {}^{\phi(g)}\phi(n) \overset{\text{(c)}}{=} \phi({}^{g}n) \in \phi(N)$$

Thus $\phi(N) \trianglelefteq H$.

(f) By (e) $\phi^{-1}(M)$ is a subgroup of G. Let $g \in G$ and $n \in \phi^{-1}(N)$. Then $\phi(n) \in M$ and so also ${}^{\phi(g)}\phi(m) \in M$. Thus by (c), $\phi({}^{g}n) \in M$ and ${}^{g}n \in \phi^{-1}(M)$. Thus $\phi^{-1}(M) \trianglelefteq H$.

(i) This follows from (h) applied to the normal subgroup $M = \{e_H\}$ of H. □

Example 2.6.4. [**ex:basic hom**] By Example 2.6.2(4), det is a homomorphism. Note that

$$\ker\phi = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\} = \mathrm{SL}_n(\mathbb{R})$$

So by 2.6.3(i), $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$.

Lemma 2.6.5. [**basicG/N**] *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) [**a**] *$TS \in G/N$, namely $(aN)(bN) = (ab)N$.*

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

(c) [**e**] *$TN = N = NT$.*

(d) [**f**] *$TT^{-1} = N = T^{-1}T$.*

(e) [**c**] *G/N is a group under the binary operation $G/N \times G/N \to G/N, (T,S) \to TS$. The identity element of G/N is $e_{G/N} = N$.*

(f) [**d**] *The map $\pi_N : G \to G/N, \quad g \to gN \quad$ 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 $G/N \times G/N \to G/N, (T,S) \to TS$ is a well-defined operation on G/N. By 2.4.12(b) 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

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

□

Example 2.6.6. [**ex:g/n**]

(a) [**1**] By 2.5.6(2) $\langle(1,2,3)\rangle$ is a normal subgroup of Sym(3) and

$$\mathrm{Sym}(3)/\langle(1,2,3)\rangle = \{\ \{(1),(1,2,3),(1,3,2)\},\ \{(1,2),(1,3),(2,3)\}\ \}$$

The Multiplication Table is

$*$	$\{(1),(1,2,3),(1,3,2)\}$	$\{(1,2),(1,3),(2,3)\}$
$\{(1),(1,2,3),(1,3,2)\}$	$\{(1),(1,2,3),(1,3,2)\}$	$\{(1,2),(1,3),(2,3)\}$
$\{(1,2),(1,3),(2,3)\}$	$\{(1,2),(1,3),(2,3)\}$	$\{(1),(1,2,3),(1,3,2)\}$

Let $N = \langle(1,2,3)\rangle$. Then $\mathrm{Sym}(3)/N = \{(1) \circ N, (1,2) \circ N\}$ and we can rewrite the multiplication table as

$*$	$(1) \circ N$	$(1,2) \circ N$
$(1) \circ N$	$(1) \circ N$	$(1,2) \circ N$
$(1,2) \circ N$	$(1,2) \circ N$	$(1) \circ N$

(b) [**2**] Let G be a group. Then G is a normal subgroup of G. Note that G is the only coset of G. So $G/G = \{G\}$ and so G/G is a group with just one element.

(c) [**3**] Let G be a group. The $\{e\}$ is a normal subgroup of G. $g\{e\} = \{g\}$ and so $G/\{e\} = \{\{g\} \mid g \in G\}$. We have $\{g\}\{h\} = \{gh\}$ and it follows that the map

$$G \to G/\{e\}, g \to \{g\}$$

is an isomorphism. Hence

$$G \cong G/\{e\}$$

(d) [**4**] Let n be an integer. Then $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$, with respect to addition. Namely $n\mathbb{Z} = \langle n \rangle$ Since $n\mathbb{Z} = -n(\mathbb{Z})$ we may assume $n \geq 0$. . If $n = 0$, then $n\mathbb{Z} = \{0\}$. If $n = 1$ then then $n\mathbb{Z} = \mathbb{Z}$. So let's assume $n > 1$. What are the the cosets of $n\mathbb{Z}$? We have

$$\begin{array}{rc} & a + n\mathbb{Z} = b + n\mathbb{Z} \\ \iff & a - b \in \mathbb{Z} \\ \iff & n \mid a - b \end{array}$$

For any $a \in \mathbb{Z}$ there exists unique integers q, r with $a = qn + r$ and $0 \leq r < n$. So there exists a unique integer r with $0 \leq r < n$ and $n \mid a - r$. That is there exists a unique integer r with $0 \leq r < n$ and $a + n\mathbb{Z} = r + n\mathbb{Z}$. Thus

$$Z/n\mathbb{Z} = \{r + n\mathbb{Z} \mid 0 \leq r < n\}$$

and if $0 \leq r, s < n$ then

$$r + n\mathbb{Z} = s + n\mathbb{Z} \qquad \iff \qquad r = s$$

In particular, $|\mathbb{Z}/n\mathbb{Z}| = |n|$.

Since $\mathbb{Z}$ is abelian, $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. So we obtain the quotient group $\mathbb{Z}/n\mathbb{Z}$. The elements of $\mathbb{Z}/n\mathbb{Z}$ are called the integers *modulo* n. For $n = 3$ we obtain the following addition table, where we wrote $\overline{a}$ for $a + n\mathbb{Z}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Corollary 2.6.7. [**normal=ker**] *Let B be a group and $N \subseteq G$. Then N is a normal subgroup of G if and only if there exist a group H and a homomorphism $\phi : G \to H$ with* $\ker \phi = N$.

Proof. Suppose first that $N \trianglelefteq G$. Then by 2.6.5(d), $N = \ker \pi_N$.

Suppose next that there exist a group H and a homomorphism $\phi : G \to H$ with $\ker \phi = N$. Then by 2.6.3(i), $\ker \phi \trianglelefteq G$ and so $N \trianglelefteq G$. □

Theorem 2.6.8 (First Isomorphism Theorem)**.** [**first iso**] *Let $\phi : G \to H$ be a homomorphism of groups. Then*

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

is a well-defined isomorphism of groups. In particular

$$G/\ker \phi \cong \operatorname{Im} \phi.$$

Proof. Put $N = \ker \phi$ and Let $a, b \in G$. Then

$$\begin{array}{rcll} & gN = hN & & \\ \Longleftrightarrow & g^{-1}h \in N & - & \\ \Longleftrightarrow & \phi(g^{-1}h) = e_H & - & \text{Definition of } N = \ker \phi \\ \Longleftrightarrow & \phi(g)^{-1}\phi(h) = e_H & - & \phi \text{ is a homomorphism}, 2.6.3(b) \\ \Longleftrightarrow & \phi(h) = \phi(g) & - & \text{Multiplication with } \phi(g) \text{ from the left,} \\ & & & \quad \text{Cancellation law} \end{array}$$

So

$$(*) \qquad gN = hN \Longleftrightarrow \phi(g) = \phi(h).$$

Since $gN = hN$ implies $\phi(g) = \phi(h)$ we conclude that $\overline{\phi}$ is well-defined.

Let $S, T \in G/N$. Then there exists $g, h \in N$ with $S = gN$ and $T = hN$.

Suppose that $\overline{\phi}(T) = \overline{\phi}(S)$. Then

$$\phi(g) = \overline{\phi}(gN) = \overline{\phi}(S) = \overline{\phi}(T) = \overline{\phi}(hN) = \phi(h),$$

and so by (*) $gN = hN$. Thus $S = T$ and ϕ is 1-1.

Let $b \in \operatorname{Im} \phi$. Then there exists $a \in G$ with $b = \phi(a)$ and so $\overline{\phi}(aN) = \phi(a) = b$. Therefore $\overline{\phi}$ is onto.

Finally

$$\overline{\phi}(ST) = \overline{\phi}(gNhN) = \overline{\phi}(ghN) = \phi(gh) = \phi(g)\phi(h) = \overline{\phi}(gN)\overline{\phi}(hN) = \overline{\phi}(S)\overline{\phi}(T)$$

and so $\overline{\phi}$ is a homomorphism. We proved that $\overline{\phi}$ is a well-defined, 1-1 and onto homomorphism, that is a well-defined isomorphism. □

The First Isomorphism Theorem can be summarized in the following diagram:

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

Example 2.6.9. [**ex:iso1**]

1. [**1**] Let G be a group and $g \in G$. Define

$$\phi : \mathbb{Z} \to G, m \to g^m.$$

By Example 2.6.2(5) ϕ is a homomorphism from $(\mathbb{Z}, +)$ to G. We have

$$\operatorname{Im}\phi = \{\phi(m) \mid m \in \mathbb{Z}\} = \{g^m \mid m \in \mathbb{Z}\} \overset{2.3.8(2)}{=} \langle g \rangle, \tag{1}$$

and

$$\ker\phi = \{m \in \mathbb{Z} \mid \phi(m) = e\} = \{m \in \mathbb{Z} \mid g^m = e\}. \tag{2}$$

If g has finite order, put $n = |g|$. Otherwise put $n = 0$. We claim that

$$\ker\phi = n\mathbb{Z}. \tag{3}$$

Indeed if $|g| = \infty$ then by Lemma 2.4.9(a), $g^m \neq e$ for all $0 \neq m \in \mathbb{Z}$. Hence $\ker\phi = \{0\} = 0\mathbb{Z} = n\mathbb{Z}$.

So suppose $|g| < \infty$. Let $m \in \mathbb{Z}$ and let d be the remainder of m when divided by n. By Lemma 2.4.9(b), $g^m = g^d$ and $g^d = e$ if and only if $d = 0$. Thus $m \in \ker\phi$ if and only if $d = 0$ and so if and only if $n \mid m$ and $m \in n\mathbb{Z}$. Thus (3) holds.

By the First Isomorphism Theorem

$$\mathbb{Z}/\ker\phi \cong \operatorname{Im}\phi$$

and so by (1) and (3).

$$\mathbb{Z}/n\mathbb{Z} \cong \langle g \rangle.$$

In particular, if $G = \langle g \rangle$ is cyclic then $G \cong \mathbb{Z}_n$. So every cyclic group is isomorphic to $(\mathbb{Z}, +)$ (in the $n = 0$ case) or $(\mathbb{Z}/n\mathbb{Z}, +), n > 0$.

2. [**2**] Let $S = \{c \in \mathbb{C} \mid ||c|| = 1\}$. By 2.1.4(e) , $(S, \cdot)$ is a group. Define

$$\phi : (\mathbb{R}, +) \to (S, \cdot), \quad r \to e^{2\pi ri}$$

We have $e^{2\pi ri}e^{2\pi si} = e^{2\pi ri + 2\pi si} = e^{2\pi(r+s)i}$ and so ϕ is a homomorphism. Since $e^{2\pi ri} = \cos 2\pi r + i \sin 2\pi r$ we see that ϕ is onto and $\phi(r) = 1$ if an only if r is an integer. So $\ker \phi = \mathbb{Z}$ and the First Isomorphism Theorem tells us:

$$\mathbb{R}/\mathbb{Z} \cong S.$$

3. [**3**] The map $\det : \mathrm{GL}_n(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot), A \to \det A$ is an onto homomorphism with $\ker \det = \mathrm{SL}_n(\mathbb{R})$. This is by the First Isomorphism Theorem

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

Theorem 2.6.10 (Second Isomorphism Theorem)**.** [**second iso**] *Let G be a group, N a normal subgroup of G and A a subgroup of G. Then $A \cap N$ is a normal subgroup of A, AN is a subgroup of G, N is a normal subgroup of AN and the map*

$$A/A \cap N \to AN/N, \quad a(A \cap N) \to aN$$

is a well-defined isomorphism. In particular,

$$A/A \cap N \cong AN/N.$$

Proof. By 2.3.5 $A \cap N$ is a subgroup of G and so also of A. Let $n \in A \cap N$ and $a \in A$. Then ${}^a n \in A \cap N$ and so $A \cap N \trianglelefteq A$. We have $(AN)(AN) = A(NA)N = AANN = AN$ and $(AN)^{-1} = A^{-1}N^{-1} = NA = AN$ and so AN is a subgroup of G. Since $N \trianglelefteq G$ also $N \trianglelefteq AN$. By 2.4.13(a), the map

$$\alpha : A/A \cap N \to AN/N, h(A \cap N) \to hN$$

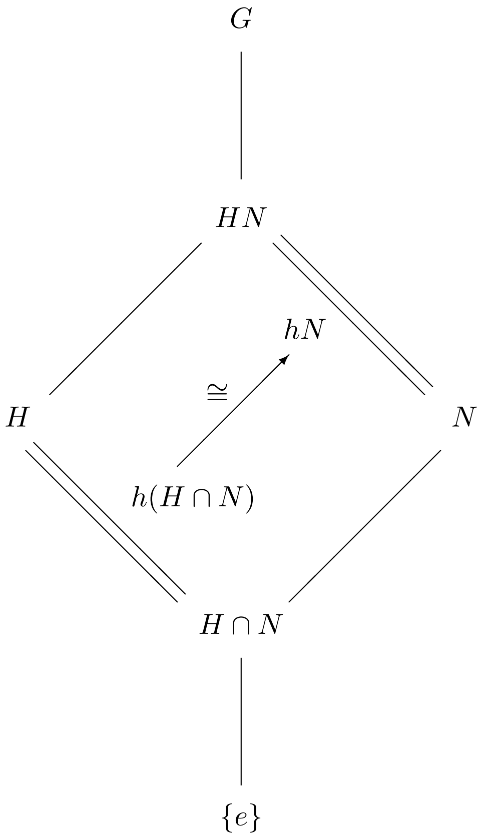
is a well-defined bijection.

Since

$$\alpha(a(A \cap N) \cdot b(A \cap N)) = \alpha(ab(A \cap N)) = abN = (aN)(bN) = \alpha(a(A \cap N))\alpha(b(A \cap N))$$

α is a homomorphism. Thus α is a well-defined isomorphism. □

The Second Isomorphism Theorem can be summarized in the following diagram.



Example 2.6.11. [**ex:iso2**] Let $G = \mathrm{GL}_2(\mathbb{R})$, $N = \mathrm{SL}_2(\mathbb{R})$ and

$$A = \left\{ \begin{pmatrix} r & 0 \\ s & 1 \end{pmatrix} \middle| \, r, s \in \mathbb{R}, r \neq 0 \right\}$$

Then $A \leq G$ and

$$B := A \cap N = \left\{ \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \middle| \, r, s \in \mathbb{R}, r \neq 0 \right\}$$

Let $g \in G$ and put $a = \begin{pmatrix} \det g & 0 \\ 0 & 1 \end{pmatrix}$. Then $a \in A$, $\det a = \det g$ and $\det a^{-1}g = 1$. So $a^{-1}g \in N$ and $g = aa^{-1}g \in AN$. Thus $AN = G$ and so by the second Isomorphism Theorem

$$A/B = A/A \cap N \cong AN/N = G/N \overset{2.6.9(3)}{\cong} (\mathbb{R} \setminus \{0\}, \cdot)$$

Note that

$$\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s+t & 1 \end{pmatrix}$$

and so

$$(\mathbb{R}, +) \to B, s \to \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}$$

is an isomorphism. Thus

$$B \cong (\mathbb{R}, +).$$

Theorem 2.6.12 (Correspondence Theorem)**.** [**third iso**] *Let N be a normal subgroup of the group G. Put*

$$\mathcal{S}(G, N) = \{H \mid N \leq H \leq G\} \text{ and } \mathcal{S}(G/N) = \{F \mid F \leq G/N\}.$$

Let

$$\pi : G \to G/N, \quad g \to gN$$

be the natural homomorphism.

(a) [**z**] *Let $N \leq K \leq G$. Then $\pi(K) = K/N$.*

(b) [**y**] *Let $F \leq G/N$. Then $\pi^{-1}(F) = \bigcup_{T \in F} T$.*

(c) [**e**] *Let $N \leq K \leq G$ and $g \in G$. Then $g \in K$ if and only if $gN \in K/N$.*

(d) [**a**] *The map*

$$\beta : \quad \mathcal{S}(G, N) \to \mathcal{S}(G/N), \quad K \to K/N$$

is a well-defined bijection with inverse

$$\alpha : \quad \mathcal{S}(G/N) \to \mathcal{S}(G, N), \quad F \to \pi^{-1}(F).$$

In other words:

(a) [**a**] *If $N \leq K \leq G$, then K/N is a subgroup of G/N.*

(b) [**b**] *For each subgroup F of G/N there exists a unique subgroup K of G with $N \leq K$ and $F = K/N$. Moreover, $K = \pi^{-1}(F)$.*

(e) [**b**] *Let $N \leq K \leq G$. Then $K \trianglelefteq G$ if and only if $K/N \trianglelefteq G/N$.*

(f) [**c**] *Let $N \leq H \leq G$ and $N \leq K \leq G$. Then $H \subseteq K$ if and only if $H/N \subseteq K/N$.*

(g) [**d**] **(Third Isomorphism Theorem)** *Let $N \leq H \trianglelefteq G$. Then the map*

$$\rho: \quad G/H \to (G/N)\big/(H/N), \quad gH \to (gN) * (H/N)$$

is a well-defined isomorphism.

Proof. (a) $\pi(K) = \{\pi(k) \mid k \in K\} = \{kN \mid k \in N\} = K/N$.

(b) Let $g \in G$. Then

$$\begin{array}{rccl} & g \in \pi^{-1}(F) & & \\ \Longleftrightarrow & \pi(g) \in F & - & \text{definition of } \pi^{-1}(F) \\ \Longleftrightarrow & gN \in F & - & \text{definition of } \pi \\ \Longleftrightarrow & gN = T \text{ for some } T \in F & & \\ \Longleftrightarrow & g \in T \text{ for some } T \in F & - & T \in G/N, 2.4.5\text{(b)} \\ \Longleftrightarrow & g \in \bigcup_{T \in F} T & - & \text{definition of union} \end{array}$$

(c) If $g \in K$ then clearly $gN \in K/N$. If $gN \in K/N$ then $gN = kN$ for some $k \in K$ and so $g \in gN = kN \subseteq K$. So $g \in K$ if and only if $gN \in K/N$.

(d) Let $N \leq K \leq G$ and $F \leq G/N$. By (a) $K/N = \pi(K)$ and so by 2.6.3(d) K/N is a subgroup of N. Hence β is well-defined. By 2.6.3(e) $\pi^{-1}(F) \leq G$. Also if $n \in N$, then $\pi(n) = nN = N = e_{G/N} \in F$ and so $n \in \pi^{-1}(N)$. Thus $N \leq \pi^{-1}(N)$ and $\pi^{-1}(N) \in \mathcal{S}(G, N)$. This shows that α is well-defined. We compute

$$\begin{array}{rcccccc} \alpha(\beta(K)) & = & \pi^{-1}(K/N) & = & \{g \in G \mid \pi(g) \in K/N\} & & \\ & = & \{g \in G \mid gN \in K/N\} & \overset{\text{(e)}}{=} & \{g \in G \mid g \in K\} & = & K \end{array}$$

Since π is onto we have $\pi(\pi^{-1}(F)) = F$ and so $\beta(\alpha(F)) = F$. Hence α is an inverse of β and so β is a bijection.

(e) Suppose that $K \trianglelefteq N$. Then since π is onto, 2.6.3(g) implies $K/N = \pi(K) \trianglelefteq N$. Suppose that $K/N \trianglelefteq G/N$. We have $\pi^{-1}(K/N) = \alpha(\beta(K)) \overset{\text{(g)}}{=} K$ and so by 2.6.3(h) $K \trianglelefteq N$.

(f) Let $h \in H$. By (c) $h \in K$ if and only if $hN \in K/N$ and so $H \subseteq K$ if and only if $H/N \subseteq K/N$.

(g) Let

$$\eta: \quad G/N \to G/N\big/H/N, \quad T \to T * (H/N)$$

be the natural homomorphism. Consider the composition:

$$\eta \circ \pi: \quad G \to G/N\Big/H/N, \quad g \to (gN) * (H/N).$$

Since η and π are homomorphisms, also $\eta \circ \pi$ is a homomorphism. Since both η and π are onto, $\eta \circ \pi$ is onto. So

$$\operatorname{Im} \eta \circ \pi = G/N \Big/ H/N. \tag{1}$$

We now compute $\ker(\eta \circ \pi)$:

$$\begin{array}{rcll}
 & g \in \ker(\eta \circ \pi) & & \\
\iff & (\eta \circ \pi)(g) = e_{(G/N)/(H/N)} & - & \text{Definition of } \ker(\eta \circ \pi) \\
\iff & \eta(\pi(g)) = e_{(G/N)/(H/N)} & - & \text{Definition of } \circ \\
\iff & \pi(g) \in \ker \eta & - & \text{Definition of } \ker \eta \\
\iff & \pi(g) \in H/N & - & 2.6.5(f) \\
\iff & gN \in H/N & - & \text{Definition of } \pi \\
\iff & g \in H & - & (c)
\end{array}$$

Thus

$$\ker(\eta \circ \pi) = H. \tag{2}$$

By the First Isomorphism Theorem 2.6.8

$$\rho: \quad G/\ker(\eta \circ \pi) \to \operatorname{Im}(\eta \circ \pi), \quad g\ker(\eta \circ \pi) \to (\eta \circ \pi)(g)$$

is a well-defined isomorphism. Thus by (1) and (2)

$$\rho : G/H \to (G/N)\Big/(H/N), \quad gH \to (gN) * (H/N).$$

is a well-defined isomorphism. □

Example 2.6.13. [**ex:third iso**] By Homework 2#1 the subgroups of Sym(3) are

$$\{1\}, \quad \langle(12)\rangle, \quad \langle(13)\rangle, \quad \langle(23)\rangle, \quad \langle(123)\rangle, \quad \operatorname{Sym}(3). \tag{1}$$

Let $A = \{(1), (12)(34), (13)(24), (14)(23)\}$ and $K = \{f \in \operatorname{Sym}(4) \mid f(4) = 4\} \cong \operatorname{Sym}(3)$. By Homework 2#7 $A \trianglelefteq \operatorname{Sym}(4)$ and the map $\phi : K \to \operatorname{Sym}(4)/A, h \to hA$ is an isomorphism. Thus we can obtain the subgroups of $\operatorname{Sym}(4)/A$ by computing $\phi(H)$ for each subgroup H of K:

$$\begin{aligned}
\phi(\{1\}) &= \{(1)A\} \\
&= \Big\{\{(1),(12)(34),(13)(24),(14)(23)\}\Big\} \\
\phi(\langle(12)\rangle) &= \{(1)A,(12)A\} \\
&= \Big\{\{(1),(12)(34),(13)(24),(14)(23)\}, \\
&\qquad \{(12),(34),(1324),(1423)\}\Big\} \\
\phi(\langle(13)\rangle) &= \{(1)A,(13)A\} \\
&= \Big\{\{(1),(12)(34),(13)(24),(14)(23)\}, \\
&\qquad \{(13),(1234),(24),(1432)\}\Big\} \\
\phi(\langle(23)\rangle) &= \{(1)A,(23)A\} \\
&= \Big\{\{(1),(12)(34),(13)(24),(14)(23)\}, \\
&\qquad \{(23),(1342),(1243),(14)\}\Big\} \\
\phi(\langle(123)\rangle) &= \{(1)A,(123)A,(132)A\} \\
&= \Big\{\{(1),(12)(34)(13)(24)(14)(23)\}, \\
&\qquad \{(123),(134),(243),(142)\}, \\
&\qquad\qquad \{(132),(234),(124),(143)\}\Big\} \\
\phi(K) &= \mathrm{Sym}(4)/A
\end{aligned}$$

By 2.6.12 taking the unions over the sets of cosets in (7) gives us the subgroups of Sym(4) containing A:

$$\begin{aligned}
A = {} & \{(1),(12)(34),(13)(24),(14)(23)\} \\
X_1 = {} & \{(1),(12)(34),(13)(24),(14)(23),(12),(34),(1324),(1423)\} \\
D_4 = {} & \{(1),(12)(34),(13)(24),(14)(23),(13),(1234),(24),(1432)\} \\
X_2 = {} & \{(1),(12)(34),(13)(24),(14)(23),(23),(1342),(1243),(14)) \\
\mathrm{Alt}(4) := {} & \{(1),(12)(34),(13)(24),(14)(23),(123),(134), \\
& \qquad (243),(142),(132),(234),(124),(143)\} \\
\mathrm{Sym}(4) &
\end{aligned} \tag{3}$$

By Example 2.5.6, $\langle(1,2)\rangle$ is not normal in Sym(3), while $\langle(1,2,3)\rangle$ is normal. Similarly neither $\langle(1,3)\rangle$ nor $\langle(2,3)\rangle$ is normal in Sym(3). Thus the normal subgroups of Sym(3) are

$$\{(1)\}, \quad \mathrm{Alt}(3) := \langle (1,2,3) \rangle, \quad \mathrm{Sym}(3). \tag{10}$$

So by 2.6.12 the normal subgroups of Sym(4) containing A are

$$A, \quad \mathrm{Alt}(4), \quad \mathrm{Sym}(4). \tag{11}$$

Example 2.6.14. [**lines in the plane**]

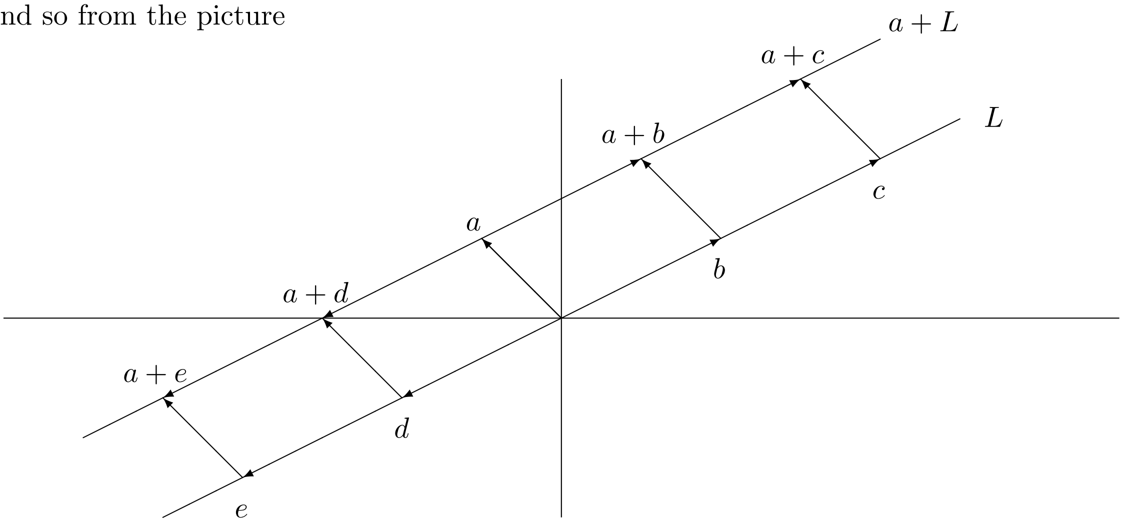
Consider the group $\mathbb{R} \times \mathbb{R}$ with respect to addition. Then the line

$$L = \{(2y, y) \mid y \in \mathbb{R}\}$$

is a subgroup of $\mathbb{R} \times \mathbb{R}$. What are the cosets of L?

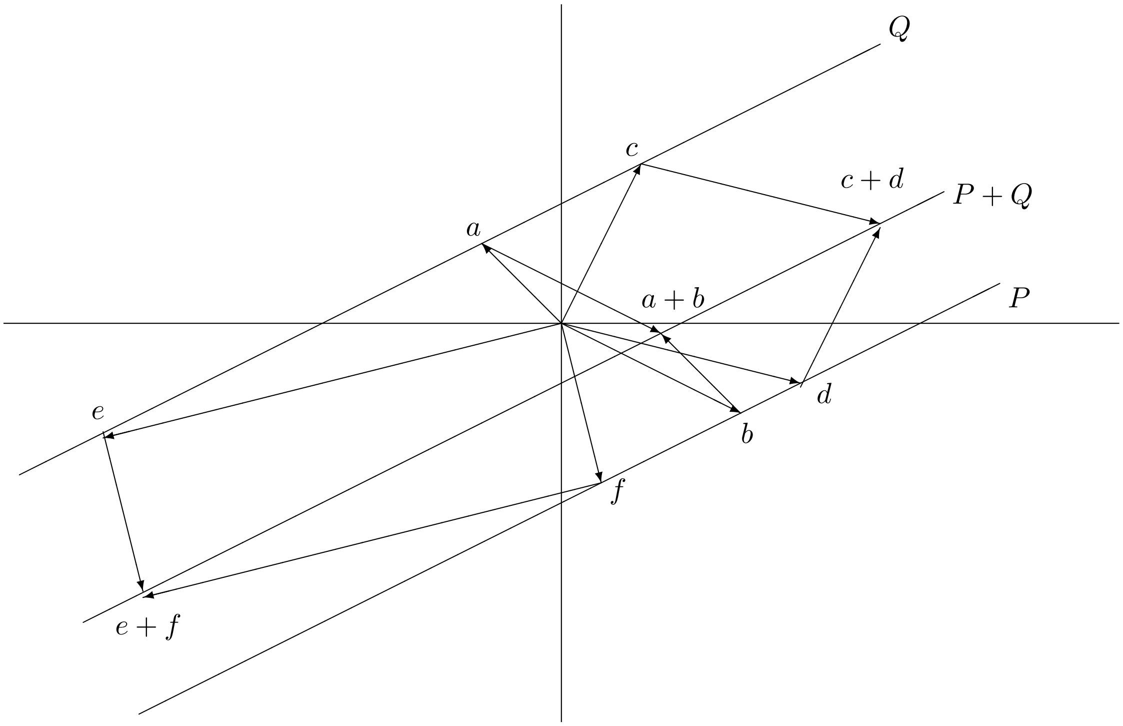
$$a + L = \{a + l \mid l \in L\}$$

and so from the picture



we see that $a + L$ is the line through a parallel to L.

Let P and Q be two lines parallel to L. The picture



illustrates that $P+Q$ is also a line parallel to L. So the set of lines parallel to L form a group under addition, namely $(\mathbb{R}\times\mathbb{R})/L$.

Consider the map α which sends each line parallel to L to its intersection with the x-axis. More concretely, α sends the line $(x,0)+L$ to x. It is easy to see that this map is a bijection and a homomorphism so

$$\mathbb{R}\times\mathbb{R}/L \cong \mathbb{R}$$

By Example 2.6.9(2), $\mathbb{Z}$ is a normal subgroups of $\mathbb{R}$ with $\mathbb{R}/\mathbb{Z}\cong S$. The inverse image of $\mathbb{Z}$ under α in $\mathbb{R}\times\mathbb{R}/L$ is

$$F := \{(z,0)+L \mid z\in\mathbb{Z}\}$$

By the Correspondence Theorem F corresponds to the subgroup

$$H := \bigcup_{M\in F} M$$

of $\mathbb{R}\times\mathbb{R}$. We have

$$H = \bigcup_{z\in\mathbb{Z}}(z,0) + L = \bigcup_{z\in\mathbb{Z}}\{(z,0) + (2y,y) \mid y \in \mathbb{R}\} = \{(2y+z,y) \mid z \in \mathbb{Z}, y \in \mathbb{R}\}$$
$$= \{(x,y) \in \mathbb{R}\times\mathbb{R} \mid x - 2y \in \mathbb{Z}\}$$

The difference between $F = H/L$ and H is that H is a set of points, while F is the set of lines parallel to L formed by these points.

From the Third Isomorphism Theorem we have

$$(\mathbb{R}\times\mathbb{R})/H \cong (\mathbb{R}\times\mathbb{R})/L\big/(\mathbb{R}\times\mathbb{R})/H = (\mathbb{R}\times\mathbb{R})/L\big/F \cong \mathbb{R}/\mathbb{Z} \cong S$$

and so

$$(\mathbb{R}\times\mathbb{R})/H \cong S.$$

Definition 2.6.15. [**def:direct product**] *Let $(G_i \mid i \in I)$ be a family of groups. Define*

$$\bigtimes_{i\in I} G_i = \{(g_i)_{i\in I} \mid g_i \in G_i \text{ for all } i \in I\}$$

and

$$* : \bigtimes_{i\in I} G_i \times \bigtimes_{i\in I} G_i \to \bigtimes_{i\in I} G_i, ((g_i)_{i\in I}, (h_i)_{i\in I}) \to (g_ih_i)_{i\in I}$$

Then $(\bigtimes_{i\in I} G_i, *)$ is called the direct product *of $(G_i \mid i \in I)$.*

Lemma 2.6.16. [**direct product**] *Let $(G_i, i \in I)$ be a family of groups.*

(a) [**a**] *$\bigtimes_{i\in I} G_i$ is a group.*

(b) [**b**] *For each $j \in J$ the group $\pi_j : \bigtimes_{i\in I} G_i \to G_j, (g_i)_{i\in I} \to g_j$ is an onto homomorphism.*

(c) [**c**] *For $j \in I$ and $g \in G_j$ let $\rho_j(g) := (h_i)_{i\in I}$ where*

$$h_i = \begin{cases} g & \text{if } i = j \\ e_{G_i} & \text{if } i \neq j \end{cases}$$

Then the map $\rho_j : G_j \to \bigtimes_{i\in I} G_i, g \to \rho_j(g)$, is a 1-1 monomorphism

Proof. To simply notation we write (g_i) for $(g_i)_{i\in I}$.

(a): We have

$$((f_i) * (g_i)) * (h_i) = (f_ig_i) * (h_i) = ((f_ig_i)h_i) = (f_i(g_ih_i)) = (f_i) * (g_ih_i) = f_i * ((g_i) * (h_i))$$

So ’*’ is associative. Put $e_i = e_{G_i}$. Then $(e_i) * (g_i) = (e_i g_i) = (g_i) = (g_i e_i) = (g_i) * (e_i)$ and so (e_i) is an identity. Also $(g_i) * (g_i^{-1}) = (g_i g_i^{-1}) = (e_i) = (g_i^{-1}) * (g_i)$ and so each $(g_i) \in \bigtimes_{i \in I} G_i$ has an inverse. So (a) holds.

(b) and (c):

Let $g \in G_j$ then $(\pi_j \circ \rho_j)(g) = \pi_j((h_i)) = h_j = g$. Hence $\pi_j \circ \rho_j = \mathrm{id}_{g_j}$. This implies that π_j is onto and ρ_j is 1-1.

$\pi_j((g_i)(h_i)) = \pi_j((g_i h_i)) = g_j h_j = \phi_j((g_i))\phi_j((h_i))$. So π_j is a homomorphism.

Let $j \in I$ and $g, h \in G_j$. For $x \in \bigtimes_{i \in G}$ define $x_i = \pi_i(x)$ and so $x = (x_i)_{i \in I}$. Then $\rho_j(g)_j = g_j, \rho_j(h)_j = h_j$ and so

$$(\rho_j(g)\rho_j(h))_j = gh = \rho_j(gh)$$

If $i \neq j$, then $\rho_j(g)_i = e, \rho_j(g)_i = e$ and so

$$(\rho_j(g)\rho_j(h))_i = ee = e = \rho_i(gh)$$

Thus $\rho_j(g)\rho_j(g) = \rho_j(gh)$ and ρ_j is a homomorphism. □

Definition 2.6.17. [**def:com**] *Let G be group and $a, b \in G$. Then*

$$[a, b] := aba^{-1}b^{-1}$$

$[a, b]$ is called the commutator of a and b.

Note here that this is not the same definition as on homework 2. But it is easy to see that the results of Homework two are still correct with the new definition of $[a, b]$.

Example 2.6.18. [**iso3 and direct**] Let G be a group and A and B be normal subgroups of G such that $A \cap B = \{e\}$ and $\langle A, B \rangle = G$. Let $a \in A$ and $b \in B$. Then

$$[a, b] = aba^{-1}b^{-1} = {}^{a}b \cdot b^{-1}$$

Since $B \trianglelefteq G$, ${}^{a}b \in B$. So B is closed under multiplication and inverses we conclude that $[a, b] = {}^{a}b \cdot b^{-1} \in B$. Now

$$[a, b] = aba^{-1}b^{-1} = a \cdot {}^{b}a^{-1}$$

Since $A \trianglelefteq G$, $a^{-1} \in A$, ${}^{b}a^{-1} \in A$ and $[a, b] = a \cdot {}^{b}a^{-1} \in A$. Thus

$$[a, b] \in A \cap B = \{e\}$$

and so by Homework 2, $ab = ba$. Thus

$$(*) \qquad ab = ba \text{ for all } a \in A, b \in B$$

Define

$$\Phi : A \times B \to G, (a,b) \to ab$$

Then

$$\Phi((a,b)\cdot(c,d)) = \Phi((ac,bd)) = (ac)(bd) = a(cb)d = a(bc)d = (ab)(cd) = \Phi((a,b))\Phi(c,d)$$

Thus Φ is a homomorphism. Hence $\operatorname{Im}\Phi \leq G$. Note that $\Phi(a,e) = ae = a$ and so $A \leq \operatorname{Im}\Phi$. Also $\Phi((e,b)) = eb = b$ and $B \leq \operatorname{Im}\Phi$. Thus

$$G = \langle A, B\rangle \leq \operatorname{Im}\Phi \leq G$$

and so

$$G = \operatorname{Im}\Phi = \{\Phi(a,b) \mid (a,b) \in A \times B\} = \{ab \mid a \in A, b \in B\} = AB$$

In particular Φ is onto. Let $(a,b) \in \ker\Phi$. Then $ab = \Phi((a,b)) = e$ and so $b = a^{-1}$. Since $b \in B$ and $a^{-1} \in A$ we have $b = a^{-1} \in A \cap B = \{e\}$. Thus $b = e, a^{-1} = e, a = e$ and $(a,b) = (e,e) = e_{A\times B}$. So $\ker\Phi = \{e_{A\times B}\}$ and by 2.6.3(f), Φ is 1-1. Thus Φ is an isomorphism and

$$G \cong A \times B$$

Let $C \trianglelefteq A$. Let $\pi_1 : A \times B \to A, (a,b) \to a$. Since π_1 is onto, $\pi_1^{-1}(C) \trianglelefteq A \times B$. Since $\pi_1(a,b) = a$, $(a,b) \in \pi^{-1}(C)$ if and only if $a \in C$. So

$$\pi_1^{-1}(C) = C \times B$$

Since Φ is an isomorphism and $C \times B \trianglelefteq A \times B$, $\Phi(C \times B) \trianglelefteq G$. We have $\Phi(C \times B) = \{\Phi(c,b) \mid c \in C, b \in B\} = \{cb \mid c \in C, b \in B\} = CB$. Thus $CB \trianglelefteq G$. By the correspondence theorem $CB/B \trianglelefteq G/B$ and

$$G/B\big/CB/B \cong G/CB$$

By the Second Isomorphism Theorem and Example 2.6.6(c):

$$A \cong A/\{e\} = A/A\cap B \cong AB/B = G/B$$

So by Homework 3 we obtain an isomorphism

$$\alpha : A \to G/B, a \to a = a\{e\} = a(A\cap B) \to aB$$

Note that $\alpha(C) = \{cB \mid c \in C\} = C/B$ and so

$$G/B\big/CB/B \cong A/C$$

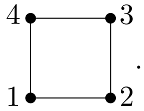
Thus by Homework 3,

$$A/C \cong G/CB = AB/CB$$

Since $\Phi(C \times B) = CB$ this implies

$$A/C \cong (A \times B)/(C \times B)$$

Example 2.6.19. **[ex:di8]**

Consider the square  .

Let D_4 be the set of all permutations of $\{1,2,3,4\}$ which map the edges (of the square) to edges.

For example $(1,3)(2,4)$ maps the edge $\{1,2\}$ to $\{3,4\}$, $\{2,3\}$ to $\{4,1\}$, $\{3,4\}$ to $\{1,2\}$ and $\{4,1\}$ to $\{2,3\}$. So $(1,3)(2,4) \in D_4$.

But $(1,2)$ maps $\{2,3\}$ to $\{1,3\}$, which is not an edge. So $(1,2) \notin D_4$.

Which permutations are in D_4? We have counterclockwise rotations by $0°, 90°, 180°$ and $270°$:

$$(1), (1,2,3,4), (1,3)(2,4), (1,4,3,2),$$

and reflections at $y = 0, x = 0$, $x = y$ and $x = -y$:

$$(1,4)(2,3), (1,2)(3,4), (2,4), (1,3)$$

Are these all the elements of D_4? Let's count the number of elements. Let $\pi \in D_4$. Then $\pi(1)$ can be $1, 2, 3$,or 4. So there are 4 choices for $\pi(1)$, $\pi(2)$ can be any of the two neighbors of $\pi(1)$. So there are two choices for $\pi(2)$. $\pi(3)$ must be the neighbor of $\pi(2)$ different from $\pi(1)$. So there is only one choice for $\pi(3)$. $\pi(4)$ is the point different from $\pi(1), \pi(2)$ and $\pi(3)$. So there is also only one choice for $\pi(4)$. Altogether there are $4 \cdot 2 \cdot 1 \cdot 1 = 8$ possibilities for π. Thus $|D_4| = 8$ and

$$D_4 = \{(1), (1234), (13)(24), (1432), (14)(23), (12)(34), (24), (13)\}.$$

If $\alpha, \beta \in \mathrm{Sym}(4)$ maps edges to edges, then also $\alpha \circ \beta$ and α^{-1} map edges to edges. Hence D_4 is a subgroup of Sym(4). (Note that we already encountered this group in 2.6.13). D_4 is called the *dihedral group* of degree 4.

2.7 Group Actions

Definition 2.7.1. **[defgroupaction]** *An* action *of a group $(G, \cdot)$ on a set S is a function*

$$\diamond : G \times S \to S, (a, s) \to a \diamond s$$

such that

(GA1) [**ga1**] $e \diamond s = s$ *for all* $s \in S$.

(GA2) [**ga2**] $(a \cdot b)s = a \diamond (b \diamond s)$ *for all* $a, b \in G,\ s \in S$.

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

We will often just write, as for $a \diamond s$. So the two axioms of a group action then read $es = e$ and $(ab)s = a(bs)$.

Example 2.7.2. [**ex:action**]

1. [**1**] Note the similarity between the definition of a group action and the definition of a group. In particular, we see that the the binary operation of a group $\cdot : G \times G \to G$ defines an action of G on G, called the action by *left multiplication.* Indeed since e is an identity, 2.7.1(*(GA1)*) holds and since $\cdot$ is associative 2.7.1(*(GA2)*) holds.

2. [**2**] The function
$$G \times G(a, s) \to a * s := sa$$
is not an action (unless G is abelian) since $(ab) * s = sab = (a * s)b = (b * a)s$. For this reason we define the action of G on G by *right multiplication* as
$$\cdot_{\mathrm{r}} : G \times G, (a, s) \to sa^{-1}.$$
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.

3. [**5**] G acts on G via conjugation:
$$G \times G \to G, (a, g) \to {}^{a}g$$
Indeed ${}^{e}g = g$ and ${}^{(ab)}g = {}^{a}({}^{b}g)$.

4. [**9**] Consider the map
$$\diamond : G \times G \to G, (a, g) \to a^2 g$$
Then $a \diamond (b \diamond g) = a^2(b^2 g) = (a^2 b^2)g$ and $(ab) \diamond g = (ab)^2 g$. So $\diamond$ is an action if and only if $a^2 b^2 = (ab)^2$ for all $a, b \in G$, and so if and only if G is abelian.

5. [**6**] 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. [**8**] Let G be a group and $H \leq G$. Then G acts on G/H via left multiplication:

$$\diamond : G \times G/H \to G/H, (a,T) \to aT$$

To see that this is well-defined we need to show that $aT \in G/H$ for all $a \in G$ and $T \in G/H$. Note that $T = cH$ for some $c \in G$. So $aT = a(cH) = (ac)H \in G/H$.

By 2.4.12(c) $eT = T$ and so (GA1) holds. Let $a, b \in G$ then by 2.4.12(b), $a(bT) = (ab)T$ and so (GA2) holds. Hence $\diamond$ is an action.

The next lemma shows that an action of G on S can also be thought of as a homomorphism from G to $\mathrm{Sym}(S)$.

Lemma 2.7.3. [**action=hom**] *Let G be a group and S a set.*

(a) [**a**] *Let $\diamond : G \times S \to S$ an action of G on S. For $g \in G$ define*

$$\phi^\diamond_g : S \to S, s \to gs$$

Then $\phi^\diamond_g \in \mathrm{Sym}(S)$ and the map

$$\Phi^\diamond : G \to \mathrm{Sym}(S), g \to \phi^\diamond_g$$

is a homomorphism.

$\Phi^\diamond$ is called the homomorphism *corresponding to $\diamond$,*

(b) [**b**] *Let $\Phi : G \to \mathrm{Sym}(S)$ be a homomorphism. Define*

$$\diamond_\Phi : G \times S \to S, (g,s) \to \Phi(g)(s)$$

then $\diamond_\Phi$ is an action of G on S.

$\diamond_\Phi$ is called the action *corresponding to Φ*

(c) [**c**] $\Phi^{\diamond_\Phi} = \Phi$ *and* $\diamond_{\Phi^\diamond} = \diamond$.

Proof. To simplify notation we just write ϕ_g for $\phi^\diamond_g$. (a) (GA1) into $\phi_e(s) = gs = s$ and so $\phi_e = id_S$. By (GA2)

$$(\phi_g \circ \phi_h)(s) = g(hs) = (gh)s = \phi_{gh}(s)$$

and so

$$\phi_g \circ \phi_h = \phi_{gh}$$

Hence Φ is a homomorphism. We still need to verify that $\phi_g \in \mathrm{Sym}(S)$. But this follows from

$$\mathrm{id}_S = \phi_e = \phi_{gg^{-1}} = \phi_g \circ \phi_{g^{-1}}$$

and so also $\phi_{g^{-1}} \circ \phi_g = \mathrm{id}_S$. So $\phi_{g^{-1}}$ is an inverse for ϕ_g and $\phi_g \in \mathrm{Sym}(S)$.

(b) Since Φ is a homomorphism $\Phi(e) = e_{\mathrm{Sym}(S)} = \mathrm{id}_S$ and so $e \diamond_\Phi s = \Phi(e)(s) = \mathrm{id}_S(s) = s$. So $(GA1)$ holds. Also

$$(gh) \diamond_\Phi s = \Phi(gh)(s) = (\Phi(g) \circ \Phi(h))(s) = \Phi(g)(\Phi(h)(s)) = \gamma \diamond_\Phi (h \diamond_\Phi s)$$

and so also (GA2) holds.

(c) $g \diamond_{\Phi^\diamond} s = \Phi_\diamond(g)(s) = g \diamond s$ and
$\Phi^{\diamond_\Phi}(g)(s) = g \diamond_\Phi s = \Phi(g)(s)$. □

Example 2.7.4. [**ex:action ii**]

1. [**3**] The homomorphism corresponding to the action $\diamond : \mathrm{Sym}(I) \times I \to I, (\pi, i) \to \pi(i)$ is

$$\mathrm{id}_{\mathrm{Sym}(I)} : \mathrm{Sym}(I) \to I, \pi \to \pi$$

Indeed, for $\pi \in \mathrm{Sym}(I)$ and $i \in I$ we have

$$\Phi^\diamond(\pi)(i) = \phi^\diamond_\pi(i) = \pi \diamond i = \pi(i)$$

Thus $\Phi^\diamond(\pi) = \pi$.

2. [**1**] Let G be a group. By 2.7.2(1) $\cdot : G \times G \to G, (a, g) \to ag$ is an action of G on G. We have

$$\phi^{\cdot}_a : G \to G, g \to ag$$

and

$$\Phi^{\cdot} : G \to \mathrm{Sym}(G), a \to \phi_a$$

By 2.7.3(a) $\Phi^{\cdot}$ is a homomorphism. If $\Phi^{\cdot}(a) = \mathrm{id}_G$, then

$$a = ae = \phi^{\cdot}_a(e) = \Phi^{\cdot}(a)(e) = \mathrm{id}_G(e) = e$$

and so $\Phi^{\cdot}$ is 1-1. Thus $G \cong \Phi^{\cdot}(G)$. In particular, G is isomorphic to a subgroup of a symmetric group. This is known as *Cayley's Theorem.*

Example 2.7.5. [**ex:cayley**] Define $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Put

$$a = (0,0), b = (1,0), c = (0,1) \text{ and } d = (1,1).$$

Then $G = \{a, b, c, d\}$. Write ϕ_g for ϕ^+_g. For each $g \in G$ we will compute ϕ_g.

For $x \in G$ we have $\phi_a(x) = (0,0) + x = x$. So

$$\phi_a = \mathrm{id}_G = (a)(b)(c)(d).$$

$\phi_b(a) = b + a = (1,0) + (0,0) = (1,0) = b.$
$\phi_b(b) = b + b = (1,0) + (1,0) = (0,0) = a.$
$\phi_b(c) = b + c = (1,0) + (0,1) = (1,1) = d.$
$\phi_b(d) = b + d = (1,0) + (1,1) = (0,1) = c.$
Thus

$$\phi_b = (a,b)(c,d).$$

$\phi_c(a) = c + a = (0,1) + (0,0) = (0,1) = c.$
$\phi_c(c) = c + c = (0,1) + (0,1) = (0,0) = a.$
$\phi_c(b) = c + b = (0,1) + (1,0) = (1,1) = d.$
$\phi_c(d) = c + d = (0,1) + (1,1) = (1,0) = b.$
Thus

$$\phi_c = (a,c)(b,d).$$

$\phi_d(a) = c + a = (1,1) + (0,0) = (1,1) = d.$
$\phi_d(d) = d + d = (1,1) + (1,1) = (0,0) = a.$
$\phi_d(b) = d + b = (1,1) + (1,0) = (0,1) = c.$
$\phi_d(c) = d + c = (1,1) + (0,1) = (1,0) = b.$
Thus

$$\phi_d = (a,d)(b,c).$$

(We could also have computed ϕ_d as follows: Since $d = a + c$, $\phi_c = \phi_a \circ \phi_b = (a,b)(c,d) \circ (a,c)(b,d) = (a,d)(b,c)$)

Hence

$$(\mathbb{Z}_2 \times \mathbb{Z}_2, +) \cong (\{(a), (a,b)(c,d), (a,c)(b,d), (a,d)(b,c)\}, \circ).$$

Using $1, 2, 3, 4$ in place of a, b, c, d we conclude

$$(\mathbb{Z}_2 \times \mathbb{Z}_2, +) \cong (\{(1), (12)(34), (13)(24), (14)(23)\}, \circ)$$

Definition 2.7.6. [**def:stabilizer**] *Let $\diamond$ be an action of the group G on the set I, $H \subseteq G$, $g \in G$, $s \in S$ and $T \subseteq S$. Then*

(a) [**a**] $\mathrm{Stab}^{\diamond}_H(T) = \{h \in H \mid ht = t \text{ for all } t \in T\}$ *and* $\mathrm{Stab}^{\diamond}_H(s) = \{h \in H \mid hs = s\}$. $\mathrm{Stab}^{\diamond}_H(T)$ *is called the* stabilizer *of T in H with respect to $\diamond$.*

(b) [**b**] $\mathrm{Fix}_T(H) = \{t \in T \mid ht = t \text{ for all } h \in H\}$ *and* $\mathrm{Fix}_T(g) = \{t \in T \mid gt = t\}$. *The elements of* $\mathrm{Fix}_T(H)$ *are called the fixed-points of H in T with respect to $\diamond$.*

(c) [**c**] $g \diamond T = \{gt \mid t \in T\}$ *and* $H \diamond s = \{hs \mid h \in H\}$.

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

(e) [**e**] *T is called H-*invariant *(with respect to $\diamond$) if $hT = T$ for all $h \in H$. T is called g-invariant if $gT = T$.*

(f) [**f**] *$N_H(T) = \{h \in H \mid hT = T\}$. $N_H(T)$ is called the* normalizer *of T in H.*

(g) [**g**] *$G^\diamond := \operatorname{Im}\Phi^\diamond$.*

We will often just write $\mathrm{Stab}_H(S)$ in place of $\mathrm{Stab}^\diamond_H(S)$, Hs for $H \diamond s$ and gT for $g \diamond T$, but of course only if it's clear from the context what the underlying action $\diamond$ is.

Example 2.7.7. [**ex:stab**] Let $\diamond$ be the action of Sym(5) on $\{1, 2, 3, 4, 5\}$. Then

$$\mathrm{Stab}_{\mathrm{Sym}(5)}(4) = \{\pi \in \mathrm{Sym}(5) \mid \pi(4) = 4\} = \mathrm{Sym}(\{1, 2, 3, 5\}) \cong \mathrm{Sym}(4)$$
$$\mathrm{Stab}_{\mathrm{Sym}(5)}(\{2, 4\}) = \{\pi \in \mathrm{Sym}(5) \mid \pi(2) = 2, \pi(3) = 2\} = \mathrm{Sym}(\{1, 3, 5\}) \cong \mathrm{Sym}(3)$$

and

$$\mathrm{N}_{\mathrm{Sym}(5)}(\{1, 3, 5\}) = \{\pi \in \mathrm{Sym}(5) \mid \pi(\{1, 3, 5\}) = \{1, 3, 5\}\,\}$$
$$\cong \mathrm{Sym}(\{1, 3, 5\}) \times \mathrm{Sym}(\{2, 4\}) \cong \mathrm{Sym}(3) \times \mathrm{Sym}(2)$$

Lemma 2.7.8. [**basic action**] *Let $\diamond$ be an action of the group G on the set S.*

(a) [**a**] *$\mathrm{Stab}^\diamond_G(S) = \ker \Phi^\diamond \trianglelefteq G$.*

(b) [**b**] *$G/\mathrm{Stab}^\diamond_G(S) \cong G^\diamond \leq \mathrm{Sym}(S)$.*

(c) [**c**] *S is a faithful G-set if and only if $\Phi^\diamond$ is $1-1$. So if S is faithful, G is isomorphic to a subgroup of* Sym(S)*.*

(d) [**d**] *Let $H \leq G$ and T an H-invariant subset of S, then*

$$\diamond\,|_{H,T}\colon H \times T \to T, (h, t) \to ht$$

is an action of H on T.

(e) [**e**] *Let $\mathcal{P}(S)$ be the set of subsets of S. Then*

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

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

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

$$\begin{array}{ccc} & g \in \mathrm{Stab}_G(S) & \\ \iff & gs = s \text{ for all } g \in G & -\text{definition of Stab} \\ \iff & \phi^\diamond_g(s) = s \text{ for all } g \in G & -\text{definition of } \phi^\diamond_g \\ \iff & \phi^\diamond(g) = \mathrm{id}_S & -\text{definition of } \mathrm{id}_S \\ \iff & \Phi^\diamond(g) = \mathrm{id}_S & -\text{definition of } \Phi^\diamond \\ \iff & g \in \ker \Phi^\diamond & -\text{definition of } \ker \end{array}$$

(b) Since $G^\diamond = \operatorname{Im}\Phi^\diamond$, this follows from (a) and the First Isomorphism Theorem.

(c) By 2.6.3(f), $\Phi^\diamond$ is 1-1 if and only if $\ker\Phi^\diamond = \{e\}$ and so by (a) if and only if $\operatorname{Stab}_G(S) = \{e\}$, that is if and only if G acts faithfully on I.

(d) See Homework 4#6.

(e) See Homework 4#5. □

Lemma 2.7.9. [**stabilizers are subgroups**] *Let $\diamond : G \times S \to S$ be a group action. Let $s \in S$ and $T \subseteq S$.*

(a) [**a**] *$\operatorname{Stab}^\diamond_G(T)$ is a subgroup of G.*

(b) [**b**] *$\operatorname{Stab}^\diamond_G(s)$ is a subgroup of G.*

(c) [**c**] *$\mathrm{N}^\diamond_G(T)$ is a subgroup of G.*

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

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

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

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 $g^{-1} \in \operatorname{Stab}_G(T)$. 2.3.3 now implies that $\operatorname{Stab}_G(T)$ is a subgroup of G.

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

(c) We have

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

(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 2.7.10. [**ex:stabilizer**] Let G be a group, let $\diamond$ be the action of G on G by conjugation and let $A \subseteq G$. Let $g \in G$. Then

$$\begin{aligned} & g \in \operatorname{Stab}^\diamond_G(A) \\ \iff\quad & g \diamond a = a \text{ for all } a \in A \\ \iff\quad & {}^g a = a \text{ for all } a \in A \\ \iff\quad & gag^{-1} = a \text{ for all } a \in A \\ \iff\quad & ga = ag \text{ for all } a \in A \\ \iff\quad & g \in C_G(A) \end{aligned}$$

So $\operatorname{Stab}^\diamond_G(A) = C_G(A)$ and by 2.7.9(a), $C_G(A) \leq G$, but of course we already proved this in 2.3.4(6).

Define $\mathrm{Z}(G) = \{g \in G \mid ga = ag \text{ for all } a \in A\}$. Then

$$\mathrm{Z}(G) = C_G(G) = \mathrm{Stab}_G^{\diamond}(G)$$

and so by 2.7.8(a), $\mathrm{Z}(G) \trianglelefteq G$.

Lemma 2.7.11. [**orbits**] *Let $\diamond : G \times S \to S$ be a group action. Define a relation $\sim_\diamond$ on S by $s \sim_\diamond t$ if and only $t = as$ for some $a \in G$. Then $\sim_\diamond$ is an equivalence relation on S.*

Proof. We write $\sim$ for $\sim_\diamond$. 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. □

Definition 2.7.12. [**def:orbits**] *Let $\diamond : G \times S \to S$ be a group action.*

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

(b) [**b**] *The set of orbits is denoted by $S/^{\diamond}G$.*

(c) [**c**] *We say that G acts* transitively *on S if G has exactly one orbit on S.*

Lemma 2.7.13. [**easy orbits**] *Let G be a group acting on a set S and let $s \in S$. Then the orbit of G on S containing s is $Gs = \{gs \mid g \in G\}$.*

Proof. The orbit of G containing s is the equivalence class of $\sim_\diamond$ containing s. So

$$[s] = \{t \in S \mid s \sim_\diamond t\} = \{t \in S \mid t = gs \text{ for some } g \in G\} = Gs$$

□

Example 2.7.14. [**ex:orbits**] Let $(G, \cdot)$ be group and $H \leq G$.

1. [**1**] What are the orbits for the action $\cdot\,|_H$ of H on G by left multiplication? Let $h \in G$. Then

$$H \cdot g = \{h \cdot g \mid h \in H\} = Hg$$

So the orbits of H on G with respect to the action by left multiplication are the right cosets H of G in H.

2. **[2]** What are the orbits for the action $\cdot_{\mathrm{r}} |_H$ of H on G by right multiplication? Let $h \in G$. Then

$$H \cdot_r g = \{h \cdot_r g \mid h \in H\} = \{g \cdot h^{-1} \mid h \in H\} = \{g \cdot h \mid h \in H\} = gH$$

   So the orbits of H on G with respect to the action by right multiplication are the left cosets H in G

3. **[3]** What are the orbits for the action $\cdot_{\mathrm{c}}$ of G on G by conjugation? Let $a \in G$. Then

$$G \cdot_{\mathrm{c}} a = \{g \cdot_{\mathrm{c}} a \mid g \in G\} = \{{}^g a \mid g \in G\}$$

   Define ${}^G a := \{{}^g a \mid g \in G\}$. ${}^G a$ is called the *conjugacy class* of G containing a. So the conjugacy classes are just the orbits of G on G with respect to the action of G on G by conjugation. Two elements of G lie in the same conjugacy class if and only if they are conjugate.

   As an example consider $G = \mathrm{Sym}(n)$.

   By Proposition B on Homework 2 two elements of $\mathrm{Sym}(n)$ are conjugate if and only if they have the same cycle type. So a conjugacy class of $\mathrm{Sym}(n)$ consists of all the elements of a fixed cycle type. For $n = 4$ we obtain the following conjugacy classes:

type	conjugacy class C	$\lvert C\rvert$
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

4. **[4]** Let I be a non-empty set and $i \in I$. Then

$$\mathrm{Sym}(I)i = \{\pi(i) \mid \pi \in \mathrm{Sym}(I)\} = I.$$

   Indeed, let $j \in I$. If $i = j$, then $j = \mathrm{id}_I(i)$. If $i \neq j$, put $\pi = (i, j)$, then $j = \pi(i)$. So $j \in \mathrm{Sym}(I)i$ and $\mathrm{Sym}(I)(i) = I$.

   Hence $\mathrm{Sym}(I)$ acts transitively on I.

5. **[5]** The action $\diamond : G \times G/H \to G/H, (g, T) \to gT$ of G on G/H be left multiplication is transitive. Indeed,

$$G \diamond H = \{gH \mid g \in G\} = G/H.$$

Lemma 2.7.15. [**trivial orbits**] *Let $\diamond$ be an action of the group G on the non-empty set S. Then the following are equivalent:*

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

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

(c) [**c**] *G acts transitively on S.*

Proof. (a) $\Longrightarrow$ (b): Since S is non-empty there exists $s \in S$. Let $t \in S$. Then by (a), $t = gs$ for some $g \in T$. Thus $t \in Gs$ and so $S \subseteq Gs \subseteq S$. Therefore $S = Gs$.

(b) $\Longrightarrow$ (c): By 2.7.13 Gs is an orbit for G on S. By assumption $S = Gs$ and so S is an orbit. Since distinct orbits are disjoint, S is the only orbit of G on S. So by definition, G is transitive.

(c) $\Longrightarrow$ (a): Since G has a unique orbit on S, $[s] = [t]$. So $t \in [s] = Gs$ and $t = gs$ for some $g \in G$. □

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

Definition 2.7.16. [**def:g-equi**] *Let G be a group, $\diamond$ 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) [**a**] *α is called G-*equivariant *if*

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

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

(b) [**b**] *α is called a G-*isomorphism *if α is G-equivariant and a bijection.*

(c) [**c**] *If there exists a G-isomorphism from S to T we say that $\diamond$ is isomorphic to $\triangle$ or that S and T are isomorphic G-sets and write*

$$\diamond \cong \triangle, \quad (S, \diamond) \cong (T, \triangle), \quad \text{or } S \cong_G T$$

Lemma 2.7.17. [**transorbits**] *Let S be a G-set, $s \in S$ and put $H = \mathrm{Stab}_G(s)$.*

(a) [**a**] *The map*

$$\alpha : G/H \to S,\ aH \to as$$

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

(b) [**b**] *α is a G-isomorphism if and only if G acts transitively on S*

(c) [**c**] $\mathrm{Stab}(as) = {}^aH$ *for all $a \in G$.*

(d) [**d**] $|Gs| = |G/\mathrm{Stab}_G(s)|$.

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

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

The forward direction 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)

$$g \in \mathrm{Stab}_G(as) \iff g(as) = as \iff a^{-1}gas = s \iff a^{-1}ga \in H \iff g \in aHa^{-1} = {}^aH$$

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

Lemma 2.7.18. [**char g-sets**] *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:

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

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 2.7.17(b) applied to S and to T:

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

□

Example 2.7.19. [**ex:iso g-sets**]

1. [**1**] Let $(G, \cdot)$ be a group. Is the action $\cdot$ of G on G by left multiplication isomorphic to the action $\cdot_{\mathrm{c}}$ of G on G by conjugation?

   We have $G \cdot e = Ge = G$ and so $\cdot$ is a transitive action.

   We have $G\cdot_{\mathrm{c}}e = {}^{G}e = \{{}^{g}e \mid g \in G\} = \{e\}$ and so $\cdot_{\mathrm{c}}$ is not transitive unless $G = \{e\}$. So for $G \neq \{e\}$, $\cdot$ and $\cdot_{\mathrm{c}}$ are not isomorphic.

2. [**2**] Let $(G, \cdot)$ be a group. Is the action $\cdot$ of G on G by left multiplication isomorphic to the action $\cdot_{\mathrm{r}}$ of G on G by right multiplication?

   We have $G\cdot_{\mathrm{r}}e = \{g\cdot_{\mathrm{r}}e \mid g \in G\} = \{eg^{-1} \mid g \in G\} = \{g^{-1} \mid g \in G\} = G$. So both $\cdot$ and $\cdot_{\mathrm{r}}$ are transitive. Thus we can use 2.7.18 to decide whether $\cdot$ and $\cdot_{\mathrm{r}}$ are isomorphic. We have

   $$\mathrm{Stab}^{\cdot}_{G}(e) = \{g \in G \mid ge = e\} = \{e\}$$

   and

   $$\mathrm{Stab}^{\cdot_{\mathrm{r}}}_{G}(e)\{g \in G \mid g\cdot_{\mathrm{r}}e = e\} = \{g \in G \mid eg^{-1} = e\} = \{e\}$$

   So the stabilizers are equal and thus conjugate. Hence by 2.7.18 $\cdot$ and $\cdot_{\mathrm{r}}$ are isomorphic. We can use 2.7.17(b) we find a concrete isomorphism. Namely we obtain the following isomorphism of G-sets:

   $$G/\{e\} \to (G, \cdot), g\{e\} \to ge = g$$

   and

   $$G/\{e\} \to (G, \cdot_{\mathrm{r}}), g\{e\} \to g\cdot_{\mathrm{r}}e = eg^{-1} = g^{-1}$$

   So the map

   $$(G, \cdot) \to (G, \cdot_{\mathrm{r}}), g \to g^{-1}$$

   is a G-isomorphism viewed from G viewed as a G-set under left multiplication and to G viewed as a G-set under right multiplication.

3. [**3**] Let $T = \{(12)(34), (14)(23), (13)(24)\}$. By Homework 4#7 Sym(4) acts on T by conjugation that is

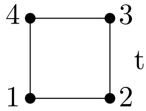
   $$\diamond : \mathrm{Sym}(4) \times T \to T, (\pi, t) \to {}^{\pi}t$$

   is a well-defined action of Sym(4). We will first show that Sym(4) is transitive on T. We have

   $${}^{(1)}(12)(34) = (12)(34), {}^{(13)}(12)(34) = (32)(14) = (14)(23) \text{ and } {}^{(14)}(12)(34) = (42)(31) = (13)(24)$$

Thus by 2.7.15(b) Sym(4) acts transitively on T.

Let $\pi \in \mathrm{Sym}(4)$. Then $\pi \in \mathrm{Stab}_{\mathrm{Sym}(4)}((13)(24))$ if and only if ${}^{\pi}(13)(24) = (13)(24)$, that is if and only if $(\pi(1)\pi(3))(\pi(2)\pi(4)) = (13)(24)$. This is the case if and only if either $\pi(\{1,3\}) = \{1,3\}$ and $\pi(\{2,4\}) = \{2,4\}$ or $\pi(\{1,3\}) = \{2,4\}$ and $\pi(\{2,4\}) = \{1,3\}$.

Now this holds if and only if whenever $\{i,j\}$ is not an edge of the square  then $\pi(\{i,j\})$ is not a edge. Finally this is the case if and only if whenever $\{i,j\}$ is an edge of the square then $\pi(\{i,j\})$ is also an edge. Thus

$$\mathrm{Stab}_{\mathrm{Sym}(4)}((13)(24)) = \mathrm{D}_4$$

Since Sym(4) is transitive on T we conclude from 2.7.17(b) that

$$T \cong_{\mathrm{Sym}(4)} \mathrm{Sym}(4)/\,\mathrm{D}_4$$

Definition 2.7.20. [**def:rep**] *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. Note that this holds if and only if the map $R \to S/G, r \to Gr$ is a bijection.*

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

Lemma 2.7.21. [**trivial trivial**] *Let G be a group acting on a set S and let $s \in S$. Then the following are equivalent.*

(a) [**a**] $s \in \mathrm{Fix}_S(G)$.

(b) [**b**] $G = \mathrm{Stab}_G(s)$.

(c) [**c**] $Gs = \{s\}$.

(d) [**d**] *$\{s\}$ is an orbit for G on S.*

(e) [**e**] *s is contained in any set of representatives for S/G.*

(f) [**f**] $|F/\mathrm{Stab}_G(s)| = 1$.

Proof. (a)-(c) all just say that $gs = s$ for all $g \in G$. The orbit containing s is Gs. So (c) and (d) are equivalent.

If $\{s\}$ is an orbit clearly any set of representative for S/G must contain s. Now suppose $\{s\}$ is not an orbit. Then there exists $t \in Gs$ with $s \neq t$. Let R be a set of representatives for S/G with $t \in R$. Then $s \notin R$. Thus (d) and (e) are equivalent.

Clearly (b) and (f) are equivalent and the lemma is proved. □

Proposition 2.7.22 (Orbit Equation)**.** [**orbiteq**] *Let G be a group, S a G-set and $R \subseteq S$ be a set of representatives for S/G.*

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

Proof. Since the orbits are the equivalence 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 2.7.17d, $|Gr| = |G/\mathrm{Stab}_G(r)|$ and so

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

If $r \in \mathrm{Fix}_S(G)$, then $\mathrm{Stab}_G(r) = G$ and $|G/\mathrm{Stab}_G(r)| = 1$. So

$$\begin{array}{rcc} |S| & = & \sum_{r\in \mathrm{Fix}_S(G)} |G/\mathrm{Stab}_G(r)| + \sum_{r\in R\setminus \mathrm{Fix}_S(G)} |G/\mathrm{Stab}_G(r)| \\ & = & \sum_{r\in \mathrm{Fix}_S(G)} 1 + \sum_{r\in R\setminus \mathrm{Fix}_S(G)} |G/\mathrm{Stab}_G(r)| \\ & = & |\mathrm{Fix}_S(G)| + \sum_{r\in R\setminus \mathrm{Fix}_S(G)} |G/\mathrm{Stab}_G(r)| \end{array}.$$

□

Example 2.7.23. [**ex:orbits equation**] Let $\mathcal{P} = \mathcal{P}(\{1,2,3,4\})$ be the set of subsets of $\{1,2,3,4\}$. Then D_4 acts on $\mathcal{P}$. We first compute the orbits: Sets of size 0: one orbit:

$$\emptyset$$

Sets of size 1: one orbit:

$$\{1\}, \{2\}, \{3\}.\{4\}$$

Sets of size 2: two orbits

$$\text{edges: } \{1,2\}, \{2,3\}, \{3,4\}, \{4,1\}$$

$$\text{non edges } \{1,3\}, \{3,4\}$$

Sets of size 3: one orbit:

$$\{1,2,3\}, \{1,3,4\}, \{1,2,4\}, \{1,2,3\}$$

Sets of size 4: one orbit:

$$\{1,2,3,4\}$$

So

$$\mathcal{R} = \{\emptyset, \{1\}, \{1,2\}, \{1,3\}, \{2,3,4\}, \{1,2,3,4\}\}$$

is a set of representatives for the orbits of D_4 on $\mathcal{P}$.

We compute

$$\begin{array}{lcl}
\mathrm{Stab}_{\mathrm{D}_4}(\emptyset) & = & D_4 \\
\mathrm{Stab}_{\mathrm{D}_4}(\{1\}) & = & \{(1),(24)\} \\
\mathrm{Stab}_{\mathrm{D}_4}(\{1,2\}) & = & \{(1),(12)(34)\} \\
\mathrm{Stab}_{\mathrm{D}_4}(\{13)\}) & = & \{(1),(24),(13),(13)(24)\} \\
\mathrm{Stab}_{\mathrm{D}_4}(\{2,3,4\}) & = & \{(1),(24)\} \\
\mathrm{Stab}_{\mathrm{D}_4}(\{1,2,3,4\}) & = & D_4
\end{array}$$

The orders of these groups are 8, 2, 2, 4, 2, 2, 8. So the orbit equation says:

$$\begin{array}{ccccccccccccc}
|\mathcal{P}| & = & \frac{8}{8} & + & \frac{8}{2} & + & \frac{8}{2} & + & \frac{8}{4} & + & \frac{8}{2} & + & \frac{8}{8} \\
16 & = & 1 & + & 4 & + & 4 & + & 2 & + & 4 & + & 1
\end{array}$$

Note that each of the summands is the length of one of the orbits.

Corollary 2.7.24 (Class Equation)**.** [**classeq**] *Let G be a group and R be a set of representatives for the conjugacy classes of G. Then* $\mathrm{Fix}_G^{\cdot_c}(G) = \mathrm{Z}(G)$ *and*

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

Proof. Recall that $\cdot_c$ is the action of G on G be conjugation. Then

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

and by 2.7.10 $\mathrm{Stab}_G^{\cdot_c}(a) = \mathrm{C}_G(a)$. So the Class Equation follows from the orbit equation. □

Example 2.7.25. [**ex:class equation**] By Proposition B in the Solutions to Homework 2, Sym(3) has exactly three conjugacy classes corresponding to the cycle 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 Sym(3). A straight forward calculation shows that

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

The orders of these centralizers are

$$6, 2, 3.$$

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

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

The Orbit Equation becomes particularly powerful if G is a finite *p-group*:

Definition 2.7.26. [**def:p-group**] *Let G be a finite group and p a prime. Then G is called a p-*group *provided that $|G| = p^k$ for some $k \in \mathbb{N}$.*

Proposition 2.7.27 (Fixed-Point Equation)**.** [**Smodp**] *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 the orbits of P on S and $r \in R \setminus \mathrm{Fix}_S(P)$. Then $\mathrm{Stab}_P(r) \lneqq P$. 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 2.7.22

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

□

Example 2.7.28. [**ex:fixed-point eq**] Consider the action of D_4 on the set $\mathcal{P}$ of subsets of $\{1,2,3,4\}$. By Example 2.7.23 $\mathrm{Fix}_{\mathcal{P}}(D_4) = \{\emptyset, \{1,2,3,4\}\}$. Thus

$$|\mathcal{P}| = 8 \text{ and } |\mathrm{Fix}_{\mathcal{P}}(D_4)| = 2$$

So by the Fixed-Point Equation

$$8 \equiv 2 \pmod 2$$

Lemma 2.7.29. [**CenterP**] *Let P be a p-group with $P \neq \{e\}$. Then $\mathrm{Z}(P) \neq \{e\}$.*

Proof. Consider the action $\cdot_{\mathrm{c}}$ of G on G by conjugation. By 2.7.27

$$|P| \equiv |\,\mathrm{Fix}_P^{\cdot_{\mathrm{c}}}(P)| \pmod p.$$

Since $|P| = p^k$ and $|P| \neq 1$ we have $p \mid |P|$ and so $|P| \equiv 0 \pmod p$. By 2.7.24 $\mathrm{Fix}_P^{\cdot_{\mathrm{c}}}(P) = \mathrm{Z}(P)$ and so

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

Hence $|\,\mathrm{Z}(P)| \neq 1$ and $\mathrm{Z}(P) \neq \{e\}$. □

2.8 Sylow p-subgroup

Hypothesis 2.8.1. [**hyp:sylow**] *Throughout this section G is a finite group and p a prime.*

Definition 2.8.2. [**def:sylow**] *A* p-subgroup *of G is a subgroup $P \leq G$ which is a p-group. A* Sylow p-subgroup *S of G is a maximal p-subgroup of G. That is S is a p-subgroup of G if and if $S \leq Q$ for some p-subgroup Q, then $S = Q$. Let $\mathrm{Syl}_p(G)$ be the set of all Sylow p-subgroups of G.*

Definition 2.8.3. [**def:p-part**] *Let n be a positive integer and p a prime. Then n_p is the* p-part *of n, that is the largest power of p dividing n. $n_{p'}$ is the* p'-part *of n, that is the largest integer m with $m \mid n$ and $p \nmid m$. So $n_p = p^k$ for some $k \in \mathbb{N}$, $n = n_p n_{p'}$ and $p \nmid n_{p'}$.*

Lemma 2.8.4. [**easy sylow**]

(a) [**a**] *If P is a p-subgroup of G, then $|P| \leq |G|_p$.*

(b) [**c**] *Let P be a p-subgroup of G and S is a p-subgroup such that $|S|$ is maximal with respect to $P \leq S$. Then $S \in \mathrm{Syl}_p(G)$. In particular, P is contained in a Sylow p-subgroup of G.*

(c) [**d**] *G has at least one Sylow p-subgroup of G.*

(d) [**b**] *If $S \leq G$ with $|S| = |G|_p$, then S is a Sylow p-subgroup of G.*

Proof. (a) Since P is a p-group, $|P| = p^n$ for some $n \in \mathbb{N}$. By Lagrange's Theorem, $|P|$ divides $|G|$ and so p^n divides $p^k l$. Since $p \nmid l$ we conclude that $n \leq k$ and so $|P| = p^n \leq p^k$.

(b) Let Q be a p-subgroup of G with $S \leq Q$. Then also $P \leq Q$ and so by maximality of $|S|$, $|Q| \leq |S|$. Since $S \leq Q$ we get $S = Q$ and so $S \in \mathrm{Syl}_p(G)$.

(c) By (d), $\{e\}$ is contained in a Sylow p-subgroup. So G must have a Sylow p-subgroup.

(d) By (a) $|S| \geq |P|$ for all p-subgroups of G. Thus by (b) applied with $P = \{e\}$, $S \in \mathrm{Syl}_p(G)$. □

Example 2.8.5. [**ex:sylow**]

(a) [**3**] $|\mathrm{Sym}(3)| = 3! = 6 = 2 \cdot 3$. $\langle (1,2) \rangle$ has order 2 and so by 2.8.4(d), $\langle (1,2) \rangle$ is a Sylow 2-subgroup of Sym(3).

$\langle (1,2,3) \rangle$ has order 3 and so is a Sylow 3-subgroup of Sym(3).

(b) [**4**] $|\mathrm{Sym}(4)| = 4! = 24 = 2^3 \cdot 3$. D_4 is a subgroup of order eight of Sym(4) and so D_4 is a Sylow 2-subgroup of Sym(4).

$\langle (1,2,3) \rangle$ is a Sylow 3-subgroup of Sym(4).

(c) [**5**] $|\mathrm{Sym}(5)| = 5! = 5 \cdot 24 = 2^3 \cdot 3 \cdot 5$. So D_4 is a Sylow 2-subgroup of Sym(5), $\langle (1,2,3) \rangle$ is a Sylow 3-subgroup of Sym(5) and $\langle (1,2,3,4,5) \rangle$ is a Sylow 5-subgroup of Sym(5).

Lemma 2.8.6. [**n choose pk**] *Let n and k be positive integers and p a prime. Suppose that p^k divides n. Then $\binom{n}{p^k}_p = \frac{n_p}{p^k}$.*

Proof. Since

$$\binom{n}{p^k} = \frac{n}{p^k} \prod_{i=1}^{p^{k-1}} \frac{n-i}{p^k - i}$$

it suffices to show that the p-parts of $n-i$ and $p^k - i$ are identical for all $1 \leq i < p^k - 1$. Let $0 < i < p^k$. Then p^k divides n and p^k and so divides neither $n-i$ nor $p^k - i$. So the p parts of $n-i$ and p^k-i are at most p^{k-1}. The lemma now follows since $(n-i)-(p^k-i) = (m-1)p^k$. □

Lemma 2.8.7. [**inner aut**] *Let G be a group and $a \in G$. Then the map*

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

is an isomorphism of G. In particular if $H \leq G$, then ${}^aH \leq H$ and $H \cong {}^aH$.

Proof. Note that $\mathrm{i}_a = \phi_g^{\cdot_\mathrm{c}}$, where $\cdot_\mathrm{c}$ is the action of G in G by conjugation. Thus by 2.7.3, i_a is a bijection. We have

$$\mathrm{i}_a(gh) = a(gh)a^{-1} = (aga^{-1})(aha^-1) = \mathrm{i}_a(g)\,\mathrm{i}_b(h)$$

and so i_a is a homomorphism.

Since ${}^aH = \mathrm{i}_a(H)$ we conclude from 2.6.3(d) that ${}^aH \leq G$. The restriction $H \to {}^aH, h \to {}^ah$ is a 1-1 and onto homomorphism and so $H \cong {}^aH$. □

Theorem 2.8.8. [**sylow of order gp**] *Let G be a finite group, p a prime and k non-negative integer such that p^k divides $|G|$. Then there exists a subgroup S of G with $|S| = p^k$. In particular there exists $P \leq G$ with $|P| = |G|_p$ and $P \in \mathrm{Syl}_p(G)$.*

Proof. Let $\mathcal{P}$ be the set of all subsets of G of size p^k. If $X \in \mathcal{P}$ and $g \in G$, then by the Cancellation law $|gX| = |X| = p^k$. So $gX \in \mathcal{P}$. Thus

$$\diamond : G \times \mathcal{P} \to \mathcal{P}, (g, X) \to gX$$

is an action of G on $\mathcal{P}$. Let $\mathcal{R}$ be a set of representatives for the orbits of G on $\mathcal{P}$. By the orbit equation,

$$|\mathcal{P}| = \sum_{R \in \mathcal{R}} |G/\mathrm{Stab}_G^{\diamond}(R)|.$$

Let $|G|_p = p^{k+r}$. By 2.8.6 $|\mathcal{P}| = \binom{|G|}{p^k}_p = p^r$. Hence there exists $R \in \mathcal{R}$ such that p^{r+1} does not divide $|G/\mathrm{Stab}_G^{\diamond}(R)|$. Put $S = \mathrm{Stab}_G^{\diamond}(R)$. Then p^{r+1} does not divide $\frac{|G|}{|S|}$ and so p^k divides S. Let $r \in R$. Then $Sr \subseteq R$. Since $|R| = p^k$ we conclude that $|S| = |Sr| \leq p^k$. Thus $|S| = p^k$.

In the case $|G|_p = p^k$ we see that there exists a subgroup P of G with $|P| = |G|_p$. Hence by 2.8.4(c), $P \in \mathrm{Syl}_p(G)$. □

Lemma 2.8.9. [**Products of subgroups**] *Let A and B be subgroups of G.*

(a) [**a**] *AB is a subgroup of G if and only if $AB = BA$.*

(b) [**b**] *If $A \leq N_G(B)$ then AB is a subgroup of G.*

Proof. (a) Suppose AB is a subgroup of G. Then $AB = (BA)^{-1} = B^{-1}A^{-1} = BA$.

Suppose next that $AB = BA$. Then $e = ee \in AB$, $(AB)(AB) = A(BA)A = A(AB)B = (AA)(BB) = AB$ and $(AB)^{-1} = B^{-1}A^{-1} = BA = AB$. So AB is a subgroup of G.

(b) If $A \leq N_G(B)$ then $aB = Ba$ for all $a \in A$. Thus $AB = BA$ and AB is a subgroup by (a). □

Theorem 2.8.10. [**Sylow's Theorem**] *Let G be a finite group and p a prime. Let $s_p = |\mathrm{Syl}_p(G)|$ be the number of Sylow p-subgroups of G.*

(a) [**a**] *Any two Sylow p-subgroups of G are conjugate in G. In other words G acts transitively on $\mathrm{Syl}_p(G)$ and if $P, Q \in \mathrm{Syl}_p(G)$ then $Q = {}^gP$ for some $g \in G$.*

(b) [**b**] *Let $S \leq G$. Then S is a Sylow p-subgroup of G if and only if $|S| = |G|_p$.*

(c) [**c**] *Let $S \in \mathrm{Syl}_p(G)$. Then $s_p = |G/\,\mathrm{N}_G(S)|$.*

(d) [**d**] *s_p divides $|G|_{p'}$ and $s_p \equiv 1 \pmod{p}$.*

Proof. We will first show that

1°. [**0**] *G acts on $\mathrm{Syl}_p(G)$ by conjugation, that is the map*

$$\diamond : G \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G), (g, S) \to {}^gS$$

is a well-defined action of G on $\mathrm{Syl}_p(G)$.

Since G acts on G by conjugation G also acts on $\mathcal{P}(G)$ be conjugation. So we only need to show that $\mathrm{Syl}_p(G)$ is G-invariant with respect to conjugation, that is if $S \in \mathrm{Syl}_p(G)$ and $g \in G$ we need to show that ${}^gS \in \mathrm{Syl}_p(G)$. By 2.8.7 $|{}^gS| = |S|$ and thus ${}^gS$ is a p-subgroup of G. Let T be a p-subgroup of G with ${}^gS \leq T$. Then $S \leq {}^{g^{-1}}T$ and so by maximality of S, $S = {}^{g^{-1}}T$ and ${}^gS = T$. Thus ${}^gS$ is indeed a maximal p-subgroup of G. So (1°) holds.

Let $P \in \mathrm{Syl}_p(G)$ and put $\mathcal{S} = {}^GP := \{{}^gP \mid g \in G\}$. So $\mathcal{S}$ is the set of Sylow p-subgroups conjugate to P.

2°. [**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 ${}^gQ = Q$ for all $g \in P$, $P \leq \mathrm{N}_G(Q)$ and by 2.8.9(b) 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, $P = PQ = Q$.

3°. [2] $|\mathcal{S}| \equiv 1 \pmod{p}$.

By (2°) $\mathrm{Fix}^{\diamond}_{\mathcal{S}}(P) = 1$ and by Fixed-Point Formula 2.7.27 $|\mathcal{S}| \equiv |\mathrm{Fix}_{\mathcal{S}}(G)| \pmod{p}$. So (3°) holds.

4°. [3] $\mathcal{S} = \mathrm{Syl}_p(G)$.

Let $Q \in \mathrm{Syl}_p(G)$. Then by The Fixed-point equation and (3°): $|\mathrm{Fix}_{\mathcal{S}}(Q)| \equiv |\mathcal{S}| \equiv 1 \pmod{p}$. Hence Q has a fixed-point $T \in \mathcal{S}$. By (3°) applied to Q, this fixed-point is Q. So $Q = T \in \mathcal{S}$ and $\mathcal{S} = \mathrm{Syl}_p(G)$

We are now able to prove (a)-(d).

(a) By (a) $\mathcal{S}$ is the unique orbit for G on $\mathrm{Syl}_p(G)$. So G acts transitively on $\mathrm{Syl}_p(G)$ and (a) holds

(b): By 2.8.4(d), any subgroup of order $|G|_p$ is a Sylow p-subgroup. Let $S \in \mathrm{Syl}_p(G)$. By 2.8.8 there exists $P \in \mathrm{Syl}_p(G)$ with $|P| = |G|_p$. By (a) $S = {}^gP$ for some $g \in G$ and so $|S| = |P| = |G|_p$ and (b) holds.

(c) Note that $\mathrm{N}_G(P) = \{g \in G \mid {}^gP = \mathrm{Stab}^{\diamond}_G(P)\}$. So by 2.7.17(d) that

$$s_p = |\mathrm{Syl}_p(G)| = |\mathcal{S}| = |G/\,\mathrm{N}_G(P)|.$$

(d) By (3°) and (4°) $|\mathrm{Syl}_p(G)| = |\mathcal{S}| \equiv 1 \pmod{p}$. Note that $P \leq \mathrm{N}_G(P)$. So by (c), (b) and Lagrange's

$$|G|_{p'} = \frac{|G|}{|G|_p} = \frac{|G|}{|P|} = \frac{|G|}{|\,\mathrm{N}_G(P)|}\frac{|\,\mathrm{N}_G(P)|}{|P|} = |G/\,\mathrm{N}_G(P)| \cdot |\,\mathrm{N}_G(P)/P| = s_p \cdot |\,\mathrm{N}_G(P)/P|$$

Hence s_p divides $|G|_{p'}$. □

Example 2.8.11. [**ex:sylow thm**] Let G be a group of order 21. Then s_7 has to divide $\frac{21}{7} = 3$ and is $1 \mod 7$. Thus $s_7 = 1$ and G has exactly one Sylow 7-subgroup S_7. Let $g \in G$. Then ${}^gS_7$ also is a Sylow 7-subgroup and so ${}^gS_7 = S_7$ and $S_7 \trianglelefteq G$. s_3 divides $\frac{21}{3} = 7$ and $s_3 = 1$ or $s_3 = 7$.

Case 1. [s3=1] $s_3 = 1$.

Then G has a unique Sylow 3-subgroup S_3 and $S_3 \trianglelefteq G$. Note that $|S_3 \cap S_7|$ divides $|S_3| = 3$ and $|S_7| = 7$. Thus $|S_3 \cap S_7| = 1$ and $S_7 \cap S_3 = \{e\}$. Hence

$$|S_3S_7| = \frac{|S_3||S_7|}{|S_3 \cap S_7|} = \frac{21}{1} = 21 = |G|$$

and so $G = S_7S_3 = \langle S_7, S_3\rangle$. Hence Example 2.6.18

$$G \cong S_3 \times S_7$$

By Homework 5#1, $S_3 \cong \mathbb{Z}_3$ and $S_7 \cong \mathbb{Z}_7$. Thus

$$G \cong \mathbb{Z}_3 \times \mathbb{Z}_7$$

Case 2. [**s7=1**] $s_3 = 1$.

Let $S_3 \in \mathrm{Syl}_3(G)$. Then $|G/\,\mathrm{N}_G(S_3)| = 7$ and so $N_G(S_3) = S_3$. Since $|A \cap B| = 1$ for distinct Sylow 3-subgroup A and B of G we conclude that

$$\mathrm{Stab}_G(\mathrm{Syl}_3(G)) = \bigcap_{A \in \mathrm{Syl}_3(G)} N_G(A) = \bigcap_{A \in \mathrm{Syl}_3(G)} A = \{e\}.$$

Hence G acts faithfully on $\mathrm{Syl}_3(G)$ and since $|Syl_3(G)| = 7$ G is isomorphic to a subgroup of $\mathrm{Sym}(7)$. So let's assume that $G \leq \mathrm{Sym}(\mathbb{Z}_7)$. Since $\mathrm{Sym}(7)$ has a unique conjugacy class of elements of order 7, namely the seven cycles, we may assume that $S_7 = \langle (0123456) \rangle$.

By the Fixed-Point Equation,

$$7 = |Z_7| \equiv |\mathrm{Fix}_{\mathbb{Z}_7}(S_3)| \pmod 3$$

and so S_3 a fixed-point on $\mathbb{Z}_7$. With out loss S_3 fixes 0. Let $t \in S_3$ and put $s = (0123456) \in S_7$. Then ${}^t s \in S_7$ and so ${}^t s = s^i$ for some $1 \leq i \leq 6$. Let $j \in \mathbb{Z}_7$. Note that $s(a) = a + 1$ for all $a \in \mathbb{Z}_7$ and so $s^2(a) = a + 2$ and $s^j(a) = a + j$. Thus

$$t(j) = t(s^j(0)) = (ts^j t^{-1} t)(0) = s^{ij}(t(0)) = s^{ij}(0) = ij$$

It follows that $t^2(j) = i^2 j$ and $t^3(j) = i^3 j$. Since $t \in S_3$ and $|S_3| = 3$ we have $t^3 = \mathrm{id}_{\mathbb{Z}_7}$. Thus $i^3 j = j$ for all $j \in \mathbb{Z}_7$ and so $i^3 \equiv 1 \mod 7$. We have $1^3 = 1$, $2^3 = 8 \equiv 1 \pmod 7$, $3^3 = 27 \equiv -1 \pmod 7$. Also $(-x)^3 = -x^3$ and so $4^3 \equiv (-3)^3 = -(-1) = 1$, $5^3 = (-2)^3 = -1$ and $6^3 = (-1)^3 = -1$. Thus $i = 1, 2$ or 4. Since i unique determines t and $|S_3|$ has order three S_3 consists of the three permutations, $t_i : j \to i^3 j$ for $i \in \{1, 2, 4\}$. Note that S_7 consists of the permutations $s_k : j \to j + k$ for $k \in \mathbb{Z}_7$. As above we have $S_7 S_3 = G$. Note that $(s_k \circ t_i)(j) = s_k(t_i(j)) = s_k(ij) = ij + k$. Thus G consists of all the permutations

$$\mathbb{Z}_7 \to \mathbb{Z}_9, \quad j \to ij + k \text{ for } i \in \{1, 2, 4\}, k \in \mathbb{Z}_7\}$$

So up to isomorphism there exists a unique group of order 21 with seven Sylow 3-subgroups.

Also observe that $t_2 = (124)(365)$ and so

$$G = \langle (0123456), (124)(365) \rangle$$

Chapter 3

Rings

3.1 Definitions and Examples

Definition 3.1.1. [**def:ring**] *A* ring *is a tuple $(R, +, \cdot)$ such that R is a set, $+$ and $\cdot$ are binary operation on R and*

(Ax 1) [**1**] *$+$ is closed, that is $a + b \in R$ for all $a, b \in R$.*

(Ax 2) [**2**] *$a + (b + c) = (a + b) + c$ for all $a, b, c \in R$.*

(Ax 3) [**3**] *$a + b = b + a$ for all $a, b \in R$.*

(Ax 4) [**4**] *There exists an element $0_R \in R$ such that $a + 0_R = a = 0_R + a$ for all $a \in R$.*

(Ax 5) [**5**] *For each $a \in R$ there exists an element $b \in R$ with $a + b = 0_R$.*

(Ax 6) [**6**] *$\cdot$ is closed, that is $a \cdot b \in R$ for all $a, b \in R$.*

(Ax 7) [**7**] *$a(bc) = (ab)c$ for all $a, b, c \in R$.*

(Ax 8) [**8**] *$a(b + c) = (ab) + (ac)$ and $(a + b)c = (ac) + (bc)$ for all $a, b, c \in R$.*

Note the first five axioms just say that $(R, +)$ is an abelian group.

Definition 3.1.2. [**def:commutative**] *Let R be a ring. Then R is called* commutative *if*

(Ax 9) [**9**] *$ab = ba$ for all $a, b \in R$.*

Definition 3.1.3. [**def:identity**] *Let R be a ring. An element 1_R in R is called an* identity *in R if*

(Ax 10) [**10**] *$1_R \cdot a = a = a \cdot 1_R$ for all $a \in R$.*

Example 3.1.4. [**ex:rings**]

1. [**1**] $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ all are commutative rings with identity.

2. [**1.1**] $(2\mathbb{Z}, +, \cdot)$ is a commutative ring without an identity.

3. [**1.5**] 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 $(\alpha+\beta)(a) = \alpha(a)+\beta(a)$ and $(\alpha\circ\beta)(a) = \alpha(\beta(a))$. We will verify that the 7 axioms of a ring hold for $(\mathrm{End}(A), +, \circ)$.

   Let $\alpha, \beta, \gamma \in \mathrm{End}(A)$ and $a, b \in A$. Then

   (Ax 1):

$$(\alpha+\beta)(a+b) = \alpha(a+b) + \beta(a+b) = \alpha(a) + \alpha(b) + \beta(a) + \beta(b) \text{and}$$
$$(\alpha+\beta)(a) + (\alpha+\beta(b)) = \alpha(a) + \beta(a) + \alpha(b) + \beta(b)$$

   Since

$$A$$

   is abelian we conclude that $\alpha+\beta$ is a homomorphism and so $+$ is closed

   (Ax 2) $(\alpha+(\beta+\gamma))(a) = \alpha(a)+(\beta(a)+\gamma(a)) = (\alpha(a)+\beta(a))+\gamma(a) = ((\alpha+\beta)+\gamma)(a)$.

   (Ax 3) $(\alpha+\beta)(a) = \alpha(a)+\beta(a) = \beta(a)+\alpha(a) = (\beta+\alpha)(a)$.

   (Ax 4) Let $\tau_0 : A \to A, a \to 0_A$. Then $\tau_0 \in \mathrm{End}(A)$ and $(\tau_0+\alpha)(a) = \tau_0(a)+\alpha(a) = 0_A+\alpha(a)$. Hence τ_0 is an additive identity.

   (Ax 5) Define $\delta : A \to A, a \to -\alpha(a)$. Since A is abelian, $-(a+b) = (-a)+(-b)$ and so δ is a homomorphism. Also $(\delta+\alpha)(a) = \delta(a)+\alpha(a) = \alpha(a)+\alpha(a) = 0_A = \tau_0(a)$ and so δ is an additive inverse of α in $\mathrm{End}(A)$.

   (Ax 6) By Homework 3#1, $\alpha\circ\beta$ is a homomorphism.

   (Ax 7) This holds since composition of functions is associative.

   (Ax 8) $(\alpha\circ(\beta+\gamma))(a) = \alpha((\beta+\gamma)(a)) = \alpha(\beta(a)+\gamma(a)) = \alpha(\beta(a)+\alpha(\gamma(a)) = (\alpha\circ\beta)(a)+(\alpha\circ\gamma)(a) = ((\alpha\circ\beta)+(\alpha\circ\gamma))(a)$

   and $((\alpha+\beta)\circ\gamma)(a) = (\alpha+\beta)(\gamma(a)) = \alpha(\gamma(a))+\beta(\gamma(a)) = (\alpha\circ\gamma)(a)+(\beta\circ\gamma)(a) = ((\alpha\circ\gamma)+(\alpha\circ\gamma))(a)$.

   So $\mathrm{End}(A)$ is indeed a ring, called the *endomorphism ring* of A.

4. [**2**] Let R be any ring and $n \in \mathbb{Z}^+$. Let $\mathrm{M}_{nn}(R)$ be the set of all $n\times n$ matrices with coefficients in R. So each $A \in \mathrm{M}_{nn}(R)$ is a tuple $(a_{ij})_{ij}$ with $a_{ij} \in R$ for all $1 \le i, j \le n$. Define

$$(a_{ij})_{ij} + (b_{ij})_{ij} = (a_{ij}+b_{ij})_{ij}$$
$$(a_{ij})_{ij} \cdot (b_{jk})_{jk} = (\sum_{j=1}^{n} a_{ij}b_{jk})_{ik}$$

   Straightforward calculation show that $(\mathrm{M}_{nn}(R), +, \cdot)$ is a ring.

$\mathrm{M}_{nn}(R)$ is usually not commutative. Suppose for example that $a \in R$ with $a^2 \neq 0$.

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a^2 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

5. [**7**] 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.

6. [**3**] Rings with one element:

$+$	0
0	0

$\cdot$	0
0	0

7. [**4**] Rings with two elements :

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	n

Here $n \in \{0, 1$ for $n = 0$ we have a ring with zero-multiplication For $n = 1$ this is $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$.

8. [**5**] Rings with three elements:

$+$	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 $0 \leftrightarrow 0$, $1 \leftrightarrow -1$.

9. [**6**] Direct products are rings. Indeed, let $(R_i, i \in I)$ be a family of rings. For $(f_i), (g_i) \in \mathop{\times}_{i \in I} R_i$

$$(f_i) + (g_i) = (f_i + g_i) \text{ and}(f_i) \cdot (g_i) = (f_i \cdot g_i)$$

With this definition $\bigoplus_{i\in I} R_i$ is a ring. 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 each R_i is commutative then $\bigtimes_{i\in I} R_i$ has an identity.

3.2 Elementary Properties of Rings

Definition 3.2.1. [**def:negative**] *Let R be a ring and $a \in A$. Then $-a$ denotes the unique element of R with*

$$a + (-a) = 0_R$$

$-a$ is called the negative *or* additive inverse *of a. For $a, b \in R$, define $a - b := a + (-b)$.*

Proposition 3.2.2. [**basic ring**] *Let R be a ring and $a, b, c \in R$. Then*

1. [**a**] $-0_R = 0_R$
2. [**b**] $a \cdot 0_R = 0_R = 0_R \cdot a$.
3. [**c**] $a \cdot (-b) = -(ab) = (-a) \cdot b$.
4. [**d**] $-(-a) = a$.
5. [**e**] $a - a = 0_R$.
6. [**f**] $-(a + b) = (-a) + (-b)$.
7. [**g**] $-(a - b) = (-a) + b = b - a$.
8. [**h**] $(-a) \cdot (-b) = ab$.
9. [**i**] $a \cdot (b - c) = ab - ac$ *and* $(a - b) \cdot c = ac - bc$.

If R has an identity

10. [**j**] $(-1_R) \cdot a = -a = a \cdot (-1_R)$.

Proof. (1) By (Ax 4) $0_R + 0_R = 0_R$ and so by Definition 3.2.1 $-0_R = 0_R$.

(2) We compute

$$0_R + a \cdot 0_R \overset{\text{(Ax 4)}}{=} a \cdot 0_R \overset{\text{(Ax 4)}}{=} a \cdot (0_R + 0_R) \overset{\text{(Ax 8)}}{=} a \cdot 0_R + a \cdot 0_R$$

and so then by Cancellation Law for groups 2.2.1 $a \cdot 0_R = 0_R$. Similarly $0_R \cdot a = 0_R$.

(3) We have

$$ab + a \cdot (-b) \overset{\text{(Ax 8)}}{=} a \cdot (b + (-b)) \overset{\text{Def } -b}{=} a \cdot 0_R \overset{(2)}{=} 0_R$$

So by Definition 3.2.1 $-(ab) = a \cdot (-b)$.

(4) This holds by 2.2.2(c).

(5) $a - a = a + (-a) = 0_R$.

(6) By 2.2.2 $-(a+b) = (-b) + (-a)$ and since addition is commutative, $-(a+b) = (-a) + (-b)$.
and so by definition $-(a+b) = (-a) + (-b)$.

(7)

$$\begin{array}{rccccc} -(a-b) = & -(a+(-b)) & \overset{(6)}{=} & (-a)+(-(-b)) & \overset{(4)}{=} & (-a)+b \\ & & \overset{(\text{Ax } 3)}{=} & b+(-a) & = & b-a \end{array}.$$

(8) $(-a)\cdot(-b) \overset{(3)}{=} a\cdot(-(-b)) \overset{(4)}{=} a\cdot b$.

(9) $a\cdot(b-c) \overset{\text{Def b-c}}{=} a\cdot(b+(-c)) \overset{(\text{Ax } 8)}{=} a\cdot b + a\cdot(-c) \overset{(3)}{=} ab+(-(ac)) \overset{\text{Def ab–ac}}{=} ab - ac$.
Similarly $(a-b)\cdot c = ab - ac$.

(10) $a + ((-1_R)\cdot a) \overset{\text{Ax 10}}{=} 1_R\cdot a + (-1_R)\cdot a \overset{(\text{Ax } 8)}{=} (1_R + (-1_R))\cdot a \overset{\text{Def} -}{=} 0_R\cdot a \overset{(2)}{=} 0_R$
Hence by Definition 3.2.1 $-a = (-1_F)\cdot a$. Similarly $-a = a\cdot(-1_F)$. □

Definition 3.2.3. [**def:unit**] *Let R be a ring with identity.*

(a) [**a**] *u in R is called a* unit *in R if there exists $v \in R$ with*

$$uv = vu = 1_R$$

In this case u is also called invertible *and v is called an* inverse *of u.*

(b) [**b**] *R is called an* integral domain *provided that R is commutative, $1_R \neq 0_R$ and whenever $a, b \in R$ with $ab = 0_R$, then $a = 0_R$ or $b = 0_R$.*

(c) [**c**] *R is called a division ring if $1_R \neq 0_R$ and every non-zero element is a unit.*

(d) [**d**] *A* field *is a commutative division ring.*

Example 3.2.4. [**ex:integral domain**]

1. [**1**] Consider $(\mathbb{Z}, +, \cdot)$. The units in $\mathbb{Z}$ are 1 and -1. So $\mathbb{Z}$ is not a field, but it is an integral domain.

2. [**2**] All non-zero elements in $\mathbb{Q}$ are invertible. So $\mathbb{Q}$ is a field. $\mathbb{Q}$ is also an integral domain.

3. [**3**] 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 domain. So suppose $n \geq 2$. Then $1 \neq 0$ in $\mathbb{Z}_n$ and thus 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.

We will show below that every finite integral domain is a field. It follows that $\mathbb{Z}_p$ is a field for all primes p.

Proposition 3.2.5. [**field is int**] *Every field is an integral domain.*

Proof. Let F be a field. Then by definition, F is a commutative ring with identity. Let $a, b \in F$ with $ab = 0_F$. Suppose that $a \neq 0_F$. Then by the definition of a field, a is a unit. Thus a has an inverse a^{-1}. So we compute

$$0_{\mathbb{F}} = a^{-1} \cdot 0_F = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1_F \cdot b = b$$

So $b = 0_F$.

We proved that if $a \neq 0_F$, then $b = 0_F$. So $a = 0_F$ or $b = 0_F$ and F is an integral domain. □

Proposition 3.2.6 (Cancellation Law)**.** [**int and cancel**] *Let R be an integral domain and $a, b, c \in R$ with $a \neq 0_R$. Then*

$$\begin{array}{lrcl} & ab & = & ac \\ \Longleftrightarrow & b & = & c \\ \Longleftrightarrow & ba & = & ca \end{array}$$

Proof. Suppose $ab = ac$. Then $ab - ac = 0_R$ and so $a(b - c) = 0_R$. Since $a \neq 0_R$ and R is an integral domain, $b - c = 0_R$. Thus $b = c$.

If $b = c$ then clearly $ab = ac$.

Finally since R is commutative, $ba = ca$ implies $ab = ac$. □

Theorem 3.2.7. [**finite int**] *Every finite integral domain is a field.*

Proof. Let R be a finite integral domain. Then R is a commutative ring with identity and $1_R \neq 0_R$. So it remains to show that every $a \in R$ with $a \neq 0_R$ is a unit. Set $S := \{ar \mid r \in R\}$. Define

$$\alpha : R \to S, r \to ar$$

By the Cancellation Law 3.2.6 α is 1-1. By definition of S, α it is also onto. So α is a bijection and $|R| = |S|$. Since $S \subseteq R$ and R is finite we conclude $R = S$. In particular, $1_R \in S$ and so there exists $b \in R$ with $1_R = ab$. Since R is commutative we also have $ba = 1_R$ and so a is a unit. □

3.3 Homomorphism and Ideals

Definition 3.3.1. [**ringhom**] *Let $(R, +, \cdot)$ and $(S, \triangle, \Box)$ be rings.*

(a) [**a**] *A* ring homomorphism *from R to S is a map $\phi : R \to S$ such that for all $a, b \in R$*

$$\phi(a + b) = \phi(a) \triangle \phi(b) \text{ and } \phi(a \cdot b) = \phi(a) \Box \phi(b)$$

(b) [**b**] *A bijective ring homomorphism is called a* ring isomorphism.

(c) [**d**] *If there exists a ring isomorphism from R to S, we say that R and S are* isomorphic *and we write $R \cong S$.*

Definition 3.3.2. [**def:subring**] *Let $(R, +, \cdot)$ be a ring.*

(a) [**a**] *A* subring *of R is a ring $(S, \triangle, \Box)$ such that S is a subset of R and*

$$s \triangle t = s + t \quad \text{and} \quad s \Box r = s \cdot t$$

for all $s, t \in R$.

(b) [**b**] *A left (right)* ideal *in R is a subring I of R such that $ri \in I$ ($ir \subseteq I$) for all $r \in R, i \in I$.*

(c) [**c**] *I is an ideal in R if I is a left ideal and a right ideal in R.*

Lemma 3.3.3. [**subring**] *Let R be a ring and $S \subseteq R$ such that*

(i) [**i**] $0_R \in S$.

(ii) [**ii**] *$a + b \in S$ for all $a, b \in S$.*

(iii) [**iii**] *$-a \in S$ for all $a \in S$.*

(iv) [**iv**] *$ab \in S$ for all $a, b \in S$.*

Define $+_S : S \times S \to S, (a, b) \to a + b$ and $\cdot_S : S \times S, (a, b) \to a \cdot b$. Then $(S, +_S, \cdot_S)$ is a subring of S.

If S fulfills (i),(ii), (iii) and

(iv′) [**ivp**] *$rb \in S$ for all $r \in R, b \in S$,*

then S is a left ideal.

If S fulfills (i),(ii), (iii) and

(iv″) [**ivpp**] *$ar \in S$ for all $r \in R, a \in S$,*

then S is a right ideal in G

If S fulfills, (i),(ii), (iii) , ((iv′)) and ((iv″)) then S is an ideal.

Proof. Straightforward and we leave the few details to the reader. □

Example 3.3.4. [**ex:ideals**]

1. [**1**] Let A be any subgroup of $(\mathbb{Z},+)$. Then by Homework 2#2b, $A = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Since A is a subgroup of $(\mathbb{Z},+)$ conditions i,ii,iii on an ideal are fulfilled. If $a \in A$ and $r \in \mathbb{Z}$, then $a = nm$ for some $m \in \mathbb{Z}$ and so $ra = ar = (nm)(r) = n(mr) \in n\mathbb{Z} = A$. So A is an ideal in $\mathbb{Z}$.

2. [**3**] Let I be any non-zero ideal in $(\mathbb{Q},+,\cdot)$. We will show that $I = \mathbb{Q}$. Indeed let $a \in I$ with $a \neq 0$ and $b \in \mathbb{Q}$. Then $b = (ba^{-1})a$ and since I is an ideal, $b \in I$. Thus $I = \mathbb{Q}$. Hence the only ideal in $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$. The same argument shows that if D is a division ring the only left ideals in D are $\{0_D\}$ and D.

3. [**2**] Let R be a ring and $n \in \mathbb{Z}^+$. Let $R^n = \{(v_i)_{i=1}^n \mid v_i \in R\}$. For $v = (v_i) \in R^n$ and $A = (a_{ij})_{ij} \in \mathrm{M}_{nn}(R)$ define

$$Av := \left(\sum_{j=1}^n a_{ij}v_j\right)_{i=1}^n$$

So if we view $(v_i)_i$ as a column vector (that is an $n \times 1$-matrix) this is just matrix multiplication. Put $\vec{0} = 0_{R^n} = (0_R)_{i=1}^n$, $S = \mathrm{M}_{nn}(R)$ and define

$$\mathrm{Ann}_S(v) = \{A \in S \mid Av = \vec{0}\},$$

$\mathrm{Ann}_S(v)$ is called the annihilator of v in S.

We will show that $\mathrm{Ann}_S(v)$ is an ideal in S. Let $A, B \in \mathrm{Ann}_S(v)$ and $C \in S$. Then

$$\begin{aligned} 0_S v &= \vec{0} \\ (A+B)v &= Av + Bv = \vec{0} + \vec{0} = \vec{0} \\ (-A)v &= -(Av) = -\vec{0} = \vec{0} \\ (CA)v &= C(Av) = A\vec{0} = \vec{0} \end{aligned}$$

Hence 0_S, $A+B$, $-A$ and CA all are in $\mathrm{Ann}_S(v)$ and so by 3.3.3 $\mathrm{Ann}_S(v)$ is a left ideal in R.

We remark that usually $\mathrm{Ann}_S(v)$ is not a right ideal. Suppose for example that $n = 2$ and there exists $a \in R$ with $a^3 \neq 0$, where we just wrote 0 for 0_R. Put

$$v = \begin{pmatrix} 0 \\ a \end{pmatrix}, A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$$

Then

$$Av = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and}$$

$$ABv = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a^2 \\ 0 \end{pmatrix} = \begin{pmatrix} a^3 \\ 0 \end{pmatrix}$$

So $A \in \mathrm{Ann}_S(v)$ but $AB \notin \mathrm{Ann}_S(v)$. This show that $\mathrm{Ann}_S(v)$ is not a right ideal.

Now suppose that $n = 2$, R has an identity $1_R = 1$ and $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \qquad \text{and so}$$

$$\mathrm{Ann}_S(v) = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \middle| b, d \in R \right\}$$

This is a left ideal. Similarly

$$\left\{ \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \middle| b, d \in R \right\}$$

is a right ideal.

Lemma 3.3.5. [**basicring hom**] *Let $\phi : R \to S$ be a ring homomorphism.*

(a) [**a**] *If T is a subring of R, $\phi(T)$ is a subring of S.*

(b) [**b**] *If T is a subring of S then $\phi^{-1}(T)$ is a subring of R.*

(c) [**c**] $\ker \phi$ *an ideal in R.*

(d) [**d**] *If I is a (left,right) ideal in R and ϕ is onto, $\phi(I)$ is a (left,right) ideal in S.*

(e) [**e**] *If J is a (left,right) ideal in S, then $\phi^{-1}(J)$ is a (left,right) ideal on R.*

Proof. (a) By 2.6.3(d), $\phi(T)$ is a subgroup of $(S, +)$. Let $a, b \in \phi(T)$. Then $a = \phi(x)$ and $b = \phi(y)$ for some $x, y \in T$. Since T is a subring of R. $xy \in T$ and so

$$ab = \phi(x)\phi(y) = \phi(xy) \in T$$

Hence T is a subring of S

(b) Similar to (a) and we skip the details.

(c) By 2.6.3(i), $\ker\phi$ is a subgroup of $(R,+)$. Let $a\in\ker\phi$ and $r\in R$. Then

$$\phi(ra)=\phi(r)\phi(a)=\phi(r)0_S=0_S$$

and so $ra\in\ker\phi$. Similarly $ar\in\ker\phi$ and so $\ker\phi$ is an ideal.

(d) Suppose T is a left ideal in R. By (a), $\phi(R)$ is a subring of R. Let $s\in S$ and $a\in\phi(T)$. Then $a=\phi(t)$ for some $t\in T$ and since ϕ is onto, $s=\phi(r)$ for some $r\in R$. Since T is left ideal, $rt\in T$. Thus

$$sa=\phi(r)\phi(t)=\phi(rt)\in\phi(T)$$

Hence $\phi(T)$ is a left ideal in S. Similarly if T is a right ideal, $\phi(T)$ is a right ideal of S. It follows that if I is an ideal in R, then $\phi(I)$ is an ideal in S.

(e) Similar to (d). □

Definition 3.3.6. [**def:a+b**] *Let R be a ring and $A,B\subseteq R$. Then*

(a) [**a**] $A+B:=\{a+b\mid a\in A,b\in B\}$.

(b) [**b**] $\langle A\rangle$ *is the subgroup of* $(R,+)$ *generated by* A.

(c) [**c**] *For* $1\leq i\leq n$ *let* $A_i\subseteq R$. *Then*

$$A_1A_2\dots A_n:=\langle a_1a_2\dots a_n\mid a_i\in A_i,1\leq i\leq n\rangle$$

(d) [**d**] $(A)=\bigcap\{I\mid I$ *is an ideal in* $R,A\subseteq I\}$. (A) *is called the* ideal *in* R *generated by* A.

One should observe that for subsets A and B of a group we defined $AB=\{ab\mid a\in A,b\in B\}$. This differs from the definition of AB for subsets of a ring.

Lemma 3.3.7. [**easy ideal**] *Let R be a ring and $A,B,C\subseteq R$.*

(a) [**y**] $\langle A\rangle=\{\sum_{i=1}^m n_ia_i\mid m\in\mathbb{N},a_i\in A\}$.

(b) [**w**] *If A or B is a subgroup of $(R,+)$, then* $AB=\{\sum_{i=1}^n a_ib_i\mid m\in\mathbb{N},a_i\in A,b_i\in B\}$.

(c) [**z**] $A(BC)=ABC=(AB)C$.

(d) [**x**] *A is an ideal in R if and only if A is subgroup of $(R,+)$ and $RA\subseteq A$.*

(e) [**a**] *If A is a left ideal, then AB is a left ideal.*

(f) [**b**] *If B is a right ideal, then AB is a right ideal.*

(g) [**c**] *If A is a left ideal in R and B is right ideal, then AB is a ideal in R.*

(h) [**v**] *If A and B are subgroup of $(R,+)$ then $A+B$ is a subgroup of $(R,+)$.*

(i) [**d**] *If A and B are (right,left) ideals then $A+B$ is a (left,right) ideal.*

(j) [**e**] *Let $(A_i, i \in I)$ be a family if (left,right) ideals of R, then $\bigcap_{i\in I} A_i$ is a (left,right) ideal.*

(k) [**f**] *(A) is an ideal.*

Proof. Let $r \in R, a \in A, b \in B$ and $c \in C$.

(a) Let $D = \{\sum_{i=1}^m n_i a_i \mid m \in \mathbb{N}, a_i \in A\}$. It is readily verified that D is a subgroup of $(R,+)$ and contains A. So $\langle A\rangle \subseteq D$ by the definition of $\langle A\rangle$. Since $\langle A >$ is closed under addition and negatives, $D \subseteq \langle A\rangle$ and (a) holds.

(b) Since $AB = \langle ab \mid a \in A, b \in B\rangle$ we conclude from (a) that

$$AB = \{\sum_{i=1}^m n_i(a_ib_i) \mid m \in \mathbb{N}, a_i \in A, b_i \in B\}$$

If A is a subgroup of $(R,+)$, then $n_ia_i \in A$ and if B is a subgroup of R then $n_ib_i \in B$. Since $n_i(a_ib_i) = (n_ia_i)b_i = a_i(n_ib_i)$ its is easy to see that (b) holds.

(c) We have $abc = a(bc) \in A(BC)$. Since $A(BC)$ is a subgroup of $(R,+)$ we conclude

$$ABC = \langle abc \mid a \in A, b \in B, c \in C\rangle \subseteq A(BC)$$

Let $d \in BC$. Then by (a) and definition of BC, $d = \sum_{i=1}^m b_ic_i$ for some $b_i \in B, c_i \in C$.

$$ad = a\sum_{i=1}^m b_ic_i = \sum_{i=1} ab_ic_i \in ABC$$

Since ABC is a subgroup of $(R,+)$ we conclude $A(BC) \leq ABC$. Thus $A(BC) = ABC$ and similarly $(AB)C = ABC$.

(d) If A is left ideal, A is a subgroup of R and $ra \in A$. Hence also $RA \subseteq A$. Suppose now that A is a subgroup of R and $RA \subseteq A$. Then $ra \in A$ and so by 3.3.3 A is an left ideal.

(e) Note that RA is a subgroup of $(R,+)$. Also $R(RA) = (RR)A \subseteq RA$ and so by (d), RA is a left ideal in A.

(f) Similar to (e).

(g) Follows from (e) and (f).

(h) Since $(R,+)$ is abelian, $A+B = B+A$. Thus by 2.8.9, $A+B$ is a subgroup of $(R,+)$.

(i) Suppose A and B are left ideals. By (h), $A+B$ is a subgroup of $(R,+)$. Since A and B are left ideal, $ra \in A$ and $rb \in B$. Hence $r(a+b) = ra + rb \in A+B$ and so $A+B$ is a left ideal. The remaining statements are proved similarly.

(j) Suppose each A_i is an left ideal. By 2.3.5 $\bigcap_{i\in I} A_i$ is subgroup of $(R,+)$. Let $a \in \bigcap_{i\in I} A_i$. The $a \in A_i$ 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. The remaining statements are proved similarly.

(k) By definition (A) is the intersection of the ideals containing A and so by (j), is an ideal. □

Lemma 3.3.8. [**ideals with id**] *Let R be a ring with identity and $A \subseteq R$.*

(a) [**u**] *A is a left ideal in R if and only if $RA \subseteq A$ and if and only if $RA = A$.*

(b) [**g**] *$RA = \bigcap\{I \mid A \subseteq I, I$ is a left ideal in $R\}$.*

(c) [**h**] *$AR = \bigcap\{I \mid A \subseteq I, I$ is a right ideal in $R\}$.*

(d) [**i**] *$(A) = RAR$.*

Proof.

[**u**] If A is a left ideal, then by 3.3.7(d), $RA \subseteq A$. Suppose $RA \subseteq A$. Since $A = 1_R A \subseteq RA$ we get $A = RA$. Suppose that $A = RA$. Then $RA \subseteq A$ and since RA is a subgroup of $(R, +)$, A is a subgroup of $(R, +)$. Thus by 3.3.7(d), A is a left ideal in R.

(b) Let $K = \bigcap\{I \mid A \subseteq I, I \text{ is a left ideal in} R\}$. Clearly $RA \subseteq I$ for each left ideal containing A and so $RA \leq K$. By 3.3.7(e), RA is a left ideal. Since R has an identity, $A \subseteq RA$ and so $K \leq RA$.

If R has an identity, the $\langle A \rangle = 1_R A \leq RA$.

(c) and (d) are proved similarly to (b). □

Lemma 3.3.9. [**RmodI**] *Let I be an ideal in the ring R.*

(a) [**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) [**b**] *$(R/I, +_{R/I}, \cdot_{R/I})$ is a ring.*

(c) [**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 2.6.5. $i, j \in I$. 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 2.6.5 $(R/I, +)$ is a group. The remaining axioms of a ring are readily verified.

(c) By 2.6.5 is a well-defined homomorphism of abelian groups with $\ker \pi = I$. Since

$$\phi(ab) = ab + I = (a+I) \cdot_{R/I} (b+I) = \pi(a) \cdot_{R/N} \pi(b)$$

and so π is a ring homomorphism. □

A little warning: Let $a, b \in R/I$. Then $a \cdot_{R/I} b$ is usually not equal to $a \cdot b$. (Note that a, b are subsets of R and so $a \cdot b = \langle xy \mid x \in a, y \in b\rangle$.) For example consider $R = \mathbb{Z}$ and $a = b = I = 2\mathbb{Z}$. Then

$$2\mathbb{Z} \cdot 2\mathbb{Z} = 4\mathbb{Z} \text{ and } 2\mathbb{Z} \cdot_{Z/2\mathbb{Z}} 2\mathbb{Z} = (0 + 2\mathbb{Z}) \cdot_{\mathbb{Z}/2\mathbb{Z}} (0 + 2\mathbb{Z}) = 0 + 2\mathbb{Z}$$

Nevertheless we still usually just write ab for $a \cdot_{R/N} b$ if its clear from the context that are viewing a, b as elements of R/I and not has subsets of R.

Theorem 3.3.10 (The Isomorphism Theorem for Rings)**.** [**iso 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 2.6.8, 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. □

3.4 Polynomials Rings

3.4.1 (Definition and Notation)**.** [**poly**]

Let R be a ring, Let $R[x]$ the set of all sequence $f = (f_i)_{i=1}^{\infty}$ with $f_i \in R$ and such that there exists $n \in \mathbb{N}$ with $f_i = 0_R$ for all $i > n$. For $f = (f_i)_i$ and $g = (g_i)_i$ in $R[x]$ define

$$(f_i)_i + (g_i)_i = (f_i + g_i)_i$$
$$(f_i)_i \cdot (g_j)_j = (\textstyle\sum_{i=0}^{k} f_i g_{k-i})_k$$

Then it is easy but somewhat tedious to verify that $(R[x], +, \cdot)$ is a ring, called the polynomial ring over R.

Let $r \in R$ and $m \in \mathbb{N}$ and consider the sequence $(h_i)_i$ with $f_m = r$ and $h_i = 0_R$ for $i \neq m$. So

$$(h_i)_i = (0_R, 0_R, 0_R, \ldots, 0_R, r, 0_R, \ldots)$$

with the r in position m We denote this sequence by rx^m. Be aware that we did not define that x but only what the symbol rx^m stands for. Then

$$(f_i) = \sum_{i=0}^{\infty} f_i x^i$$

Note that since almost all of the $f_i x^i$ are equal to zero, this seemingly infinite sum is finite and makes sense.

Addition and multiplication now read:

$$\textstyle\sum_{i=0}^{\infty} f_i x^i + \sum_{i=0}^{\infty} g_i x_i = \sum_{i=0}^{\infty} (f_i + g_i) x^i$$
$$\textstyle\sum_{i=0}^{\infty} f_i x^i \cdot \sum_{j=0}^{\infty} g_j x_j = \sum_{k=0} \left(\sum_{i=0}^{k} f_i g_{k-i} \right) x^k$$

and hence

$$\sum_{i=0}^{\infty} f_i x^i \cdot \sum_{j=0}^{\infty} g_j x^j = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} f_i g_j x^{i+j}$$

Observe that the map $r \to rx^0$ is a 1-1 ring homomorphism from R to $R[x]$. We therefore can identify r with rx^0. So r is identified with the sequence

$$(r, 0_R, 0_R, 0_R, \ldots)$$

and R becomes a subring of $R[x]$. Also $0_{R[x]} = 0_R$.

Suppose that R has an identity. Then 1_R is also an identity in $R[x]$. Denote $1_R x^1$ by x. So x is the sequence $(0_R, 1_R, 0_R, 0_R, \ldots)$. Then $x^m = 1_R x^k$ and $r \cdot x^m = (rx^0) \cdot (1_R x^m) = (r \cdot 1_R) x^{0+m} = rx^m$.

If $0_R \neq f \in R[x]$, then we can write $f = \sum_{i=0}^{m} f_i x^i$ with $f_m \neq 0_R$. m is called the degree of f and is denoted by $\deg f$. If $f = 0_R$ we define $\deg f = -\infty$.

Lemma 3.4.2. [**poly universal**] *Let $\alpha : R \to S$ be a ring homomorphism and $s \in R$ such that $\alpha(r)s = s\alpha(r)$ for all $r \in R$.*

(a) [**a**] *The map*

$$\alpha_s : R[x] \to S, \sum_{i=0}^{\infty} f_i x^i \to \sum_{i=0}^{\infty} \alpha(f_i) s^i$$

is a ring homomorphism. (Here we defined $ts^0 = t$ for all $t \in R$.)

(b) [**b**] *Suppose that R and S are rings with identity and $\alpha(1_R) = 1_S$. Then α_s is the unique ring homomorphism from $R[x]$ to S with*

$$\alpha_s(r) = \alpha(r) \text{ and } \alpha_s(x) = s$$

for all $r \in R$.

Proof. (a)

Let $f = \sum_{i=0}^{\infty} f_i x^i$ and $g = \sum_{i=0}^{\infty} g_i x^i$ be elements of $R[x]$. Then

$$\begin{aligned}
\alpha_s(f+g) &= \alpha_s\big(\textstyle\sum_{i=0}^{\infty}(f_i+g_i)x^i\big) &&= \textstyle\sum_{i=0}^{\infty}\alpha(f_i+g_i)s^i \\
&= \textstyle\sum_{i=0}^{\infty}(\alpha(f_i)+\alpha(g_i))s^i &&= \big(\textstyle\sum_{i=0}^{\infty}\alpha(f_i)s^i\big)+\big(\textstyle\sum_{i=0}^{\infty}\alpha(g_i)s^i\big) \\
& &&= \alpha_s(f)+\alpha_s(g)
\end{aligned}$$

and

$$\begin{aligned}
\alpha_s(fg) &= \alpha_s\Big(\textstyle\sum_{k=0}^{\infty}\big(\sum_{i=0}^{k}f_ig_{k-i}\big)x^k\Big) &&= \textstyle\sum_{k=0}^{\infty}\alpha\big(\sum_{i=0}^{k}f_ig_{k-i}\big)s^k \\
&= \textstyle\sum_{k=0}^{\infty}\sum_{i=0}^{k}\alpha(f_i)\alpha(g_{k-i})s^{i+(k-i)} &&= \textstyle\sum_{k=0}^{\infty}\sum_{i=0}^{k}\alpha(f_i)s^i\alpha(g_{k-i})s^{k-i} \\
&= \textstyle\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\alpha(f_i)s^i\alpha(g_j)s^j &&= \big(\textstyle\sum_{i=0}^{\infty}\alpha(f_i)s^i\big)\cdot\big(\textstyle\sum_{j=0}^{\infty}\alpha(g_j)s^j\big) \\
& &&= \alpha_s(f)\alpha_s(g)
\end{aligned}$$

Thus α_s is a homomorphism.

(b) We have

$$\alpha_s(r) = \alpha_s(rx^0)\alpha(r)s^0 = \alpha(r)1_S = \alpha(r)$$

and

$$\alpha_s(x) = \alpha_S(1_R)x^1) = \alpha(1_R)s^1 = 1_S s = s$$

and α_s fulfills the requirements on α_s.

Now let $\beta : R[x] \to S$ be any ring homomorphism from $R[x]$ to S with $\beta(r) = \alpha(r)$ and $\beta(x) = s$ for all $r \in R$. If T is any ring with identity we define $t^0 = 1_T$ for all $t \in T$. We claim that $\beta(x^i) = s^i$ for all $i \in \mathbb{N}$. Indeed $\beta(x^0) = \beta(1_R) = \alpha(1_R) = 1_S = s^0$ and inductively

$$\beta(x^{i+1}) = \beta(x^i)\beta(x) = s^i s = s^{i+1}$$

Thus

$$\beta(\sum_{i=0}^{\infty} f_i x^i) = \sum_{i=0}\beta(f_i)\beta(x^i) = \sum_{i=0}^{\infty}\alpha(f_i)s^i$$

Thus $\beta = \alpha_s$. □

Example 3.4.3. [**ring of functions**] *Let R be a ring and I a set. Let R^I be the set of all functions from I to R. For $f, g \in R^I$ define $f+g$ and fg in R^I by $(f+g)(r) = f(r)+g(r)$ and $(fg)(r) = f(r)g(r)$. Then $(R^I, +, \cdot)$ is a ring, called the* ring of functions *from R to R. Indeed we put $R_i = R$ for all $i \in R$, then R^I is precisely the direct product $\bigtimes_{i\in I} R_i$.*

Lemma 3.4.4. [**poly as function**] *Let R be a commutative ring. For $f = \sum_{i=0}^{\infty} f_i x^i \in R[x]$ define*

$$f^* : R \to R, r \to \sum_{i=0} f_i r^i$$

$$^*: R[x] \to R^R, f \to f^*$$

is a ring homomorphism, that is $(f+g)^* = f^* + g^*$ *and* $(fg)^* = f^*g^*$ *for all* $f, g \in R[x]$.

Proof. Note that $f^*(r) = \mathrm{id}_r(f)$, in the notation of 3.4.2 with $\alpha = \mathrm{id}_R$. So id_r is a homomorphism and thus

$$(f+g)^*(r) = \mathrm{id}_r(f+g) = \mathrm{id}_r(f) + \mathrm{id}_r(g) = f^*(r) + g^*(r) = (f^* + g^*)(r)$$
$$(fg)^*(r) = \mathrm{id}_r(fg) = \mathrm{id}_r(f)\mathrm{id}_r(g) = f^*(r)g^*(r) = (f^*g^*)(r)$$

□

Example 3.4.5. [**ex f***] The table below lists the functions corresponding to the polynomials of degree less than or equal to 2 with coefficients in $\mathbb{Z}_2$.

f	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
$f^*(0)$	0	1	0	1	0	1	0	1
$f^*(1)$	0	1	1	0	1	0	0	1

We conclude that $x^* = (x^2)^*$. So two distinct polynomials can lead to the same polynomial function. Also $(x^2+x)^*$ is the zero function but x^2+x is not the zero polynomial.

3.5 Euclidean Rings

Definition 3.5.1. [**def:pre-euclidean**] *Let R be a commutative ring.*

(a) [**c**] $R^\sharp := R \setminus \{0_R\}$

(b) [**a**] *A function*

$$d : R \to \mathbb{N}$$

is called a pre-Euclidean *function provided that for all* $a, b \in R$

(a) [**a**] $d(r) = 0$ *if and only if* $r = 0_R$*; and*

(b) [**b**] *If* $0 < d(b) \leq d(a)$*, then there exists* $t \in R$ *with* $d(a - tb) < d(a)$

(c) [**b**] *R is called an* Euclidean domain *if R is an integral domain and there exists an pre-Euclidean function on R.*

Example 3.5.2. [**ex:euclidean**]

1. [**1**] Let $d : \mathbb{Z} \to \mathbb{Z}, m \to |m|$ 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 is negative, then $|a + b| > |a|$. So d is a pre-Euclidean function.

2. [**2**] Let $\mathbb{F}$ be any field, for $f = \sum_{i=0}^{n} f_i x^i \in F[x]$ let $d(f) \in \mathbb{N}$ be minimal with $f_i = 0$ for all $i \geq d(f)$. So $d(f) = 0$ if $f = 0_{\mathbb{F}}$ and $d(f) = \deg(f) + 1$ if $f \neq 0$. Let $0_F \neq f, g \in \mathbb{F}[x]$ of degree n and m respectively. Suppose that $d(f) < d(g))$. Then also $n < m$. 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.

Lemma 3.5.3 (Division Algorithm)**.** [**division algorithm**] *Let d be a pre-Euclidean function on a commutative ring R. Let $a, b \in R$ with $b \neq 0_R$. Then there exist $s, r \in R$ with*

$$a = qb + r \text{ and } d(r) < d(b).$$

Proof. If $d(a) < d(b)$ we can choose $q = 0$ and $r = a$.

So suppose that $d(b) \leq d(a)$. Then by the definition of a pre-Euclidean function there exists $t \in R$ such that $d(a - tb) < d(a)$. By induction on $d(a)$ there exists $\tilde{r}, \tilde{q} \in R$ with

$$a - tb = \tilde{q}b + \tilde{r}$$

with $d(\tilde{r}) < d(r)$. So we can choose $q = \tilde{q} + t$ and $r = \tilde{r}$. □

Note that the proof of 3.5.3 provides a concrete algorithm to compute q and r (provided one has a method to find $t \in R$ with $d(a - tb) < d(a)$ whenever $a, b \in R$ with $b \neq 0_R$ and $d(a) \geq d(b0)$. This algorithm is called the *division algorithm*

Example 3.5.4. [**ex:division algorithm**] As an example we consider the ring $R = \mathbb{Z}_2[x]$, $a = x^5 + x^2 + 1$ and $b = x^3 + x + 1$. Then the division algorithm is nothing else but long division of polynomials:

$$\begin{array}{r|ccccccccc}
\multicolumn{1}{r}{} & x^2 & + & 1 & & & & & & \\ \cline{2-10}
x^3+x+1 & x^5 & & & + & x^2 & & & + & 1 \\ \cline{1-1}
\multicolumn{1}{r}{} & x^5 & + & x^3 & + & x^2 & & & & \\ \cline{2-10}
\multicolumn{1}{r}{} & & & x^3 & & & & & + & 1 \\
\multicolumn{1}{r}{} & & & x^3 & & & + & x & + & 1 \\ \cline{3-10}
\multicolumn{1}{r}{} & & & & & & & x & &
\end{array}$$

So $a = qb + r$ where $q = x^2 + 1$ and $r = x$.

Definition 3.5.5. [**def:euclidean**] *Let R be ring. A function $d : R \to \mathbb{N}$ is called an* Euclidean function *if for all $a \in R$ and $b \in R^{\#}$:*

(i) [**c**] $d(a) = 0$ *if and only if* $a = 0_R$.

(ii) [**a**] *if* $ab \neq 0_R$ *then* $d(ab) \geq d(b)$.

(iii) [**b**] *There exist q, r in R with*

$$a = qb + r \text{ and } d(r) < d(b).$$

Lemma 3.5.6. [**pre-euclidean gives euclidean**] *Let d be a pre-euclidean function on the ring R with identity. Let $a \in R$. If $a = 0_R$ define $d^*(a) = 0$, otherwise put*

$$d^*(a) = \min\{d(b) \mid 0_R \neq b \in Ra\}.$$

Then d^* is a Euclidean function.

Proof. If $x \in R$ with $x \neq 0_R$ pick $x^* \in Rx$ with $x \neq 0_R$ and $d(x)$ minimal. Then by definition of d^*, $d^*(x) = d(x^*)$. Since R has an identity, $a = 1_R a \in Ra$ and so $d^*(a) \leq d(a)$. We need to verify the conditions ii-iii in the definition of a Euclidean function.

(ii): If $a = 0_R$, then $d^*(a) = 0$. If $a \neq 0_R$, then also $a^* \neq 0_R$ and so by definition of a pre-Euclidean function, $d^*(a) = d(a^*) \neq 0_R$.

(ii): $Rab \subseteq Rb$ and so by definition of $d^*(b)$, $d^*(b) \leq d(e)$ for all $e \in Rab$. In particular, $d^*(b) \leq d^*(ab)$.

(iii): Let $a, b \in R$ with $b \neq 0_R$. Pick $b^* \in Rb$ with $d^*(b) = d(b^*)$. By 3.5.3 there exists $\tilde{q}$ and $\tilde{r}$ with

$$a = \tilde{q}b^* + r^* \text{ and } d(\tilde{r}) < d(b^*).$$

Since $b^* \in Rb$, $b^* = tb$ for some $t \in R$. Put $q = \tilde{q}t$ and $r = \tilde{q}$. Then

$$a = \tilde{q}b^* + \tilde{r} = \tilde{q}ta + \tilde{r} = qb + r$$

and

$$d^*(r) \leq d(r) < d(b^*) = d^*(b).$$

So d^* is indeed a Euclidean function. □

Definition 3.5.7. [**def:principal**] *Let R be a commutative ring.*

(a) [**a**] *An ideal I in R is called a principal ideal if $I = Ra$ for some $a \in R$.*

(b) [**b**] *R is a principal ideal ring if every ideal is a principal ideal.*

(c) [**c**] *R is a principal ideal domain (PID) if R is an integral domain and a principal ideal domain.*

Example 3.5.8. [**ex:pid**]

1. [**1**] Let I be an ideal in $\mathbb{Z}$. Then by 3.3.4(1), $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Since $\mathbb{Z}$ is commutative, $I = \mathbb{Z}n$ and so I is a principal ideal ring. By 3.2.4(1), $\mathbb{Z}$ is an integral domain and so $\mathbb{Z}$ is a principal ideal domain.

2. [**2**] Let $R = \mathbb{Z}[x]$ and define $I = \{f \in Z[x] \mid f^*(0) \in 2\mathbb{Z}\}$. So I consists of all polynomials whose constant coefficient is even. We will show that I is an ideal and that I is not a principal ideal. By 3.4.2(a), the map $\mathrm{id}_0 : \mathbb{Z}[x] \to \mathbb{Z}, f \to f^*(0)$ is a ring homomorphism. Since $z^*(0) = z$ for all $z \in \mathbb{Z}$, id_0 is onto. Note that $I = \mathrm{id}_0^{-1}(2\mathbb{Z})$. Since $2\mathbb{Z}$ is an ideal in $\mathbb{Z}$ we conclude from 3.3.5(e), that I is an ideal in R.

   Suppose for a contradiction that $I = Rf$ for some $R \in I$. Since $2 \in I$, $2 = gf$ for some $g \in R$. Then both g and f are non-zero. Let $n = \deg f$, $m = \deg g$, a is the leading coefficient of f and b is the leading coefficient of g. Then $gf = abx^{n+m}+$ terms of lower degree. Since $ab \neq 0$, gf has degree $n + m$. Since $gf = 2$, $\deg gf = 0$ and so $n + m = 0$. Since $n, m \in \mathbb{N}$ this gives $n = m = 0$ and so $f = a, g = b$ and $ab = 2$. Since $f \in I$, $a = f^*(0)$ is even. Hence for all $h \in R^\#$, $hf = fh = ah$ and the leading coefficient of hf is even. Thus $hf \neq x$ and so $x \notin Rf$. This is a contradiction since $x \in I$ and $I = Rf$.

Theorem 3.5.9. [**Euclidean implies PID**] *Every Euclidean domain is a principal ideal domain. More precisely if I is a non zero ideal in the Euclidean domain R and $0 \neq a \in I$ with $d(a)$ minimal, then $I = Ra$.*

Proof. Let R be an integral domain and d a pre-Euclidean function on R. Let I be an ideal in R. We need to show that $I = Rb$ for some $b \in R$.

If $I = \{0\}$, then $I = R0_R$.

So suppose that $I \neq \{0_R\}$. Let $0_R \neq b \in I$ with $d(b)$ minimal. Let $a \in I$. By 3.5.3 there exist $s, r \in R$ such that $a = sb + r$ with

$$d(r) < d(b)$$

Since $r = a - sb$ and both a, b are in I we get $r \in I$. So the minimal choice of $d(b)$ implies

$$r = 0_R \text{ or } d(r) \geq d(b)$$

The two displayed statements imply $r = 0_R$. Thus $a = sb$ and so $a \in Rb$. Since $a \in I$ was arbitrary, $I \subseteq Rb$. Clearly $Rb \subseteq I$ and so $I = Rb$ is a principal ideal. □

3.6 Primes in Integral Domains

Definition 3.6.1. [**def:divide**] *Let R be an integral domain and $a, b \in R$.*

(a) [**a**] *We say that a* divides *b and write $a \mid b$ if $b = ra$ for some $r \in R$.*

(b) [**b**] *We say that a and b are* associate *and write $a \sim b$ if $a \mid b$ and $b \mid a$.*

(c) [**d**] *We say that a is* proper *if a is neither zero nor a unit.*

(d) [**e**] *A proper element a is* irreducible *if $a = bc$ with $b, c \in R$ implies that b or c is a unit.*

(e) [**f**] *A proper element a is a* prime *if $a \mid bc$ with $b, c \in R$ implies $a \mid b$ or $a \mid c$.*

Lemma 3.6.2. [**divide**] *Let R be an integral domain and $a, b, c, d \in R$.*

(a) [**a**] *$a \mid b$ if and only if $b \in Ra$ and if and only if $Rb \subseteq Ra$.*

(b) [**b**] *If $a \mid b$ and $b \mid c$ then $a \mid c$.*

(c) [**c**] *$a \sim b$ if and only if $Ra = Rb$.*

(d) [**d**] *$\sim$ is an equivalence relation.*

(e) [**e**] *Let $a \sim b$ and $c \sim d$. Then $a \mid c$ if and only if $b \mid d$.*

Proof. (a) Suppose $a \mid b$. Then $b = ra$ for some $r \in R$ and so $b \in Ra$.

Suppose $b \in Ra$. Since Ra is an left ideal, $Rb \subseteq Ra$.

Suppose $Rb \subseteq Ra$. The $b = 1_R b \in Ra$ and so $b = ra$ for some $r \in R$ and $a \mid b$.

(b) If $a \mid b$ and $b \mid c$ then by (a) $Rc \subseteq Rb \subset Ra$ and so $a \mid c$.

(c) By (a) $a \mid b$ and $b \mid a$ if and only if $Rb \leq Ra$ and $Ra \leq Rb$. So if and only if $Ra = Rb$.

(d) By (c) $a \sim b$ if and only if $Ra = Rb$. So by 2.4.2(2) $\sim$ is an equivalence relation.

(e) Since $a \sim b$, $Ra = Rb$ and since $c \sim d$, $Rc = Rd$. So both $a \mid c$ and $b \mid d$ are equivalent to $Rc \subseteq Ra$. □

Lemma 3.6.3. [**easy unit**] *Let R be an integral domain and $a \in R$. The the following are equivalent*

(a) [**a**] *a is a unit.*

(b) [**b**] *$a \mid 1_R$.*

(c) [**c**] *$a \sim 1_R$.*

(d) [**d**] *$Ra = R$.*

Proof. Suppose a is a unit. Then $ba = 1_R$ for some $r \in R$ and $a \mid 1 - R$.

Suppose $a \mid 1_r$. Since $a = a1 - R$, $1_R \mid a$ and so $a \sim 1_R$.

Suppose $a \sim 1_R$. Then by 3.6.2(c), $Ra = R1_R = R$.

Suppose $Ra = R$. Then $1_R = ba$ for some $b \in R$. Since R is commutative, $ab = 1_R$ and so a is a unit. □

Lemma 3.6.4. [**unit and sim**] *Let R be an integral domain and $a, b \in R$ with $b \neq 0_R$. Then $b \sim ab$ if and only if a is a unit.*

Proof. Suppose that a is a unit. Then $ca = 1_R$ for some $c \in R$. Thus $b = 1_R b = (ca)b = c(ab)$ and so $ab \mid a$. Clearly $b \mid ab$ and so $b \sim ab$.

Suppose that $b \sim ab$. Then $b = c(ab)$ for some $c \in R$ and so $1_R b = b = c(ab) = (ca)b$. By the Cancellation Law 3.2.6 $ca = 1_R$. So a is a unit. □

Lemma 3.6.5. [**char irr**] *Let R be integral domain and a a proper element in R. Then a is irreducible if and only if for all $b \in R$, $b \mid a$ implies that b is a unit or $a \sim b$.*

Proof. Suppose that a is irreducible and $b \mid a$. Then $a = rb$ for some $r \in R$. Thus by the definition of irreducible, r is a unit or b is a unit. If r is a unit then by 3.6.4 $a \sim b$. So b is a unit or $a \sim b$.

Conversely suppose that $b \sim a$ implies that b is a unit or $b \sim a$. Let $a = xy$ with $x, y \in R$. Then $x \mid a$ and so x is a unit or $x \sim a$. If $x \sim a = xy$ then by 3.6.4 y is a unit. So x is a unit or y is a unit. Thus a is irreducible. □

Lemma 3.6.6. [**primes are irreducible**] *All primes in an integral domain are irreducible.*

Proof. Let a be a prime in the integral domain R. The by definition a is proper. Suppose that $a = bc$ with $b, c \in R$. Then $a \mid bc$ and since a is a prime, $a \mid b$ or $a \mid c$. Say $a \mid c$. Since also $c \mid a$ we get $bc = a \sim c$ and so by 3.6.4 c is a unit. Thus a is irreducible. □

Definition 3.6.7. [**def:gcd**] *Let R be an integral domain, $A \subseteq R$ and $b \in R$.*

(a) [**a**] *We say that b is a common divisor of A and write $b \mid A$ if $b \mid a$ for all $a \in A$.*

(b) [**b**] *We say that d is a greatest common divisor of A if d is a common divisor for A and $b \mid d$ for all common divisors of b of A.*

Note that we do not claim the existence of greatest common divisors. Indeed this is false in arbitrary integral domains.

Example 3.6.8. [**ex:gcd**] Consider the ring $\mathbb{Z}$. The divisors of 24 are

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$$

The divisors of 20 are

$$\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$$

So the common divisors of $\{20, 25\}$ are

$$\pm 1, \pm 2, \pm 4$$

Hence the greatest common divisors of $\{20, 25\}$ are

$$\pm 4$$

So we see that a set can have more than one greatest common divisor. But note that 4 and -4 are associated.

Lemma 3.6.9. [**gcd is unique up to associates**] *Let R be an integral domain, $A \subseteq R$ and a any greatest common divisor for A. Let $b \in R$. Then b is a greatest common divisor of A if and only if $a \sim b$.*

Proof. Suppose first that b is a greatest common divisor of A. Since a is a common divisor for A and b is a greatest common divisor $b \mid a$. By symmetry $a \mid b$ and so $a \sim b$.

Suppose next that $a \sim b$. Then $b \mid a$. Since $a \mid d$ for all $d \in A$, we get from 3.6.2(b) that $b \mid d$ for all $d \in A$. So b is a common divisor of A. Let e be any common divisor of A. Then $e \mid a$ and since $a \mid b$ we get $e \mid b$. Thus b is a greatest common divisor of A. □

Lemma 3.6.10. [**sum divides**] *Let R be an integral domain, $A \subseteq R$ and b a common divisor of A in R. Then $b \mid x$ for all $x \in RA$.*

Proof. Let $a \in A$. Then $b \mid a$ and so $a \in Rb$. Thus $A \subseteq Rb$ and since Rb is an ideal, $RA \subseteq Rb$. Since $x \in RA$ we conclude $x \in Rb$ and so $b \mid x$. □

Proposition 3.6.11. [**gcd in PID's**] *Let R be a PID and $A \subseteq R$.*

(a) [**a**] *A has a greatest common divisor.*

(b) [**b**] *Let $d \in R$. Then d is a greatest common divisor of A if and only if $Rd = RA$.*

(c) [**c**] *Let d be a greatest common divisor of A. Then*

$$d = r_1a_1 + r_2a_2 + \ldots + r_na_n$$

for some $n \in \mathbb{N}$, $a_i \in A$ and $r_i \in R$.

Proof. (a) Since R is a PID and RA is an ideal in R, there exists $e \in R$ with $Re = RA$. Then $a \in Re$ for all $a \in R$ and so e is a common divisor of A. Let b be any common divisor of A. Since $e \in RA$, 3.6.10 gives $b \mid e$. Hence e is a greatest common divisor of A.

(b) Let $d \in R$. Then by 3.6.9 d is a greatest common divisor if and only if $d \sim e$. So by 3.6.2(c) if and only if $Rd = Re = RA$.

(c) By (b), $d \in Rd = RA$ and so by 3.3.7(b), $d = r_1a_1 + r_2a_2 + \ldots + r_na_n$ for some $n \in \mathbb{N}$, $a_i \in A$ and $r_i \in R$. □

Proposition 3.6.12. [**in PiD's irreducible = prime**] *An element in a PID is a prime if and only if its is irreducible.*

Proof. Let $a \in R$ be proper. If a is a prime then a is irreducible by 3.6.6.

So suppose a is irreducible and let $b, c \in R$ with $a \mid bc$. By 3.6.11 there exists a greatest common divisor d for a and b. Then $d \mid a$ and so by 3.6.5, d is a unit or $d \sim a$. If $d \sim a$, then $a \mid d$ and $d \mid b$ and so $a \mid b$. So suppose that d is a unit. Then $1_R \sim d$ and by 3.6.9 1_R is a gcd for a and b. Thus by 3.6.11 $1_R = ra + sb$ for some $r, s \in R$. Hence $c = rac + sbc$. Since a divides bc and a we conclude that a divides c. We showed that $a \mid b$ or $a \mid c$ and so a is prime. □

Example 3.6.13. [**ex:gcd in pid**]

We have $\gcd(20, 24) = \pm 4$ and $24 = 20 + 4$. So $4 = 24 - 20 = 1 \cdot 24 + (-1) \cdot 20$.

For a more complicated example consider 63 and 37. We have

$$\begin{array}{rcrcr}
63 & = & 37 & + & 26 \\
37 & = & 26 & + & 11 \\
26 & = & 2 \cdot 11 & + & 4 \\
11 & = & 2 \cdot 4 & + & 3 \\
4 & = & 1 \cdot 3 & + & 1 \\
3 & = & 3 \cdot 1 & + & 0
\end{array}$$

So according to Homework 6#7 1 is a gcd of 63 and 37. To compute 1 as a linear combination of 63 and 37, we use a backtracking method:

$$\begin{array}{rcl cl}
1 & = & 4 - 3 & & \\
3 & = & 11 - 2 \cdot 4 & & \\
1 & = & 4 - (11 - 2 \cdot 4) & = & 3 \cdot 4 - 11 \\
4 & = & 26 - 2 \cdot 11 & & \\
1 & = & 3 \cdot (26 - 2 \cdot 11) - 11 & = & 3 \cdot 26 - 7 \cdot 11 \\
11 & = & 37 - 26 & & \\
1 & = & 3 \cdot 26 - 7 \cdot (37 - 26) & = & 10 \cdot 26 - 7 \cdot 37 \\
26 & = & 63 - 37 & & \\
1 & = & 10 \cdot (63 - 27) - 7 \cdot 37 & = & 10 \cdot 63 - 17 \cdot 37
\end{array}$$

So $1 = 10 \cdot 63 - 17 \cdot 37$.

Lemma 3.6.14. [**prime and associate**] *Let R be an integral domain and $a, b \in R$ with $a \sim b$.*

(a) [**a**] *a is proper if and only if b is proper.*

(b) [**b**] *a is a prime if and only if b is a prime.*

Proof. Note that by 3.6.2(c), $Ra = Rb$. So it suffices to show the properties 'proper' and 'prime' only depended on Ra.

(a) a is proper if and only if $a \neq 0_R$ and a is not a unit. By 3.6.3 this is the case if and only if $Ra \neq \{0_R\}$ and $Ra \neq R$.

(b) By (a) we may assume that a and b are proper. Then a is prime if and only if $a \mid bc$ implies $a \mid b$ or $a \mid c$. This is the case if and only if $bc \in Ra$ implies $b \in Ra$ or $c \in Ra$. □

Lemma 3.6.15. [**divide and irreducible**] *Let R be an integral domain and $q, b \in R$. Suppose that $q \mid b$ and q is a prime.*

(a) [**a**] *If b is irreducible, then $q \sim b$ and b is a prime.*

(b) [**b**] *If $b = b_1 \dots b_n$ with $n \in \mathbb{Z}^+$ and $b_i \in R$, then $q \mid b_i$ for some $1 \le i \le n$.*

(c) [**c**] *If $b = p_1 \dots p_n$ with $n \in \mathbb{Z}^+$ and each $p_i, 1 \le i \le n$ is irreducible in R, then $q \sim p_i$ for some $1 \le i \le n$.*

Proof. (a) Since b is irreducible and $q \mid b$ we conclude from 3.6.5, q is a unit or $q \sim b$. But a is a prime and so not a unit. Hence $q \sim b$. Thus by 3.6.14(b), b is a prime.

(b) If $n = 1$, then $b = b_1$. So suppose $n > 1$ and let $a = b_1 \dots b_{n_1}$. Then $b = ab_n$ and since $q \mid b$ and q is a prime, $q \mid a$ or $q \mid b_n$. In the first case we conclude by induction on n, that $q \mid b_i$ for some $1 \le i \le n-1$. So (b) holds.

(c) By (b), $q \mid p_i$ for some $1 \le i \le n$ and so by (a), $q \sim p_i$. □

Proposition 3.6.16. [**Uniqueness of prime factorizations**] *Let R be an integral domain and $a \in R$. Suppose that $a = p_1 \cdot \ldots \cdot p_n$ and $a = q_1 \dots q_m$ where $n, m \in \mathbb{Z}^+$, p_i is a irreducible for $1 \le i \le n$ and q_j are is a prime for $1 \le i \le n$. Then $n = m$ and there exists $\pi \in \mathrm{Sym}(n)$ with $q_i \sim p_{\pi(i)}$ for all $1 \le i \le n$.*

Proof. . Note that $q_m \mid a$. Hence by 3.6.15(c), $q_m \sim p_i$ for some $1 \le i \le n$. Without loss, $i = n$. Then $p_n \sim q_m$ and so $up_n = q_m$ for some unit $u \in R$.

Suppose $n = 1$. If $m = 1$ we are done. So suppose for a contradiction that $m > 1$. Then$(q_1 \dots q_{m-1})q_m = a = p_m \sim q_m$. Thus by 3.6.4, $q_1 \dots q_{m-1}$ is a unit and so divides 1_R. Hence also q_1 divides 1_R and so q_1 is a unit. A contradiction since q_1 is a prime and so proper.

Suppose $n > 1$. Then $q_{m-1}q_m = q_{m-1}(up_n) = (uq_{m-1})p_n$. By 3.6.4 $uq_{m-1} \sim q_{m-1}$ and by 3.6.14, q_{m-1} is a prime and p_n are primes. So replacing q_m by p_n and q_{m-1} by uq_{m-1} we may assume that $p_n = q_m$. Put $b = q_1 \dots q_{m-1}$ if $m > 1$ and $b = 1_R$ if $m = 1$. Then

$$(p_1 \dots p_{n-1})p_n = a = (q_1 \dots q_{m-1}q_m = bq_m$$

Since R is an integral domain, R has no non-zero zero-divisors and so the Cancellation Law 3.2.6 implies

$$p_1 \dots p_{n-1} = b$$

Suppose that $m = 1$. Then $b = 1_R$ and so p_1 is a unit, a contradiction since p_1 is irreducible and so proper.

Thus $m > 1$ and

$$p_1 \dots p_{n-1} = q - 1 \dots q_{m-1}$$

So by induction on n, $n - 1 = m - 1$ and there exists $\mu \in Sym(n-1)$ with $q_i \sim p_{\mu(i)}$ for all $1 \le i \le n-1$. Define $\pi \in \mathrm{Sym}(n)$ by $\pi(n) = n$ and $\pi(i) = \mu(i)$ for $1 \le i \le n-1$. Then the Lemma holds. □

Definition 3.6.17. [**def:ufd**] *A unique factorization domain (UFD) is an integral domain in which each proper element is a product of primes.*

Lemma 3.6.18. [**In UFD's irreducible=primes**] *An element in a UFD is a prime if and only if its is irreducible.*

Proof. Let a be an irreducible element in the UFD R. Since a is a product of primes, there exists a prime p with $p \mid a$. Hence by 3.6.15(a), a is a prime.

If a is a prime, then a is irreducible by 3.6.6 □

Lemma 3.6.19. [**divisor in Euclidean domains**] *Let R be an Euclidean domain with Euclidean function d. Let $a, b \in R^{\#}$ with $a \mid b$.*

(a) [**a**] $d(a) \leq d(b)$.

(b) [**b**] $a \sim b$ *if and only* $d(a) = d(b)$.

Proof. (a) $b = ra$ for some $r \in R$. Since $b \neq 0_R$ the definition of an Euclidean function implies $d(b) \geq d(a)$.

(b) Suppose $a \sim b$. Then $a \mid b$ and $b \mid a$. By (a), $d(a) \leq d(b)$ and $d(b) \leq d(a)$. Thus $d(a) = d(b)$.

So suppose that $d(a) = d(b)$. By(a)

$$d(b) = d(a) = \min\{d(e) \mid e \in Ra.e \neq 0_R\}$$

Thus by 3.5.9 $Ra = Rb$. Hence by 3.6.3 $a \sim b$. □

Proposition 3.6.20. [**Euclidean domains are UFD**] *Every Euclidean domain is a UFD.*

Proof. Let R be a Euclidean domain with Euclidean function d. By 3.5.9 R is a PID and so by 3.6.12 every irreducible element in R is a prime. So it suffices to show that each proper element a is a product of irreducible elements. If a is irreducible we are done. So suppose $a = bc$ with neither b nor c units. Then by 3.6.4 $a \nsim b$ and $a \nsim c$. Hence by 3.6.19(b), $d(a) \neq d(b)$ and $d(a) \neq d(c)$. So by 3.6.19(a), $d(b) < d(a)$ and $d(c) < d(a)$. Thus by induction of $d(a)$, b and c are products of irreducible elements. Thus also a is. □

3.7 The Gaussian integers

Definition 3.7.1. [**def:s adjoint i**] *Let R be a ring, S a subring of R and I a subset. Then $S[I]$ denotes the intersection of all subrings of R containing S and I. Note that $S[I]$ itself is a subring if R and is the smallest subring of R containg S and I. $S[I]$ is pronounced "S adjoint I". If $I = \{i_1, i_2, \ldots, i_n\}$ we also write $S[i_1, i_2, \ldots i_n]$ for $S[I]$.*

Definition 3.7.2. [**def:gauss**]

(a) [**a**] *The subring $\mathbb{Z}[i]$ of $\mathbb{C}$ is called the ring of Gaussian integers.*

(b) [**b**] *A prime in $\mathbb{Z}[i]$ is called an Gaussian prime.*

(c) [**c**] *For $x = a+bi \in \mathbb{C}$ let $\overline{x} = a-bi$ and $d(x) = x\bar{x} = a^2+b^2$. The map $:: \mathbb{C} \to \mathbb{C}, x \to \overline{x}$ is is called complex conjugation.*

In this section we will show that $\mathbb{Z}[i]$ is an Euclidean domain and will determine the primes in $\mathbb{Z}[i]$.

Lemma 3.7.3. [**the elements in Z[i]**] $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$

Proof. Since $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ and contains $\mathbb{Z}$ and i, $\mathbb{Z}+\mathbb{Z}i \subseteq \mathbb{Z}[i]$. Since $(a+bi)+(c+di) = (a+c)+(b+d)i$ and $(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i$, $\mathbb{Z}+\mathbb{Z}i$ is also closed under addition and multiplication. Hence $\mathbb{Z}+\mathbb{Z}i$ is a subring of $\mathbb{C}$ containing $\mathbb{Z}$ and i. So $\mathbb{Z}[i]] \subseteq \mathbb{Z}+\mathbb{Z}i$. □

Lemma 3.7.4. [**Properties of complex conjugation**]

(a) [**a**] *Complex conjugation is ring automorphism of $\mathbb{C}$.*

(b) [**b**] *Restricted to $\mathbb{Z}[i]$, complex conjugation is a ring automorphism of $\mathbb{Z}[i]$*

(c) [**c**] *$d(x) = x\overline{x}$ and $d(xy) = d(x)d(y)$ for all $x, y \in \mathbb{C}$.*

(d) [**d**] *Let $x \in \mathbb{C}$. Then $d(x) \geq 0$ with equality if and only if $x = 0$.*

(e) [**e**] *$d(x) \in \mathbb{N}$ for all $x \in \mathbb{Z}[i]$*

Proof. (a) Since $\overline{\overline{a+bi}} = \overline{a-bi} = a+bi$, is an inverse of and so complex conjugation is a bijection. Let $a, b, c, d \in \mathbb{R}$. Then

$$\overline{a+bi}+\overline{c+di} = (a-bi)+(c-di) = (a+c)-(b+d)i = \overline{(a+c)+(b+d)i} = \overline{(a+bi)+(c+di)}$$

and

$$\overline{a+bi}\cdot\overline{c+di} = (a-bi)\cdot(c-di) = (ac+bd)-(ac+bc)i = \overline{(ac+bd)-(ac+bc)i} = \overline{(a+bi)\cdot(c+di)}$$

So is a ring homomorphism. Thus (a) holds.

(b) Observe that $\overline{x} \in \mathbb{Z}[i]$ for all $x \in \mathbb{Z}[i]$. Thus the restriction of to $\mathbb{Z}[i]$ is 1 its own inverse and ring homomorphism.

(c) Let $x = a + bi$ with $a, b \in \mathbb{R}$. Then $d(x) = a^2 + b^2 = (a + bi)(a - bi) = x\overline{x}$.

$$d(xy) = (xy)\overline{xy} = xy\overline{x}\overline{y} = (x\overline{x})(y\overline{y}) = d(x)d(y)$$

(d) Clearly $d(x) = a^2 + b^2 \geq 0$ and $d(x) = 0$ if and only if $a = b = 0$ and so if and only if $x = 0$.

(e) Obvious. □

Lemma 3.7.5. [**approximation by gaussian integers**] *Let $x \in \mathbb{C}$ then there exists $y \in \mathbb{Z}[i]$ with $d(x - y) \leq \frac{1}{2}$.*

Proof. Let $x = x_1 + x_2 i$ with $x_i \in \mathbb{R}$. Then there exists $y_i \in \mathbb{Z}$ with $|x_i - y_i| \leq \frac{1}{2}$ (Just round x_i to the nearest integer). Let $y = y_1 + y_2 i$. Then

$$d(x - y) = (x_1 - y_1)^2 + (x_2 - y_2)^2 \leq \frac{1}{2}^2 + \frac{1}{2}^2 = \frac{1}{2}$$

□

Lemma 3.7.6. [**Gaussian integers form an Euclidean domain**] *$\mathbb{Z}[i]$ is an Euclidean domain with Euclidean function on d.*

Proof. Since $\mathbb{C}$ is a field, $\mathbb{C}$ is an is an integral domain. Hence also $\mathbb{Z}[i]$ is a integral domain. It remains to show that d is an Euclidean function. Let $a, b \in \mathbb{Z}[i]^{\#}$. Then $d(a)$ and $d(b)$ are positive integers and so

$$d(ab) = d(a)d(b) \leq d(b)$$

By 3.7.5 there exists $s \in \mathbb{Z}[i]$ with $d(\frac{a}{b} - s) \leq \frac{1}{2} < 1$. Put $r = a - sb$. Then

$$d(r) = d(b(\frac{a}{b} - s)) = d(b)d(\frac{a}{b} - s) < d(b)$$

and

$$a = sb + r$$

So d is an Euclidean function. □

Lemma 3.7.7. [**units in gaussian integers**] *Let a be a Gaussian integer. Then the following are equivalent:*

(a) [**a**] *a is a unit in $\mathbb{Z}[i]$.*

(b) [**b**] *$d(a) = 1$*

(c) [**c**] *a is one of $1, -1, i$ and $-i$.*

Proof. (a) $\Longrightarrow$ (b): Suppose that $ab = 1$ for some $b \in \mathbb{Z}[i]$. Then $d(a)d(b) = d(ab) = d(1) = 1$. Since $d(a)$ and $d(b)$ are non-negative integers we conclude that $d(a) = 1$.

(b) $\Longrightarrow$ (c): Let $a = x + iy$ with $x, y \in \mathbb{Z}$. Then $x^2 + y^2 = d(a) = 1$ and so $\{|x|, |y|\} = \{0, 1\}$. So either $x = 0$ and $y = \pm 1$ or $y = 0$ and $x = \pm 1$. Thus $a = \pm 1, \pm i$.

(c) $\Longrightarrow$ (a): In each case $d(a) = 1$. Thus $a\overline{a} = 1$ and a is a unit. □ □

Lemma 3.7.8. [**associates and unit**] *Let R be an integral domain and $a, b \in R$. Then $a \sim b$ if and only if $a = ub$ for some unit u in R.*

Proof. Suppose first that $a \sim b$. Then $b \mid a$ and so $a = ub$ for some $u \in R$. If $b \neq 0_R$, then by 3.6.4 u is a unit. If $b = 0_R$, then also $a = 0_R$ and $a = 1_R b$. So in both cases $a = ub$ for a unit b in R.

Suppose next that $a = ub$ for a unit $u \in R$. Then $b = u^{-1}b$. Hence $a \mid b$ and $b \mid a$ and so $a \sim b$. □

Lemma 3.7.9. [**associates of Gaussian integers**] *Let $x, y \in \mathbb{Z}$ and $a = x + yi$. Then the associates of a in $\mathbb{Z}[i]$ are $a = x + yi, -a = -x - yi, ia = -y + xi$ and $-ia = y - xi$.*

Proof. Let $b \in \mathbb{Z}[i]$. By 3.7.8 $n \sim a$ if and only if $b = ua$ for some unit u in $\mathbb{Z}[i]$ and so by 3.7.7 if and only if b is one of $a, -a, ia, -ia$ □

Lemma 3.7.10. [**Gaussian primes**] *Let a be a Gaussian prime. Then there exists an positive prime integer p such that one of the follwing holds:*

(a) [**a**] *$d(a) = p^2$, $a \sim p$ and p is a Gaussian prime.*

(b) [**b**] *$d(a) = p$, $a \not\sim p$ and p is not a Gaussian prime.*

Proof. Since $d(a$ is a positive integer, $d(a) = p_1 p_2 \ldots p_n$ where each p_i is a positive prime integer. Since $d(a) = a\overline{a}$, a divides $d(a)$. Since a is a Gaussian prime we conclude from 3.6.15(b) that $a \mid p_i$ (in $\mathbb{Z}[i]$) for some $1 \leq i \leq n$. Put $p = p_i$. Then $a \mid p$ and $p \mid d(a)$. Hence $a = pb$ for some $b \in Z[i]$ and so $p^2 = d(p) = d(ab) \overset{3.7.4(c)}{=} d(a)d(b)$.

Thus $d(a)$ divides $d(p) = p^2$ in $\mathbb{Z}$. Since a is not a unit, we from 3.7.7 that $d(a) > 1$ and so $d(a) \in \{p, p^2\}$.

If $d(a) = p^2$ we get $d(b) = 1$. So by 3.7.7 b is a unit and $a \sim p$. Since a is a Gaussian prime, 3.6.14(b) implies that p is a Gaussian prime. Thus (a) holds in this case.

If $d(a) = p$ then $d(b) = p$. So 3.7.7 b is not a unit and by 3.6.4 $p \nsim bp = a$. Since a divides p and a is neither p nor $a \sim p$ we conclude from 3.6.5 that p is not irreducible. Thus by 3.6.6 p is not a prime. hence (b) holds in this case. □

Lemma 3.7.11 (Wilson)**.** [**Wilson's Lemma**] *Let p be prime. Then* $(p-1)! \equiv -1 \pmod{p}$

Proof. If $p = 2$, then $(p-1)! = 1! = 1 \equiv -1 \pmod 2$. So suppose that p is odd.

Let $i \in Z_p$ with $i \neq 0$. Since Z_p is a field i has an inverse i^{-1}. For $n \in n\mathbb{Z}$ let $\tilde{n} = n + \phi Z \in \mathbb{Z}_p$ We have

$$\begin{aligned} & i = i^{-1} \\ \iff \quad & i^2 = \tilde{1} \\ \iff \quad & (i-\tilde{1})(i+\tilde{1}) = \tilde{0}0 \\ \iff \quad & i - \tilde{1} = \tilde{0} \text{ or } i + \tilde{1} = \tilde{0} \\ \iff \quad & i = \tilde{1} \text{ or } i = -\tilde{1} \end{aligned}$$

Let $k = \frac{|\mathbb{Z}_p^\sharp|-2}{2} = \frac{p-3}{2}$. Then we can choose $a_1, \dots a_k \in \mathbb{Z}_p$ with

$$\mathbb{Z}_p^\sharp \setminus \{\tilde{1}, -\tilde{1}\} = \{a_i, a_i^{-1} \mid 1 \leq i \leq k\}$$

Thus

$$\prod_{i \in Z_p^\sharp} i = \tilde{1} \cdot -\tilde{1} \cdot \prod_{i=1}^{k} a_i a_i^{-1} = -\tilde{1}$$

Since $Z_p^\sharp = \{\tilde{n} \mid 1 \leq n \leq p-1\}$ we get

$$(p-1)! \equiv \prod_{n=1}^{p-1} n \equiv -1 \pmod p$$

□

Theorem 3.7.12. [**More on Gaussian primes**] *Let p be a prime integer. Then the following are equivalent:*

(a) [**a**] *p is not a Gaussian prime.*

(b) [**b**] *There exists a Gaussian prime a with $p = a\overline{a}$.*

(c) [**c**] *There exists integers a and b with $p = a^2 + b^2$.*

(d) [**d**] *$p = 2$ or $p \equiv 1 \mod 4$.*

(e) [**e**] *There exists an integer x with $x^2 \equiv -1 \mod p$.*

Proof. (a) $\Longrightarrow$ (b):

Since p is not a unit and $\mathbb{Z}[i]$ is Euclidean and so a UFD, p is a product of Gaussian primes. In particular there exists a Gaussian prime a with $a \mid p$. Hence $d(a)$ divides

$d(p) = p^2$ in $\mathbb{Z}$. If $d(a) = p^2$, then by 3.7.10 p is a Gaussian prime, a contradiction to (a). Since a is not a unit, $d(a) \neq 1$ and so $d(\alpha) = p$.

(b) $\Longrightarrow$ (c):

Let $\alpha = a + ib$ with $a, b \in \mathbb{Z}$. Then $p = \alpha\overline{\alpha} = a^2 + b^2$.

(c) $\Longrightarrow$ (d):

Let $a = 2k + u$ and $b = 2l + v$ with $k, l \in \mathbb{Z}$ and $u, v \in \{0, 1\}$. Then

$$p = a^2 + b^2 = 4k^2 + 4k + u^2 + 4l^2 + 4l + v^2 \equiv u + v \mod 4$$

If $u + v$ is even, then p is even and so $p = 2$.

If $u + v$ is odd, then $u + v = 1$ and so $p \equiv 1 \mod 4$.

(d) $\Longrightarrow$ (e): If $p = 2$ we can choose $x = 1$. So suppose that $p \equiv 1 \mod 4$. Put $x = \frac{p-1}{2}!$. Since $\frac{p-1}{2}$ is even we conclude

$$\begin{aligned} x &= (-1) \cdot (-2) \cdot \ldots \cdot (-\frac{p-1}{2}) \\ &\equiv (p-1) \cdot (p-2) \cdot \ldots \cdot \frac{p+1}{2} \mod p \end{aligned}$$

So 3.7.11 implies Thus $x^2 \equiv (p-1)! \equiv -1 \mod p$.

(e) $\Longrightarrow$ (a):

Suppose that p is a Gaussian prime. Since $x^2 \equiv -1 \mod p$ we get that $p \mid x^2 + 1 = (x+i)(x-i)$. Since p is a Gaussian prime, p has devide $x + i$ or $x - i$. Since $p = \overline{p}$ we conclude that p divides $x + i$ and $x - i$ and so also $(x+i) - (x-i) = 2i$. But then $d(p) = p^2$ divides $d(2i) = 4$ and so $p = 2$. But $2 = (1+i)(1-i)$ and neither $1 + i$ nor $1 - i$ is a unit. Thus $p = 2$ is not irreducible and so also not a prime in $\mathbb{Z}[i]$. □

Note that part (c) and (d) of the previous theorem say that an integral prime is the sum of two integral squares if and only if its 2 or 1 mod 4.

3.8 Constructing fields from rings

Lemma 3.8.1. [**field of fractions**] *Let R be an integral domain. Then there exists a field $\mathbb{F}$ such that R is a subring F and R is not contained in any proper subfield of F. Moreover, $F = \{ab^{-1} \mid a, b \in R, b \neq 0_R\}$ and if K is any other such field then there exists a unique ring isomorphism $\alpha : F \to K$ with $\alpha(r) = r$ for all $r \in R$. F is called the* field of fractions *of R and denoted by F_R.*

Proof. Informally F consists of all $\frac{a}{b}$ with $a, b \in R$ and $b \neq 0_R$. Addition and multiplication are defined by

$$(*) \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

Moreover two fraction $\frac{a}{b}$ and $\frac{c}{d}$ are equal if $ad = bc$.

But what really is $\frac{a}{b}$? We will define a fraction as an equivalence class of pairs (a, b):

Let $D = R \times R^\sharp = \{(a, b) \mid a, b \in R \mid b \neq 0_R$. Define the relation $\approx$ on D by $(a, b) \approx (c, d)$ if $ad = bc$. We will show that $\approx$ is a equivalence relation. Since R is commutative, $ab = ba$ and so $(a, b) \approx (a, b)$ for all $(a, b) \in D$. Thus $\approx$ is reflexive. If $ad = bc$ then $cb = da$ and so $(c, d) \approx (a, b)$. Thus $\approx$ is symmetric. Suppose now that $(a, b) \approx (c, d)$ and $(c, d) \approx (e, f)$ with $(a, b), (c, d), (e, f) \in D$. Then $ad = bc$ and $cf = de$. Hence also $adf = bcf$ and $bcf = bde$. Thus $adf = bde$ and $(af)d = (be)d$. Since $d \neq 0_R$, the Cancellation Law 3.2.6 implies that $af = bd$ and so $(a, f) \approx (b, e)$. Hence $\approx$ is transitive and so an equivalence relation. For $(a, b) \in D$ let $\frac{a}{b}$ be the equivalence class of $\approx$ containing (a, b). So

$$\frac{a}{b} = \{(c, d) \mid c, d \in R, d \neq 0_R, ad = bc\}$$

Let $F = D/\approx$ be the set of equivalence class of $\approx$. So

$$F = \{\frac{a}{b} \mid a, b \in R, b \neq 0_R\}$$

We use (*) to define addition and multiplication on F, but we must verify that this definition does not depend on the choice of the representatives. So let $(a, b), (c, d), (\tilde{a}, \tilde{b}), (\tilde{c}, \tilde{d}) \in D$ with

(**)
$$a\tilde{b} = \tilde{a}b \quad c\tilde{d} = \tilde{c}d$$

We need to show that

$$\frac{ad + bc}{bd} = \frac{\tilde{a}\tilde{d} + \tilde{b}\tilde{c}}{\tilde{b}\tilde{d}} = \qquad \text{and} \qquad \frac{a}{b}\frac{c}{d} = \frac{\tilde{a}\tilde{c}}{\tilde{b}\tilde{d}}$$

This is true if and only if

$$(ad + bd)(\tilde{c}\tilde{d}) = (\tilde{a}\tilde{c} + \tilde{b}\tilde{d})(cd) \quad \text{and} \quad ab\tilde{c}\tilde{d} = cd\tilde{a}\tilde{b}$$

and so if and only if

$$(a\tilde{d})(c\tilde{c}) + (b\tilde{c})(d\tilde{d}) = (\tilde{a}d)(c\tilde{c}) + (\tilde{b}c)(d\tilde{d}) \quad \text{and} \quad (a\tilde{d})(b\tilde{c}) = (\tilde{a}c)(d\tilde{b})$$

But the latter equation follows easily from (**). Thus addition and multiplication is well defined. Some routine calculation show that F is a commutative ring with $0_F = \frac{0_R}{1_R}$ and $1_F = \frac{1_R}{0_R}$. Since $0_R O_R = O_R \neq 1_R = 1_R 1_R$, $0_F \neq 1_F$. $\frac{a}{b} = 0_R$ if and only if $a = a1_R = b0_R = 0_R$. $\frac{a}{b} = 1_F$ if and only if $a = a1_R = b1_R = b$. If $a \neq 0_R$, then $(b, a) \in D$ and $\frac{b}{a} \cdot \frac{a}{b} = \frac{ab}{ab} = 1_F$. So every non-zero element in F has an inverse and F is a field.

It is easy to check that the map $\sigma : R \to F, \mid r \to \frac{r}{1_R}$ is a 1-1 ring homomorphism. So we may identify r with $\frac{r}{1_R}$ and view R has a subfield of F. We have

$$\frac{a}{b} = \frac{a}{1_R}\frac{1_R}{b} = ab^{-1}$$

and so $F = \{ab^{-1} \mid a, b \in R, b \neq 0_R\}$.

Now let K be any field containing R with R not contained in any proper subfield of K. Define $\alpha : F \to K, \frac{a}{b} \to ab^{-1}$. We need to show that α is well defined. Indeed if $ad = bc$ in R then also $ab^{-1} = cd^{-1}$ in K. It is easy to see that α is a ring homomorphism. By Homework 1#1, $1_R = 1_K$ and so for $r \in R$ we have $\alpha(r) = \alpha(\frac{r}{1_R}) = r1_R^{-1} = r1_K^{-1} = r$. Since $\alpha(1_R) = 1_R = 1_K \neq 0_R$ we conclude from Homework 1#2, that α is 1-1 and $\alpha(F)$ is a subfield of K. Since $R = \alpha(R) \subseteq \alpha(F)$ we conclude, from the assumption that R is not contained in a proper subfield of K, that $\alpha(F) = K$. So α is onto. Hence α is an ring isomorphism. □

Definition 3.8.2. [**def:ordered ring**] *Let R be a ring. An* ordering *on R is a subset R^+ such that*

(i) [**i**] *If $r \in R$ then exactly one of the following holds:*

$$r \in R^+, r = 0_R, -r \in R^+$$

(ii) [**ii**] *Let $x, y \in R^+$, then $x + y \in R^+$ and $xy \in R^+$.*

Given an ordering R^+ of R, we define the relation $<$ on R be $x \leq y$ if $y - x \in R^+$ and the relation $\leq$ by $x \leq y$ if $x = y$ or $x \leq y$.

Definition 3.8.3. [**def:partial**] *Let $\leq$ be a relation on the set I.*

(a) [**a**] *$\leq$ is called antisymmetric if $a \leq b$ and $b \leq a$ implies $a = b$.*

(b) [**b**] *$\leq$ is called a partial ordering if $\leq$ is reflexive, anti-symmetric and transitive.*

(c) [**c**] *$\leq$ is called a total ordering if $\leq$ is a partial ordering and for all $x, y \in R$ we have $x \leq y$ or $y \leq x$.*

Lemma 3.8.4. [**ordered rings**] *Let R^+ be an ordering on the ring R. Then*

(a) [**a**] *$x, y \in R$, then exactly one of the following holds:*

$$x < y, x = y, y < x$$

(b) [**z**] *Let $x, y, z \in R$. Then $x < y$ if and only if $x + z \leq y + z$.*

(c) [**y**] *Let $a, b, c, d \in R$ with $a < b$ and $c < d$, then $a + c < c + d$.*

(d) [**b**] *Let $x, y \in R$ and $r \in R^+$,*

(a) [**a**] *$x < y$ if and only if $rx < ry$.*

(b) [**b**] *$x = y$ if and only if $rx = ry$.*

(c) [**c**] *$x \leq y$ if and only if $rx \leq ry$.*

(e) [**c**] *$<$ is transitive and $\leq$ is total ordering on R.*

(f) [**d**] *Let $n \in \mathbb{Z}^+$ and $a \in R^+$. Then $na \in R^+$. In particular $na \neq 0_R$.*

(g) [**e**] *Suppose R has an identity and $1_R \neq 0_R$. Then $1_R \in R^+$. Moreover, if $u \in R^+$ is a unit, then $u^{-1} \in R^+$.*

Proof. (a) By definition of an ordering exactly one of the following holds:

$$y - x \in R^+, y - x = 0_R, -(y - x) \in R^+$$

(a)

Since $-(y - x) = x - y$ we conclude that exactly one of the following holds:

$$x \leq y, x = y, y \leq x$$

(d) If $x < y$, then $y - x \in R^+$ and so also $r(y - x) \in R^+$. Thus $ry - rx = r(y - x) \in R^+$ and so $ry < rx$. If $x = y$ then $rx = ry$ and if $y > x$, $ry > rx$.

So if $rx < ry$ we conclude that $x \neq y$ and $y \not< $ and so $x < y$. Thus (d:a) holds. If $rx = ry$ we conclude that neither $x < y$ nor $y < x$ and so $x = y$. So (d:b) holds.

(d:c) follows from (d:a) and (d:c)

(b) This follows from $(y + z) - (x + z) = y - x$.

(c) $(a + c) - (b + d) = (a - b) + (c - d) \in R^+$ since both $a - b$ and $c - d$ are in R^+. Thus $a + c < b + d$.

(e) Suppose $x < y$ and $y < z$. Then $y - x \in R^+$ and $z - y \in R^+$. Thus also $z - x = (z - y) + (y - x) \in R^+$ and $x < z$. Hence $<$ is transitive

Clearly $\leq$ is reflexive. Suppose that $x \leq y$, $y \leq x$ and $x \neq y$. Since $x \leq y$, this means $x < y$ and since $y \leq x$, $y < x$, a contradiction to (a). S

Suppose $x \leq y$ and $y \leq z$. If $x = y$ or $y = z$, then clear $x \leq z$. So suppose $x < y$ and $y < z$. Then $x < z$ and so $x \leq z$. The $\leq$ is transitive. Hence $\leq$ is a partial ordering. By (a), $x \leq y$ or $y \leq x$ and so $\leq$ is a total ordering.

(f) If $1a = a \in R^+$. Suppose $na \in R^+$ for some $n \in \mathbb{Z}^+$. Then $(n + 1)a = na + a \in R^+$. So (f) follows from the principal of induction.

(g). Suppose that $1_R \notin R^+$. Since $1_R \neq 0_R$, $-1_R \in \mathbb{R}^+$ and so $1_R = (-1_R)(-1_R) \in R^+$, a contradiction. Thus $1_R \in R^+$. Let $u \in R^+$ be a unit. Then $u0_R = 0_R < 1_R = uu^{-1}$ and so by (e), $0_R < u^{-1}$. Thus $u^{-1} \in R^+$. □

Definition 3.8.5. [**def:archimedian**] *An ordering R^+ on a ring R is called Archimedean, if for all $a, b \in R^+$ there exists $n \in \mathbb{Z}^+$ with $a \leq nb$.*

Definition 3.8.6. [**def:complete**] *Let I be a set, $J \subseteq I$, $m \in I$ and $\leq$ a partial ordering on I.*

(a) [**a**] *m is called an upper bound for J if $j \leq m$ for all $j \in M$.*

(b) [**b**] *J is called bounded if there exists an upper bound for J in I.*

(c) [**c**] *m is called a least upper bound if m is an upper bound for J and $m \leq k$ for all upper bounds $k \in J$.*

(d) [**d**] *$\leq$ is called a complete if every non-empty bounded subset of I has a least upper bound.*

Lemma 3.8.7. [**ordered field of fraction**] *Let R be an integral domain with field of fraction F. Suppose R^+ is an ordering on R and put $F^+ = \frac{a}{b} \mid a, b \in R^+\}$.*

(a) [**a**] *F^+ is an ordering on F and $\mathbb{F}^+ \cap R = R^+$.*

(b) [**b**] *If $a, c \in R$ and $b, d \in R^+$, then $\frac{a}{b} < \frac{c}{d}$ if and only if $ad < bc$.*

(c) [**c**] *R^+ is Archimedean so is F^+.*

Proof. (a) Let $x \in F$ then $x = \frac{a}{b}$ for some $a, b \in R$, $b \neq 0_R$. If $a = 0_R$, then $x = 0_F$. If $a, b \in R^+$ or $-a, -b \in R^+$, then $\frac{b}{=}\frac{-a}{-b} \in R^+$ and if $a \in R^+$ and $-b \in R^+$ or $-a \in R^+$ and $b \in R^+$, then $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b} \in R^+$.

Suppose now that $x \in F^+$ and $-x \in F^+$. Then $x = \frac{a}{b}$ and $-x = \frac{c}{d}$ with $a, b, c, d \in \mathbb{F}$. Thus $\frac{a}{b} = \frac{-c}{d}$ and $ad = -bc$. Put $ab \in R^+$ and $cd \in R^+$. So $-cd \notin R^+$ and $ad \neq -bc$, a contradiction. Also $x \neq 0_R$ for all x with $x \in F^+$ and so also $x \neq 0_R$ for all x with $-x \in \mathbb{F}^+$. Thus exactly one of $x \in F^+, x = 0_R, -x \in F^+$ holds.

let $a, b, c, d \in R^+$, Then ad, bc, ac, bd and $ad + bc$ all are in R^+ and so $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{db}$ and $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ are in $\mathbb{F}^+$. Thus F^+ is an ordering.

Let $r \in R$ with $\frac{r}{1_R} \in F^+$. Then $\frac{r}{1} = \frac{a}{b}$ with $a, b \in R^+$. Thus $rb = a > 0_R = 0_R b$ and so $r > 0_R$ by 3.8.4(d:a).

(b) By 3.8.4(d:a), $\frac{a}{b} < \frac{c}{d}$ if and only if $bd\frac{a}{b} < bd\frac{c}{d}$ and so if and only if $ad < bc$.

(c) Suppose now that R^+ is Archimedean and let $a, b, c, d \in \mathbb{R}^+$. Then ac and $ad, bc \in R^+$ and since R^+ is Archimedean, $ad \leq nbc$ for some $n \in \mathbb{Z}^+$. Thus by (b), $\frac{a}{b} \leq n\frac{c}{d}$. □

3.8.8 (Real Numbers)**.** [**real numbers**]

Let F be a field with a Archimedean ordering F^+. Let $\overline{S}$ be the set of all subsets A of R such that

(i) [**a**] $A \neq \emptyset$ and $A \neq F$.

(ii) [**b**] If $a \in A$ and $b \in \mathbb{Q}$ with $b \leq a$, then $b \in A$.

Let $\overline{S}$ be the set of all $A \in S$ such that

(iii) [**c**] A has no maximal element, that is for each $a \in A$ there exists $c \in A$ with $a < c$.

Put $2_R = 21_R = 1 + r + 1_R$. By 3.8.4 2_R and $2_R^{-1} \in R^+$.

1°. [**1**] *Let $x, y \in F$ with $x < y$. Put $z = \frac{x+y}{2_R}$. Then $x < z < y$.*

Indeed $z - x = \frac{x+y}{2_R} - x = \frac{y-x}{2_R} = (y - x)2_R^{-1} \in R^+$ and similarly $y - z \in F^+$. So (1°) holds.

For $r \in F$ let $A_r = \{a \in F \mid a < r\}$. Since $r - 1_R \in A_r$, $A_r \neq \emptyset$ and since $r \notin A_r$, $A_r \neq F$. If $a \in A_r$ then $a < \frac{a+r}{2_R} < r$ and so a is not a maximal element of A_r. If $b \in F$ with $b \leq a$, then also $b < r$ and so $b \in A + r$. Thus $A_q \in S$. Next we show

2°. [**2**] *The map $F \to S, r \to A_r$ is 1-1.*

Let $r, s \in F$ with $r \neq s$. Without loss $r < s$. Then $r \in A_s$ and $r \notin A_r$. Thus $A_r \neq A_s$ and the map is 1-1.

3°. [**3**] *Let $A \in \overline{S}$ and $b \in F \setminus A$. Then $a < b$ for all $a \in A$.*

If $b \leq a$ for some $a \in A$ we would get $b \in A$, a contradiction. Thus $b \nleq a$ and so $a < b$ for all $a \in A$.

4°. [**4**] *Let $A \in S$ and $B \in \overline{S}$. Define $A \oplus B = A + B = \{a + b \mid a \in A, b \in B\}$. Then $A + B \in S$.*

Since both A and B are proper subsets there exists $a \in A, b \in B$, $x \in F \setminus A$ and $y \in F \setminus B$ with $A \oplus +B$ is not empty. Then $a + b \in A \oplus B$. So $A \oplus B \neq emptset$. By (3°), $a < x$ and $b < y$. Hence by 3.8.4(c), $a + b < x + y$. Thus $a + b \neq x + y$ and $x + y \notin A + B$. Thus $A \oplus B \neq S$. Let $a \in A, b \in B$. Since a is not maximal in A there exists exists $c \in A$ with $a < c$ Then $a + b < c + b$ and so $a + b$ is not maximal in $A \oplus B$. Let $z \in F$ with $z \leq a + b$. Then $z - a \leq b$ and so $z - a \in B$. Thus $z = (z - a) = a \in A \oplus B$. So $A \oplus B \in S$.

5°. [**5**] *Let $a \in F^+$ and $B \in \overline{S}$, then there exists $b \in B$ and $c \in R \setminus B$ with with $c - b = a$.*

Pick $d \in B$ and $e \in F \setminus B$. Since F^+ is Archimedean there exists $n \in \mathbb{Z}^+$ with $e - d \leq na$. Hence $d + na \notin F$ and we can choose $m \in \mathbb{Z}^+$ minimal with $c := d + ma \notin B$. Put $b = d + (m - 1)a$. Then $b \in B$ and $b + a = c$.

6°. [**6**] *Let $A \in S$ and $B \in \overline{S}$. Define $A \ominus B = \{a - c \mid a \in A \mid c \in R \setminus B\}$. Then $A \ominus B \in S$ and $B \oplus (A \ominus B) = A$.*

Let $\tilde{B} = \{-c \mid c \in R \setminus B\}$. Since B proper subset of F, $R \setminus B$ is a proper subset of F and also $\tilde{B} = -(R \setminus B)$ is a proper subset. Let $d \leq -c$ for some $d \in F$ and $c \in R \setminus B$. Then $c \leq -d$ and since $c \notin B$, $-d \notin B$. Thus $d = -(-d) \in \tilde{B}$. So $\tilde{B} \in \overline{S}$ and by (4°), $A \ominus B = A + \tilde{B} \in S$

Let $a \in A, b \in B$ and $c \in F \setminus B$. Then $b < c$, $b - c < 0_F$ and $b + (a - c) = a + (b - c) < a$. Thus $b + (a - c) < a$ and $B \oplus (A \ominus B) \subseteq A$. Since a is not maximal in A, there exists $d \in A$ with $a < d$. By (4°) there exists $x \in B$ and $y \in R \setminus C$ with $y - x = d - a$. So $x - y = a - d$ and $a = (a - d) + d = x - y + d = (x + d) - y \in B \oplus (A \ominus -B)$.

7°. [7] *$F^- = A_{0_F} \in S$ and $A + F^- = A$ for all $A \in S$.*

The first statement is obvious. Let $a \in A$ and $b \in F^-$. Then $a + b < a$ and so $a + b \in A$. Since a is a not a maximal element of A, there exists $c \in A$ with $c \nleq a$ and so $c < a$. Then $a = \frac{a+c}{2_R} + \frac{c-a}{2_F} \in A + F^-$ and so $A = A + F^-$.

8°. [8] *$(S, +)$ is an abelian group. The identity is F^- and the additive inverse of $A \in S$ is $\ominus A := F^- \ominus A$.*

By 2.4.12(a), " + " is associative. Clearly $A + B = B + A$. By (7°), F^- is an additive identity and by (6°), $\ominus A$ is an additive inverse of A.

For $A \subseteq F$ put $A^+ = A \cap F^+$. Let $\overline{S}^+ = \{A \in \overline{S} \mid A^+ \neq \emptyset$ and $S^+ = S \cap \overline{S}^+$. Put $\overline{S}- = S \setminus \overline{S}^+ \cup F^-\}$ and $S^=S \cap \overline{S}^-$. Let $F_0^- = \{a \in F \mid a \leq 0_F\}$. If $A, B \in \overline{S}^+$ define $A \odot B = A^+B^+ \cup F_0^-$. If $A = F^-$ or $B = F^-$ define $A \odot B = F^-$. If $A \in \overline{S}$ and $B^{\in}\S^-$ define $A \odot B = \ominus(A \odot (\ominus B))$ and if $A \in S^-$ and $B \in S$ define $A \odot B = \ominus((\ominus A) \odot B)$.

9°. [9] *$A \odot B \in S$ for all $A \in S, B \in \overline{S}$.*

By definition of $\odot$ is suffices to treat the case where $A, B \in S^+$. As in (4°) one shows that A^+B^+ is a proper subset of F^+, A^+B^+ does not have a maximal element and $x \in A^+B^+$ whenever $x \in F^+$ with $x \leq ab$ for some $a \in A^+, b \in B^+$.

10°. [10] *Put $1_S = A_{1_R}$. Then $1_S \odot A = A$ for all $A \in S$.*

Since $\ominus(\ominus A) = A$ it suffices to treat the case $A \in S^+$. If $b < 1_F$ and $a \in A^+$, then $ba < 1_F a = a$ and so $ba \in A$. Thus $1_S \otimes A \subseteq A$. Since a is not maximal element of A, there exists $c \in A$ with $a < c$. Then $ac^{-1} < 1 - F$ and so $a = ac^{-1}c \in 1_S \otimes A$. Hence $1_S \cdot A = A$.

11°. [11] *Let $B \in \overline{S}^+$ and $e \in F$ with $1_F < e$. Then there exists $x \in B^+$ and $y \in F \setminus B$ with $yx^{-1} = e$.*

Pick $b \in B^+$. Since $1_F < e$, $b < eb$ and so $eb - b \in F^+$. Thus by (5°) there exists $c \in B$ and $d \in R \setminus B$ with $d - c = eb - b$. let $x = \max(b, c)$ and $y = ex$. Then $x \in B$. Since $b \leq x$ and $e - 1_F \in F^+$ we $b(e - 1_F) \leq x(e - 1 - F)$ and so

$$d - c = eb = b = (e - 1_F)b \leq (e - 1_F)x = ex - x = y - x$$

Also $c \leq b$ and thus

$$d = (d - c) + c \leq (y - x) + x = y$$

Since $d \notin B$ we get $y \notin B$. Also $yx^{-1} = exx^{-1} = e$ and (11°) holds.

Let $A \in S$ and $B \in S^\sharp$. Suppose $B \in S^+$ and define $\hat{B} = (F \setminus B)^{-1} \cup F_0^-$. Then $\hat{B} \in \overline{S}^+$. Define $\frac{A}{B} = A \otimes \hat{B}$. If $\overline{B} \in S^-$ define $\frac{A}{B} = \ominus \frac{A}{\ominus B}$.

12°. [12] *Let $A \in S$ and $B \in S^\sharp$. Then $\frac{A}{B} \in S$ and $B \odot \frac{A}{B} = A$.*

Suppose $B \in S^+$. The there exists $b \in B^+$ and $b^{-1} \notin \hat{B}$. Thus $\hat{B} \neq \emptyset$. Let $c \in F \setminus B$. Then $c \in F^+$ and $c^{-1} \in \hat{B}^+$. Thus $\hat{B}^+ \neq \emptyset$. Let $d \in F^+$ with $d \leq c^{-1}$. Then $c \leq d^{-1}$ and since $c \notin B$, $d^{-1} \notin B$. Thus $d = (d^{-1})^{-1} \in \hat{B}$. So $\hat{B} \in \overline{S}$ and by (9°), $\frac{A}{B} = A \odot \hat{B} \in \overline{S}^+$.

To prove $B \odot \frac{A}{B} = A$ it suffices to consider the case $A, B \in S^+$. Let $a \in A^+, b \in B^+$ and $c \in F \setminus B$. Then $b < c$, $bc^{-1} < 1_F$ and $a(bc^{-1}) < a$. Thus $abc^{-1} \in A$ and $B \cdot \frac{A}{B} \subseteq A$. Since a is not maximal in A, there exists $d \in A$ with $a < d$. hence $1_F < da^{-1}$. By (11°) there exists $x \in B^+$ and $y \in F \setminus B$ with $yx^{-1} = da^{-1}$. Then $ad^{-1} = xy^{-1}$ and

$$a = ad^{-1}d = (yx^{-1}d = xdy^{-1} \in B \odot \frac{A}{B}.$$

Hence $A = B \odot \frac{A}{B}$.

13°. [13] *$(S, \oplus, \odot)$ is a field.*

By (10°) 1_S is a identity with respect to $\odot$. By (12°), $B \cdot \frac{1_S}{B} = 1_S$ and so $\frac{1_S}{B}$ is an inverse of $B \in S^\sharp$. By (2°) $1_S = A_{1_F} \neq A_{0_F} = 0_F$. The associative law and commutative law for $\cdot$ and the distributive laws are readily verified. So S is a field.

14°. [14] *S^+ is an ordering on S. Moreover, $A < B$ if and only if $A \subsetneq B$.*

Let $A \in S$. Note that

$$\ominus A = F^- \ominus A = \{c - d \mid c \in F^-, d \in F \setminus A\}$$

If $A \in S^+$, then $A^+ \neq \emptyset$ and so $A \neq 0_S = F^-$. Also $\ominus A \subseteq F^-$ and so $\ominus A \notin S^+$.

If $A = 0_S$, then neither A nor $- \ominus A = A$ is in S^+.

Suppose $A \notin S^+$ and $A \neq F^-$. Then $A^+ = \emptyset$ and so $A \subseteq F_0^-$. Since A has no maximal element, 0_F $/A$. Thus $A \subseteq F^-$. Since $A \neq F^-$ there there exists $e \in F^- \setminus A$. Then $\frac{e}{2_F} - e = -\frac{e}{2_F} \in \mathbb{F}^+ \cap (\ominus A)$ and so $\ominus A \in S^+$.

We conclude that exactly one of $A \in \overline{S}^+, A = 0_S$ and $\ominus A \in \overline{S}^+$ holds. The other properties of an ordering are readily verified.

We have

$$\begin{aligned}
& A < B \\
\iff \quad & B \ominus A \in S^+ \\
\iff \quad & b - d \in S^+ \text{ for some } b \in B, d \in F \setminus A \\
\iff \quad & d < b \text{ for some } b \in B, d \in F \setminus A
\end{aligned}$$

We will show that the last statement is equivalent to $A \subsetneq B$.

If $d < b$ for some $b \in B, d \in F \setminus A$, then by (3°), $b \notin A$ and again by (3°) $a < b$ for all $a \in A$. So using (3°) one more time $a \in B$ and thus $A \subseteq B$. Since $b \notin A$, $A \neq B$ and $A \subsetneq B$.

Conversely suppose $A \subsetneq B$ and let $d \in B \setminus A$. Since B has no maximal element $d < b$ for some $b \in B$. Thus (14°) holds.

15°. [15] *S^+ is Archimedean.*

To show that S^+ is Archimedean let $A, B \in S^+$. Pick $b \in B^+$ and $d \in F \setminus A$. Then since F^+ is Archimedean, $a \leq nb$. Then $nb + b \notin A$ and so $nB \nsubseteq A$. Thus $nB \nleq A$ and $A < nB$. So S^+ is Archimedean.

16°. [16] *S^+ is complete.*

Let $\mathcal{B}$ be a non-empty bounded subset of S. Define $M = \bigcup \mathcal{B}$. Since $\mathcal{B}$ is not empty there exists $B \in \mathcal{B}$. Then $B \in S$ and so $B \neq \emptyset$. Since $B \subseteq M$, $M \neq \emptyset$.

Let K be any upper bound for $\mathcal{B}$. Define $B \subseteq K$ for all $B \in \mathcal{B}$ and so $M \subseteq K$ and $M \leq K$. Since $K \neq F$ we get $M \neq F$ and so M is a proper subset if F. Let $a \in F$ and $b \in M$ with $a \leq b$. Then $b \in B$ for some $B \in \mathcal{B}$. So $a \in B$ and $a \in M$. Suppose d is an maximal element of M. Then $d \in B$ for some $B \in \mathcal{B}$ and d is maximal element of $\mathcal{B}$, a contradiction. Thus $M \in S$. Since $B \leq M$ for all $B \in \mathcal{B}$, M is an upper bound. We already proved $M \leq K$ for all upper bounds of $\mathcal{B}$ and so M is a least upper bound.

Lemma 3.8.9. [**irreducible-maximal**] *Let c be a proper element in the integral domain R. Then the following are equivalent*

(a) [**1**] *c is irreducible.*

(b) [**2**] *For all $a \in R$,*

$$a \mid c \Longrightarrow a \sim c \text{ or } a \text{ is a unit}$$

(c) [**3**] *Rc is maximal in the set of proper principal ideals, that if $a \in R$ with $Ra \neq R$ and $Rc \leq Ra$, then $Rc = Ra$.*

Proof. (a) $\Longrightarrow$ (b): See 3.6.5.

(b) $\Longrightarrow$ (c): Since c is proper, $Rc \neq R$. Suppose $Rc \subseteq Ra$ for some $a \in R$ with $Ra \neq R$. Then $c \mid a$. Thus by (b), $a \sim c$ or a is a unit. If a is a unit, the $Ra = R$ by 3.6.3, a contradiction. Hence $a \sim c$ and so $Ra = Rc$ by 3.6.2(d). Thus (c) holds.

(c) $\Longrightarrow$ (a): Let $a, b \in R$ with and $c = ab$. Then $Rc \subseteq Rb$ and so by (c), $Ra = Rc$ or $Ra = R$ In the first case $a \sim c$ and so by 3.6.4 b is a unit. In the second case a is a unit by 3.6.3 Hence c is irreducible. □

Lemma 3.8.10. [**char max**] *Let R be a commutative ring with identity $1_R \neq 0_R$. Let M be a ideal in R with $R \neq M$. Then R/M is a field if and only if M is a maximal ideal in R.*

Proof. Since $M \neq R$, $1_R \not inM$ and so $1_{R/M} = 1_R + M \neq 0_R + M = 0_{R/M}$.

Suppose first that R/M is a field and let I be an ideal in R with $M \subsetneq R$. Pick $r \in M \setminus R$. Since R/M is a field, $r + M$ has an inverse $s + M$ in R/M. Then

$$rs + M = (r + M)(s + M) = 1_{R/M} = 1_R + M$$

and so $1_R = rs + m$ for some $m \in M$. Since M is an ideal and both r and m are in M we get $rs \in M$ and then $1_R \in M$. Then $R = R1_R \subseteq M$ and $M = R$.

Suppose next that M is a maximal ideal in R and let $0_{R/M} \neq x \in R/M$. Then $x = r + M$ for some $r \in R$ with $r \neq M$. By 3.3.7 $Rr + M$ is an ideal in R. Since $r \in Rr + M$, $M \subsetneq Rr + M$ and so by maximality of M, $R = Rr + M$. Thus $1_R = sr + m$ for some $s \in M$. Then

$$(s + M)(r + M) = rs + +m = (1_R - m) + M = 1_R + M = 1_{R/M}$$

and so $x = r + M$ is invertible in R/M. Thus R/M is a field. □

Lemma 3.8.11. [**constructing fields**] *Let R be a PID and $0_R \neq a \in R$. Then the following are equivalent:*

(a) [**a**] *a is a prime*

(b) [**b**] *a is irreducible*

(c) [**c**] *Ra is a maximal ideal in R.*

(d) [**d**] *R/Ra is a field.*

(e) [**e**] *R/Ra is an integral domain.*

Proof. (a) $\Longrightarrow$ (b): By 3.6.12 every prime in a PID is irreducible.

(b) $\Longrightarrow$ (c): . Since a is irreducible, a is proper. Thus by 3.8.9 Ra is maximal among the proper principal ideals. Since R is a PID, every ideal is principal and so Ra is a maximal ideal.

(c) $\Longrightarrow$ (d): See 3.8.10.

(d) $\Longrightarrow$ (e): By 3.2.5 every field is an integral domain.

(e) $\Longrightarrow$ (a): Let $a, b \in R$ with $c \mid ab$. Then $ab \in Rc$ and so

$$(a + Rp)(b + Rc) = ab + Rc = Rp = 0_{R/Rc}$$

Since R/Rc is an integral domain we get $a + Rc = 0_{Rc} = Rc$ or $b + Rp = 0_{Rc} = Rc$. Hence $a \in Rc$ or $b \in Rc$ and so $c \mid a$ or $c \mid b$. Thus c is a prime. □

Lemma 3.8.12. [**basic deg**] *Let R be an integral domain and $f, g \in R[x]$. Then*

(a) [**a**] $\deg(f + g) \leq \max(\deg f, \deg g)$.

(b) [**b**] $\deg(fg) = \deg f + \deg g$.

(c) [**c**] *$R[x]$ is an integral domain.*

(d) [**d**] *If f divides g in $R[x]$ and $g \neq 0_F$, then* $\deg f \leq \deg g$.

(e) [**e**] *Let f is a unit if and only if $f \in R$ and f is a unit in R.*

Proof. If $f = 0_R$ or $g = 0_R$, the statements about f and g are readily verified. So suppose $f \neq 0_R$ and $g \neq 0_R$. Let $f = \sum_{i=0}^{\infty} f_i x^i$ and $g = \sum_{i=0}^{\infty} g_i x^i$ with $f_i, g_i \in R$, almost all 0. Let $n = \deg f$ and $m \deg m$. Then $f_n \neq 0_R$ and $g_m \neq 0_R$. if

(a) Let $d = \max(n.m)$. Then $f_i = 0 + R = g_i$ for all $i > d$ and so $f + g = \sum_{i=0}^{s}(f_i + g_i)x^i$. Thus $\deg f + g \leq d$.

(b) and (c) We have $fg = \sum_{n=0} \sum_{i=0}^{m} f_i g_j x^{i+k}$. Thus the coefficient of x^k is 0_R for all $k > n + m$ and the coefficient of x^{n+m} is $f_n g_m$. Since R is an integral domain $f_n g_m \neq 0_R$. Thus $\deg(fg) = n + m - \deg f + \deg g$ and $fg \neq 0_R$. Thus (b) and (c) hold.

(d) Let $g = fh$ with $h \in \mathbb{R}[x]$. Since $g \neq 0_R$ also $h \neq 0_R$. Thus $\deg h \geq 0$ and so by (b) $\deg f \leq \deg f + \deg h = \deg(fh) = \deg g$.

(e) Suppose $fg = 1_{\mathbb{K}}$. Then $f \neq 0_R \neq g$ and by (b) $\deg f + \deg g = \deg)fg) = \deg 1_R = 0$. Thus $\deg f = 0 = \deg g$ and $f, g \in R$. So if f is a unite in $K[x]$, then f is a unit in R. The converse is obvious. □

Lemma 3.8.13. [**fields from poly**] *Let $\mathbb{K}$ be a field and let $f \in \mathbb{K}[x]$ with $\deg f \geq 1$. For $g \in \mathbb{K}[x]$, let $\overline{g} = g + f\mathbb{K}[x]$. Put $\mathbb{E} := \mathbb{K}[x]/f\mathbb{K}[x]$*

(a) [**f**] *$\mathbb{K}[x]$ is a Euclidean domain and so also a PID and a UFD.*

(b) [**a**] *$\mathbb{E}$ is a field if and only if f is irreducible and if and only if $\mathbb{E}$ is an integral domain.*

(c) [**b**] *The map $\pi : \mathbb{K}[x] \to \mathbb{E}, g \to \overline{g}$ is a ring homomorphism with $\ker \pi = f\mathbb{K}[x]$.*

(d) [**d**] *For each $e \in \mathbb{E}[x]$ there exists a unique $g \in \mathbb{K}[x]$ with $\deg g < \deg f$ and $e = \overline{g}$. Morever, if $e = \overline{h}$ for some $h \in \mathbb{K}[x]$, then g is the remainder of h, then divided by f.*

(e) [**c**] *The map $\pi|_{\mathbb{K}}\colon \mathbb{K} \to \mathbb{E}, k \to \overline{k}$ is a 1-1 ring homomorphism.*

(f) [**e**] *In view of (e) we may identify $k \in \mathbb{K}$ with $\overline{k} \in \mathbb{E}$. So $\mathbb{K}$ is a subring of $\mathbb{E}$ and $f \in \mathbb{E}[x]$. Then $\overline{x}$ is a root of f in $\mathbb{E}$.*

Proof. (a) By Example 3.5.2(2), $\mathbb{K}[x]$ is an Euclidean ring and by 3.8.12(c), $\mathbb{K}[x]$ is an integral domain. Thus $\mathbb{K}[x]$ is an Euclidean domain. Hence by 3.5.9 $\mathbb{K}[x]$ is a PID and 3.6.20 $\mathbb{K}[x]$ is a UFD.

(b) By (a) $\mathbb{K}[x]$ is a PID. Thus (b) follows from 3.8.11.

(c) See 3.3.9(c).

(d) Let $g \in \mathbb{K}[x]$. By the division algorithm 3.5.3 there exists $q, r \in \mathbb{K}[x]$ with $g = qf + r$ and $\deg r < \deg f$. Since $qf \in f\mathbb{K}[x]$, $g + f\mathbb{K}[x] = (qf + r0 + f\mathbb{K}[x]$ and so $\overline{g} = \overline{r}$.

Suppose now that $s \in \mathbb{K}[x]$ with $\deg s < \deg f$ and $\overline{s} = \overline{g}$. Then $\deg s - r < \deg f$ and $\overline{s} = \overline{r}$. Thus $s - r = tf$ for some $t \in \deg \mathbb{K}[x]$. If $s - r \neq 0_R$ then by 3.8.12(d), $\deg f \leq \deg s - r$ a contradiction. Thus $r - s = 0_{\mathbb{K}}$ and $r = s$.

(e) By (c), $\pi_{\mathbb{K}}$ is a ring homomorphism. Let $k, l \in \mathbb{K}$ with $\overline{k} = \overline{l}$. Then $\deg k = \deg l = 0 < \deg f$ and so by (d), $k = l$.

(f) Let $f = \sum_{i=0}^{n} k_i x^i$ with $k)i \in \mathbb{K}$. Then

$$f(\overline{x}) = \sum_{i=0}^{n} k_i\overline{x}^i = \sum_{i=0}^{n} \overline{k}_i\overline{x}^i = \overline{\sum_{i=0}^{n} k_i x^i} = \overline{f}$$

Since $f \in f\mathbb{K}[x]$, we have $\overline{f} = f + f\mathbb{K}[x] = \mathbb{K}[x] = 0_{\mathbb{E}}$. Hence $f(\overline{x}) = 0_{\mathbb{E}})$ and $\overline{x}$ is a root of f in $\mathbb{E}$. □

Definition 3.8.14. [**def:root**] *Let R be a commutative ring with identity.*

(a) [**a**] *A proper r in R is called* reducible *if $r = st$ for some proper elements s and t in R, that is if R is not irreducible.*

(b) [**b**] *Let $f \in R[x]$ and $a \in R$. Then a is a* root *of f if $f(a) = 0_R$.*

Lemma 3.8.15. [**factor theorem**] *Let $\mathbb{K}$ be a field, $a \in \mathbb{K}$ and $f \in \mathbb{K}[x]$.*

(a) [**a**] *There exists $q \in \mathbb{K}[x]$ with $f = q \cdot (x - a) + f(a)$.*

(b) [**c**] *If $g \in \mathbb{K}[x]$ divides f and a is a root of g, then a is a root of f.*

(c) [**b**] *$x - a$ divides f if and only if $f(a) = 0_{\mathbb{K}}$.*

(d) [**d**] *If* $\deg f = 1$*, f has a root in $\mathbb{K}$.*

Proof. (a) By the Division Algorithm 3.5.3 $f = q \cdot (x - a) + r$ for some $q, r \in \mathbb{K}[x]$ with $\deg t < \deg(x - a) = 1$. Thus $r \in \mathbb{K}$ and

$$f(a) = q(a)(a - a) + r(a) = q(a)0_{\mathbb{K}} + r = r$$

(b) Let $f = gh$ with $h \in \mathbb{K}[x]$. Then $f(a) = g(a)h(a) = 0_{\mathbb{K}}h(a) = 0_{\mathbb{K}}$.

(c) If $f(a) = 0_R$, then by (a), $f = q \cdot (x - a)$ for some $q \in \mathbb{K}[x]$. Thus $q \mid f$. If $x - a \mid f$ then by (b), a is a root of f.

(d) Let $f = bx + c$ with $b \in \mathbb{K}^\sharp, c \in \mathbb{K}$. Then $f = b(x - (-\frac{c}{b})$ and $-\frac{c}{b}$ is a root of f. □

Corollary 3.8.16. [**deg 3 irr**] *let $\mathbb{K}$ be a field and $f \in \mathbb{K}[x]$.*

(a) [**a**] *f is proper id and only if $f \notin \mathbb{K}$, that is* $\deg f \geq 1$*.*

(b) [**c**] *Suppose f is irreducible. Then f has a root in $\mathbb{F}$ if and only if* $\deg f = 1$*.*

(c) [**d**] *Suppose* $\deg f \in \{2, 3\}$*. Then f is irreducible if and only if f has no root in $\mathbb{K}$.*

Proof. (a) By 3.8.12(e), f is a unit if and only if $f \in \mathbb{K}^\sharp$. So f is 0_F or a unit if and only if $f \in \mathbb{K}$

(b) By 3.8.15(c), a is a root of f if and only if $f = (x - a)g$ for some $g \in \mathbb{K}[x]$.

If $\deg f = 1$, then f has a root. (3.8.15(d)).

If $f = (x - a)g$ then since f is irreducible, $x - a$ or g is a unit. $x - a$ is not and so g is a unit and $g \in \mathbb{K}$. Thus $\deg f = 1$.

(c) If f is irreducible then by (b), f has no root in $\mathbb{K}$. Suppose f is not irreducible. Then $f = gh$ with g and h proper. Since $\deg g + \deg h = \deg(gh) = \deg f \leq 3$ we get $\deg g = 1$ or $\deg h = 1$. Say $\deg g = 1$. Then by 3.8.15 g has a root and since g divides f, f has a root in $\mathbb{K}$. □

Example 3.8.17. [**ex:field from poly**]

(1) [**1**] Let $\mathbb{K}$ be a field and let $f = x^2 + rx + s$ be a polynomial of degree two which has no root on $\mathbb{K}$. Then by 3.8.16(c), f is irreducible and we can apply 3.8.13. In particular, $\mathbb{E} := \mathbb{K}[x]/(f\mathbb{K}[x]$ is a a field. For $g \in \mathbb{K}[x]$ put $\overline{g} = g + f\mathbb{K}[x]$. Then the map $\mathbb{K} \to \mathbb{E}, k \to \overline{k}$ is a 1-1 homomorphism and so we may identify k with $\overline{k}$. Put $t = \overline{x}$. If $e \in \mathbb{E}$ the $e = \overline{g}$ for some $g \in \mathbb{K}[x]$ with $\deg g < \deg f = 2$. So $g = a + bx$ for some $a, b \in \mathbb{K}$. Thus

$$e = \overline{a + bx} = \overline{a} + \overline{b}\overline{x} = a + bd$$

Thus

$$\mathbb{E} = \{a + bt \mid a, b \in \mathbb{K}$$

Moreover, for $a, b, c, d \in \mathbb{K}$.

$$a + bt = c + td \Longleftrightarrow a = c \text{ c=d}$$

The addition in $\mathbb{E}$ is easy:

$$(a + bt) + (c + dt) = (a + c) + (b + d)t$$

To determine the multiplicatio we compute

$$(a + bt) \cdot (c + dt) = ac + (bc + ad)t + bdt^2$$

t^2 must be of the form $u + vt$ for some $u, v \in \mathbb{K}$. Since $f \in f\mathbb{K}[x]$ we have $\overline{f} = 0_{\mathbb{K}}$ and so

$$0_K = \overline{x^2 + rx + s} = t^2 + rt + s$$

(So t is a root of f in $\mathbb{K}$).) Hence $t^2 = -rt - s$ and

$$(a+bt)\cdot(c+dt) = ac+(bc+ad)t+bdt^2 = ac+(bc+ad)t-bdrt-bds = (ac-sbd)+(bc+ad)-rbd$$

(2) [**2**] For a more concrete version of (1) consider the case $\mathbb{K} = \mathbb{R}$ and $f = x^2 + 1$. (So $r = 0$ and $s = 1$.) Since $a^2 + 1 > 0$ for all $a \in \mathbb{R}$, $x^2 + 1$ has no roots in $\mathbb{R}$. We have

$$\mathbb{E} = \{a+bt \mid a, b \in \mathbb{R}\}, (a+bt)+(c+dt) = (a+c)+(b+d)t \text{ and } (a+bt)(c+dt) = (ac-bd)+(ad = bc)T$$

Note also that $t^2 = -1$. The field $\mathbb{E}$ is called the field of *complex* numbers and denoted by $\mathbb{C}$.

(3) [**3**] Now consider $\mathbb{K} = \mathbb{Z}_2$. Are there any monic polynomials of degree 2 without a root?

f	$f(0)$	$f(1)$	roots
x^2	0	1	0
$x^2 + x$	0	0	$0, 1$
$x^2 + 1$	0	1	1
$x^2 + x + 1$	1	1	0

So there is only one choice for f namely $f = x^2 + x + 1$ and so $r = s = 1$. Hence

$$\mathbb{E} = \{0, 1, t, t+1\}, (a+bt)+(c+dt) = (a+c)+(b+d)t \text{ and } (a+bt)(c+dt) = (ac+bd)+(ad = bc+bd)$$

This gives the following addition and multiplication table:

$+$	0	1	t	$t+1$
0	0	1	t	$t+1$
1	1	0	$t+1$	t
t	t	$t+1$	0	1
$t+1$	$t+1$	t	1	0

$\cdot$	0	1	t	$t+1$
0	0	0	0	0
1	0	1	t	$t+1$
t	0	t	$t+1$	1
$t+1$	0	$t+1$	1	t

Chapter 4

Field Theory

4.1 Vector Spaces

Definition 4.1.1. [**def:vector space**] *Let $\mathbb{K}$ be a field. A* vector space *over $\mathbb{K}$ (or a $\mathbb{K}$-space) is a tuple $(V, +, \diamond)$ such that*

(i) [**i**] $(V, +)$ *is an abelian group.*

(ii) [**ii**] $\diamond : \mathbb{K} \times V \to V$ *is a function called* scalar multiplication .

(iii) [**iii**] $a \diamond (v + w) = (a \diamond v) + (a \diamond w)$ *for all* $a \in \mathbb{K}, v, w \in V$.

(iv) [**iv**] $(a + b) \diamond v = (a \diamond v) + (b \diamond v)$ *for all* $a, b \in \mathbb{K}, v \in V$.

(v) [**v**] $(ab) \diamond v = a \diamond (b \diamond v)$ *for all* $a, b \in \mathbb{K}, v \in V$.

(vi) [**vi**] $1_{\mathbb{K}} \diamond v = v$ *for all* $v \in V$

An element of a vector space is called a vector*. We usually just write kv for $k \diamond v$.*

Example 4.1.2. [**ex:vector space**] Let $\mathbb{K}$ be a field.

(1) [**2**] Let $n \in \mathbb{N}$. Then $\mathbb{K}^n$ is an $\mathbb{K}$-space via $k \diamond (a_1, \ldots, a_n) = (ka_1, \ldots, ka_n)$ for all $k, a_1, \ldots, a_n \in \mathbb{K}$.

(2) [**3**] The ring $\mathbb{K}[x]$ of polynomials with coefficients in $\mathbb{K}$ is a $\mathbb{K}$-space via

$$k \diamond (a_0 + a_1 x + \ldots a_n x^n) = (ka_0) + (ka_1)x + \ldots (ka_n x^n)$$

for all $k, a_0, \ldots, a_n \in \mathbb{K}$.

Definition 4.1.3. [**def:list**] *Let A be a set.*

(a) [**a**] *A* list *in A is a function $f : \{1, 2, 3, \dots, n\} \to A$, where $n \in \mathbb{N}$ and A is set. Put $a_i = f(i)$, $1 \leq i \leq n$. Then the list f will be denoted by*

$$(a - 1, a_2, \dots, a_n) \text{ or } (a_i)_{i=1}^n$$

In the case $n = 0$, f is called the empty list and is denoted by $()$.

(b) [**b**] *Let $\mathcal{A} = (a_i)_{i=1}^n$ and $\mathcal{B} = (b_j)_{j=1}^m$ be list in A. Then*

$$(\mathcal{A}, \mathcal{B})$$

denotes the list

$$(a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m)$$

(c) [**c**] *Let $\mathcal{A} = (a_i)_{i=1}^n$ and $\mathcal{B} = (b_j)_{j=1}^m$ be list in A. Then we say that $\mathcal{A}$ is* contained *in $\mathcal{A}$ or that $\mathcal{A}$ is a* sublist *of $\mathcal{B}$ if there exists $1 \leq j_1 < j_2 < \dots < j_n \leq m$ with*

$$a_1 = a_{j_1}, a_2 = b_{j_2}, \dots a_n = b_{j_n}$$

Definition 4.1.4. [**def:basis**] *Let $\mathbb{K}$ be a field and V and $\mathbb{K}$-space. Let $\mathcal{L} = (v_1, \dots, v_n) \in V^n$ be a list of vectors in V.*

(a) [**a**] *$\mathcal{L}$ is called* $\mathbb{K}$-linearly independent *if*

$$a_1 v_1 + a v_2 + \dots a v_n = 0_V$$

for some $a_1, a_2, \dots, a_n \in \mathbb{K}$ implies $a_1 = a_2 = \dots = a_n = 0_{\mathbb{K}}$.

(b) [**b**] *Let $(a_1, a_2 \dots, a_n) \in \mathbb{K}^n$. Then $a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ is called a* $\mathbb{K}$-linear combination *of $\mathcal{L}$.*

$$\operatorname{Span}_{\mathbb{K}}(\mathcal{L}) = \{a_1 v_1 + a_2 v_2 + \dots a_n v_n \mid (a_1, \dots, a_n) \in \mathbb{K}^n\}$$

is called the $\mathbb{K}$-span *of $\mathcal{L}$. So $\operatorname{Span}_{\mathbb{K}}(\mathcal{L})$ consists of all the $\mathbb{K}$-linear combination of $\mathcal{L}$. We consider 0_V to be a linear combination of the empty list $()$ and so $\operatorname{Span}_{\mathbb{K}}\big(()\big) = \{0_V\}$.*

(c) [**c**] *We say that $\mathcal{L}$* spans *V, if $V = \operatorname{Span}_{\mathbb{K}}(\mathcal{L})$, that is if every vector in V is a linear combination of $\mathcal{L}$.*

(d) [**d**] *We say that $\mathcal{L}$ is a* basis *of V if $\mathcal{L}$ is linearly independent and spans V.*

(e) [**e**] *We say that $\mathcal{L}$ is a* linearly dependent *if it is not linearly independent, that is, if there exist $k_1, \dots, k_n \in \mathbb{K}$, not all zero such that*

$$k_1 v_1 + k v_2 + \dots + k v_n = 0_V.$$

Example 4.1.5. [ex:basis]

(1) [**1**] *Put $e_i = (0_{\mathbb{K}}, \ldots, 0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, \ldots, 0_{\mathbb{K}}) \in \mathbb{K}^n$ where the $1_{\mathbb{K}}$ is in the i-position. Then $(e_1, e_2, \ldots, e_n)$ is a basis for $\mathbb{K}^n$, called the* standard basis *of $\mathbb{K}^n$.*

(2) [**4**] *$\mathbb{K}[x]$ has no $\mathbb{K}$-basis: Given a list $(f_1, f_2 \ldots, f_n)$ of polynomials over $\mathbb{K}$. Let $m_i = \deg f_i$ and $m = \max_{i=1}^n m_i$. Then each $\mathbb{K}$-=linear combination of $(f_1, \ldots, f_n)$ has degree at most m. So $(f_1, \ldots, f_n)$ does not span $\mathbb{K}[x]$ and $\mathbb{K}[x]$ has no $\mathbb{K}$-basis.*

(3) [**2**] *$(1_{\mathbb{K}}, x, x^2, \ldots x^n)$ is a basis for $\mathbb{K}_n[x]$, where $\mathbb{K}_n[x]$ is set of all polynomials with coefficients in $\mathbb{K}$ and degree at most n.*

(4) [**3**] *The empty list () is a basis for the $\mathbb{K}$-space $\{0_K\}$.*

Lemma 4.1.6. [**char basis**] *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and $\mathcal{L} = (v_1, \ldots, v_n)$ a list of vectors in V. Then $\mathcal{L}$ is a basis for V if and only if for each $v \in V$ there exist uniquely determined $k_1, \ldots, k_n \in \mathbb{K}$ with*

$$v = \sum_{i=1}^{m} k_i v_i.$$

Proof. $\Longrightarrow$ Suppose that $\mathcal{L}$ is a basis. Then $\mathcal{L}$ spans v and so for each $v \in V$ there exist $k_1, \ldots, k_n$ with

$$v = \sum_{i=1}^{m} k_i v_i.$$

Suppose that also $l_1, \ldots, l_n \in \mathbb{K}$ with

$$v = \sum_{i=1}^{m} l_i v_i.$$

Then

$$\sum_{i=1}^{m} (k_i - l_i) v_i = \sum_{i=1}^{m} k_i v_i - \sum_{i=1}^{m} l_i v_i = 0_V.$$

Since $\mathcal{L}$ is linearly independent we conclude that $k_i - l_i = 0_{\mathbb{K}}$ and so $k_i = l_i$ for all $1 \leq i \leq n$. So the k_i's are unique.

$\Longleftarrow$: Suppose each v in V is a unique linear combination of $\mathcal{L}$. Then clearly $\mathcal{L}$ spans V. Let $k_1, \ldots, k_n \in \mathbb{K}$ with

$$\sum_{i=1}^{m} k_i v_i = 0_V$$

Since also

$$\sum_{i=1}^{m} 0_{\mathbb{K}} v_i = 0_V$$

the uniqueness assumption gives $k_1 = k_2 = \ldots = k_n = 0_{\mathbb{K}}$. Hence $\mathcal{L}$ is linearly independent and thus a basis for V.

□

Lemma 4.1.7. [**not in span**] *Let $\mathbb{K}$ be field and V a $\mathbb{K}$-space. Let $\mathcal{L} = (v_1, \ldots, v_n)$ be a list of vectors in V. Suppose the exists $1 \leq i \leq n$ such that v_i is linear combination of $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$. Then $\mathcal{L}$ is linearly dependent.*

Proof. By assumption,

$$v_i = k_1 v_1 + \ldots + k_{i-1} v_{i-1} + k_{i+1} v_{i+1} + \ldots + k_n v_n$$

for some $k_j \in \mathbb{K}$. Thus

$$k_1 v_1 + \ldots + k_{i-1} v_{i-1} + (-1_{\mathbb{K}}) v_i + k_{i+1} v_{i+1} + \ldots + k_n v_n = 0_V$$

and $\mathcal{L}$ is linearly dependent. □

Lemma 4.1.8. [**min-max**] *Let $\mathbb{K}$ be field, V an $\mathbb{K}$-space and $\mathcal{L} = (v_1, v_2, \ldots v_n)$ a finite list of vectors in V. Then the following three statements are equivalent:*

(a) [**a**] *$\mathcal{L}$ is basis for V.*

(b) [**b**] *$\mathcal{L}$ is a minimal spanning list, that is $\mathcal{L}$ spans V but for all $1 \leq i \leq n$,*

$$(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$$

does not span V.

(c) [**c**] *$\mathcal{L}$ is maximal linearly independent list, that is $\mathcal{L}$ is linearly independent, but for all $v \in V$, $(v_1, v_2, \ldots, v_n, v)$ is linearly dependent.*

Proof. We will show that (a)$\iff$ (b) and (a) $\iff$ (c).

(a) $\implies$ (b): Since $\mathcal{L}$ is basis, it spans V. Since $\mathcal{L}$ is linearly independent 4.1.7 implies that v_i is not in the span of $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ and so $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ does not span V.

(b) $\implies$ (a): By assumption, $\mathcal{L}$ spans V so we only need to show that $\mathcal{L}$ is linearly independent. Suppose not. Then $\sum_{i=1}^n k_i v_i = 0_V$ for some $k_1, k_2, \ldots, k_n \in \mathbb{K}$, not all $0_{\mathbb{K}}$. Relabeling we may assume $k_1 \neq 0_{\mathbb{K}}$. Thus

$$v_1 = -k_1^{-1} \left(\sum_{i=2}^n k_i v_i \right).$$

Let $v \in V$. Then $v = \sum_{i=1}^n a_i v_i$ for some $a_i \in \mathbb{K}$ and so

$$v = a_1 \left(-k_1^{-1} \left(\sum_{i=2}^n k_i v_i \right) \right) + \sum_{i=2}^n a_i v_i = \sum_{i=2}^n (a_i - a_1 k_1^{-1} k_i) v_i.$$

Thus $(v_2, \ldots, v_n)$ spans V, contrary to the assumptions.

(a) $\implies$ (c): Let $v \in V$. Since $\mathcal{L}$ spans V, v is a linear combination of $\mathcal{L}$ and so by 4.1.7 $(v_1, v_2, \ldots, v_n, v)$ is linearly dependent.

(c) $\implies$ (a): By assumption $\mathcal{L}$ is linear independent, so we only need to show that $\mathcal{L}$ spans V. Let $v \in V$. By assumption $(v_1, \ldots, v_n, v)$ is linearly dependent and so

$$\left(\sum_{i=1}^{n} a_i v_i\right) + av = 0_V$$

for some $a_1, a_2, \ldots, a_n, a$ in $\mathbb{K}$ not all $0_{\mathbb{K}}$. If $a = 0_{\mathbb{K}}$, then since $\mathcal{L}$ is linearly independent, $a_i = 0_{\mathbb{K}}$ for all $1 \leq i \leq n$, contrary to the assumption. Thus $a \neq 0$ and

$$v = \sum_{i=1}^{n} (-a^{-1} a_i) v_i.$$

So $\mathcal{L}$ spans V. □

Definition 4.1.9. [**def:linear**] *Let $\mathbb{K}$ be a field and V and W $\mathbb{K}$-spaces. A* $\mathbb{K}$-linear map from V to W is function

$$f : V \to W$$

such that

(a) [**a**] $f(u + v) = f(u) + f(v)$ for all $u, v \in W$

(b) [**b**] $f(kv) = kf(v)$ for all $k \in \mathbb{K}$ and $v \in V$.

A $\mathbb{K}$-linear map is called a $\mathbb{K}$-*isomorphism* if it is 1-1 and onto.

We say that V and W are $\mathbb{K}$-isomorphic and write $V \cong_{\mathbb{K}} W$ if there exists a $\mathbb{K}$-isomorphism from V to W.

Example 4.1.10. [ex:linear]

(1) [**a**] The map $\mathbb{K}^2 \to \mathbb{K}, (a, b) \to a$ is $\mathbb{K}$-linear.

(2) [**b**] The map $\mathbb{K}^3 \to \mathbb{K}^2$, $(a, b, c) \to (a + 2b, b - c)$ is $\mathbb{K}$-linear.

(3) [**x**] Let V be a $\mathbb{K}$-space and $l \in \mathbb{K}$. Then the map $f : V \to V, v \to lv$ is $\mathbb{K}$-linear. Indeed, $f(u + v) = l(u + v) = lu + lv = f(u) + f(v)$ and

$$f(kv) = l(kv) = (lk)v = (kl)v = k(lv) = kf(v)$$

for all $u, v \in V, k \in \mathbb{K}$.

(4) [**c**] We claim that the map $f : \mathbb{K} \to \mathbb{K}, k \to k^2$ is $\mathbb{K}$-linear if and only if $\mathbb{K} = \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}$.

Indeed, if $\mathbb{K} = \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}$, then $k = k^2$ for all $k \in \mathbb{K}$ and so f is $\mathbb{K}$-linear.

Conversely, suppose f is $\mathbb{K}$-linear. Then for all $k \in \mathbb{K}$,

$$k^2 = f(k) = f(k \cdot 1_{\mathbb{K}}) = kf(1_{\mathbb{K}}) = k1_{\mathbb{K}}^2 = k$$

So $0_{\mathbb{K}} = k^2 - k = k(k - 1_{\mathbb{K}})$. Since $\mathbb{K}$ is a field and hence an integral domain we conclude that $k = 0_{\mathbb{K}}$ or $k = 1_{\mathbb{K}}$. Hence $\mathbb{K} = \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}$.

(5) [**y**] Let V and W be $\mathbb{K}$-spaces. Then the map $V \to W, v \to 0_W$ is $\mathbb{K}$-linear.

(6) [**e**] For $f = \sum_{i=0}^n f_i x^i \in \mathbb{K}[x]$ define

$$f' = \sum_{i=1}^n i f_i x^{i-1}.$$

Then

$$D : \mathbb{K}[x] \to \mathbb{K}[x], f \to f'$$

is a $\mathbb{K}$-linear map.

Lemma 4.1.11. [**invertible**] *Let $\mathbb{K}$ be a field and V and W be $\mathbb{K}$-spaces. Suppose that $(v_1, v_2, \ldots, v_n)$ is basis of V and let $w_1, w_2, \ldots w_n \in W$. Then*

(a) [**a**] *There exists a unique $\mathbb{K}$-linear map $f : V \to W$ with $f(v_i) = w_i$ for each $1 \leq i \leq n$.*

(b) [**b**] *$f(\sum_{i=1}^n k_i v_i) = \sum_{i=1}^n k_i w_i$, for all $k_1, \ldots, k_n \in \mathbb{K}$.*

(c) [**c**] *f is 1-1 if and only if $(w_1, w_2, \ldots, w_n)$ is linearly independent.*

(d) [**d**] *f is onto if and only if $(w_1, w_2, \ldots, w_n)$ spans W.*

(e) [**e**] *f is an isomorphism if and only if $(w_1, w_2, \ldots, w_n)$ is a basis for W.*

Proof. (a) and (b): If $f : V \to W$ is $\mathbb{K}$-linear with $f(v_i) = w_i$, then

$$f\left(\sum_{i=1}^n a_i v_i\right) = \sum_{i=1}^n a_i f(v_i) = \sum_{i=1}^n a_i w_i. \tag{1}$$

So (b) holds. Moreover, since $(v_1, \ldots v_n)$ spans V, each v in V is of the form $\sum_{i=1} a_i v_i$ and so by (1), $f(v)$ is uniquely determined. So f is unique.

It remains to show the existence of f. Since $(v_1, \ldots, v_n)$ is a basis for V, any $v \in V$ can by uniquely written as $v = \sum_{i=1} a_i v_i$. So we obtain a well-defined function

$$f : \quad V \to W, \quad \sum_{i=1}^n a_i v_i \to \sum_{i=1}^n a_i w_i.$$

It is now readily verified that f is $\mathbb{K}$-linear and $f(v_i) = w_i$. So f exists.

(c) From (b)

$$\ker f = \{v \in V \mid f(v) = 0_W\} = \left\{ \sum_{i=1}^n k_i v_i \,\middle|\, \sum_{i=1}^n k_i w_i = 0_W, k_1, k_2 \ldots, k_n \in \mathbb{K} \right\}. \tag{2}$$

Hence

$$\begin{array}{rcll} & f \text{ is 1-1} & & \\ \iff & \ker f = \{0_V\} & - & 2.6.3(f) \\ \iff & \{\sum_{i=1}^n k_i v_i \mid \sum_{i=1}^n k_i w_i = 0_W, k_1, k_2, \ldots, k_n \in \mathbb{K}\} = \{0_V\} & - & (2) \\ \iff & k_1 = \ldots = k_n = 0_{\mathbb{K}} \text{ for all } k_1, \ldots, k_n \in \mathbb{K} \text{ with } \sum_{i=1}^n k_i w_i = 0_W & - & (v_1, \ldots, v_n) \text{ is linearly indep.} \\ \iff & (w_1, \ldots, w_n) \text{ is linearly indep.} & - & \text{definition of linearly indep.} \end{array}$$

So (c) holds.
(d)

$$\operatorname{Im} f = \{f(v) \mid v \in V\} = \left\{ \sum_{i=1}^n a_i w_i \middle| a_1, \ldots a_n \in \mathbb{K} \right\} = \operatorname{Span}(w_1, w_2, \ldots, w_n).$$

f is onto if and only if $\operatorname{Im} f = W$ and so if and only if $(w_1, \ldots, w_n)$ spans W.
(e) follows from (c) and (d). □

Corollary 4.1.12. [**v iso kn**] *Let $\mathbb{K}$ be a field and W a $\mathbb{K}$-space with basis $(w_1, w_2 \ldots, w_n)$. Then the map*

$$f : \mathbb{K}^n \to W, (a_1, \ldots a_n) \to \sum_{i=1}^n a_i w_i$$

is a $\mathbb{K}$-isomorphism. In particular,

$$W \cong_{\mathbb{K}} \mathbb{K}^n.$$

Proof. By Example 4.1.5(1), $(e_1, e_2, \ldots, e_n)$ is basis for $\mathbb{K}^n$. Also $f(e_i) = w_i$ and so by 4.1.11(e), f is an isomorphism. □

Definition 4.1.13. [**def:subspace**] *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and $W \subseteq V$. Then W is called a* $\mathbb{K}$-subspace *of V provided that*

(i) [**i**] *$0_V \in W$.*

(ii) [**ii**] *$v + w \in W$ for all $v, w \in W$.*

(iii) [**iii**] *$kw \in W$ for all $k \in \mathbb{K}$, $w \in W$.*

Proposition 4.1.14 (Subspace Proposition)**.** [**subspaces prop**] *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and W an $\mathbb{K}$-subspace of V.*

(a) [**a**] *Let $v \in V$ and $k \in \mathbb{K}$. Then $0_{\mathbb{K}} v = v$, $(-1_{\mathbb{K}})v = -v$ and $k0_V = 0_V$.*

(b) [**b**] *W is a subgroup of V with respect to addition.*

(c) [**c**] *W together with the restriction of the addition and scalar multiplication to W is a well-defined $\mathbb{K}$-space.*

Proof. (a) I will just write 1 for $1_{\mathbb{K}}$ and 0 for $0_{\mathbb{K}}$. Then

$$0 \diamond v + 0_V = 0 \diamond v = (0+0) \diamond v = (0 \diamond v) + (0 \diamond v).$$

So by the Cancellation Law 2.2.1, $0 \diamond v = 0_V$.

Hence

$$0_V = 0 \diamond v = (1 + (-1)) \diamond v = (1 \diamond v) + (-1) \diamond v = v + (-1) \diamond v.$$

So $(-1) \diamond v = -v$.

$$0_V + k \diamond 0_V = k \diamond 0_V = k \diamond (0_V + 0_V) = k \diamond 0_V + k \diamond 0_V$$

and so by the Cancellation Law 2.2.1, $k \diamond 0_V = 0_V$.

(b) By definition of a $\mathbb{K}$-subspace, W is closed under addition and $0_V \in W$. Let $w \in W$. Since W is closed under scalar multiplication, $(-1) \diamond v \in W$. So by (a), $-v \in W$. Hence W is closed under additive inverses. So by the Subgroup Proposition 2.3.3, W is a subgroup of V with respect to addition.

(c) Using (b) this is readily verified and the details are left to the reader. □

Proposition 4.1.15 (Quotient Space Proposition)**.** [**quotient spaces**] *Let $\mathbb{K}$ be field, V a $\mathbb{K}$-space and W a $\mathbb{K}$-subspace of V.*

(a) [**a**] *$V/W := \{v + W \mid v \in V\}$ together with the addition*

$$+_{V/W} : \quad V/W \times V/W \to V/W, (u + V, v + W) \to (u + v) + W$$

and scalar multiplication

$$\diamond_{V/W} : \quad \mathbb{K} \times V/W \to V/W, (k, v + W) \to kv + W$$

is a well-defined vector space.

(b) [**b**] *The map $\phi : V \to V/W, v + W$ is an onto and $\mathbb{K}$-linear. Moreover, $\ker \phi = W$.*

Proof. (a) By Theorem 2.6.5 $(V/W, +_{V/W})$ is a well-defined group. We have

$$(u + W) + (v + W) = (u + v) + W = (v + u) + W = (v + W) + (v + W)$$

and so $(V/W, +_{V/W})$ is an abelian group. Thus Axiom (i) of a vector space holds.

Let $k \in V$ and $u, v \in V$ with $u + W = v + W$. Then $u - v \in W$ and since W is a subspace, $k(u-v) \in W$. Thus $ku - kv \in W$ and $ku + W = kv + W$. So $\diamond_{V/W}$ is well-defined and Axiom (ii) of a vector space holds. The remaining four axioms (iii)-(vi) are readily verified.

(b) By 2.6.5 ϕ is an homomorphism of abelian groups and $\ker\phi = W$. Let $k \in \mathbb{K}$ and $v \in V$. Then

$$\phi(kv) = kv + W = k(v + W),$$

and so ϕ is a $\mathbb{K}$-linear map. □

Lemma 4.1.16. [**span and quotient**] *Let $\mathbb{K}$ be field, V a $\mathbb{K}$-space, W a subspace of V. Suppose that $(w_1, \ldots, w_l)$ is a list of vector on W of W and $(v_1, \ldots, v_l)$ a list of vector in V. Suppose that $(w_1, w_2, \ldots, w_k, v_1, v_2, \ldots v_l)$ spans V. Then $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is spans V/W.*

Proof. Let $T \in V/W$. Then $T = v + W$ for some $v \in V$. $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is spans there exist $a_1, \ldots, a_k$, $b_1, \ldots b_k \in \mathbb{K}$ with

$$v = \sum_{i=1}^{k} a_i w_i + \sum_{j=1}^{l} b_j v_j.$$

Since $\sum_{i=1}^{k} a_i w_i \in W$ we conclude that

$$T = v + W = \left(\sum_{i=1}^{k} b_i v_i\right) + W = \sum_{i=1}^{k} b_i (v_i + W).$$

Therefore $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is a spanning list for V/W. □

Lemma 4.1.17. [**basis and quotients**] *Let $\mathbb{K}$ be field, V a $\mathbb{K}$-space, W a subspace of V. Suppose that $(w_1, \ldots, w_l)$ be a basis for W and let $(v_1, \ldots, v_l)$ be a list of vectors in V. Then the following are equivalent*

(a) [**a**] *$(w_1, w_2, \ldots, w_k, v_1, v_2, \ldots v_l)$ is a basis for V.*

(b) [**b**] *$(v_1 + W, v_2 + W, \ldots, v_l + W)$ is a basis for V/W.*

Proof. Put $\mathcal{B} = (w_1, w_2, \ldots, w_k, v_1, v_2, \ldots v_l)$.

(a) $\Longrightarrow$ (b): Suppose that $\mathcal{B}$ is a basis for V. Then $\mathcal{B}$ spans V and so by 4.1.17 $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is a spanning list for V/W.

Now suppose that $b_1, \ldots b_l \in \mathbb{K}$ with

$$\sum_{j=1}^{l} b_i (v_i + W) = 0_{V/W}.$$

Then $(\sum_{j=1}^{l} b_i v_i) + W = W$ and $\sum_{j=1}^{l} b_i v_i \in W$. Since $(w_1, w_2, \ldots, w_k)$ spans W there exist $a_1, a_2 \ldots, a_k \in \mathbb{K}$ with

$$\sum_{j=1}^{l} b_i v_i = \sum_{i=1}^{k} a_i w_i,$$

and so

$$\sum_{i=1}^{k}(-a_i)w_i + \sum_{j=1}^{l} b_j v_j = 0_V.$$

Since $\mathcal{B}$ is linearly independent, we conclude that $-a_1 = -a_2 = \ldots = -a_k = b_1 = b_2 = \ldots = b_l = 0_{\mathbb{K}}$. Thus $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is linearly independent and so a basis for V/W.

(b) $\implies$ (a): Suppose $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is a basis for W. Let $v \in V$. Then $v + W = \sum_{j=1}^{l} b_i(v_i + W)$ for some $b_1, \ldots b_l \in \mathbb{K}$. Thus

$$v - \sum_{i=1}^{l} b_i v_i \in W,$$

and so

$$v - \sum_{i=1}^{l} b_i v_i = \sum_{i=1}^{k} a_i w_i$$

for some $a_1, \ldots, a_k \in \mathbb{K}$. Thus

$$v = \sum_{i=1}^{k} a_i w_i + \sum_{j=1}^{l} b_j v_j,$$

and $\mathcal{B}$ is a spanning list.

Now let $a_1, \ldots, a_k$, $b_1, \ldots b_k \in \mathbb{K}$ with

$$(*) \qquad \sum_{i=1}^{k} a_i w_i + \sum_{j=1}^{l} b_j v_j = 0_V.$$

Since $\sum_{i=1}^{k} a_i w_i \in W$, this implies

$$\sum_{j=1}^{l} b_j(v_j + W) = 0_{V/W}.$$

Since $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is linearly independent, $b_1 = b_2 = \ldots = b_l = 0$. Thus by (*)

$$\sum_{i=1}^{k} a_i w_i = 0_V,$$

and since $(w_1, \ldots, w_k)$ is linearly independent, $a_1 = \ldots = a_k = 0_{\mathbb{K}}$.

Hence $\mathcal{B}$ is linearly independent and so a basis. □

Lemma 4.1.18. [**cluing basis**] *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space, Let $\mathcal{L}$ a linearly independent list of vectors in V and and $\mathcal{S}$ is spanning list of vectors in V. Put $W = \operatorname{Span}(\mathcal{L})$. Then there exists a sublist $\mathcal{T}$ of $\mathcal{S}$ such that*

(a) [**a**] *$(\mathcal{L}, \mathcal{T})$ is a basis for V.*

(b) [**b**] *$(v + W)_{v\in\mathcal{T}}$ is a basis for V/W.*

Proof. By 4.1.16 $(v + W)_{v\in\mathcal{S}}$ spans V/W. So we can choose a sublist $\mathcal{T}$ minimal such that $(v + W)_{v\in\mathcal{T}}$ spans V/W. Then by 4.1.6 $(v + W)_{v\in\mathcal{T}}$ is a basis for V/W. Note that $\mathcal{L}$ is a basis for W and so by 4.1.17, $(\mathcal{L}, \mathcal{T})$ is a basis for V. □

Lemma 4.1.19. [**dimension**] *Let $\mathbb{K}$ be field, V a $\mathbb{K}$-space and $(v_1, \ldots, v_n)$ and $(w_1, \ldots w_m)$ be bases for V. Then $n = m$.*

Proof. The proof is by induction on $\min(n, m)$. If $n = 0$ or $m = 0$, then $V = \{0_V\}$. So V contains no non-zero vectors and $n = m = 0$.

So we may assume that $1 \leq n \leq m$. Put $W = \operatorname{Span}(w_1)$. By 4.1.18 there exists a sublist say $(v_1, v_2 \ldots v_k)$ of $(v_1, \ldots, v_n)$ such that $(w_1, v_1, \ldots, v_k)$ is a basis for V and $(v_1 + W, \ldots, v_k + W)$ is a basis for V/W. By 4.1.8(b), $(w_1, v_1, \ldots, v_n)$ is linearly dependent. Thus $k < n$. So by induction any basis for V/W has size k. Since w_1 is a basis for W and $(w_1, \ldots, w_n)$ is a basis for V, 4.1.17 implies that $(w_2 + W, \ldots, w_m + W)$ is a basis for V/W. Thus $m - 1 = k$ and so $m = k + 1 \leq n \leq m$. So $m = k + 1 = n$. □

Definition 4.1.20. [**def:dimension**] *A vector space V over the field $\mathbb{K}$ is called* finite dimensional *if V has a finite basis $(v_1, \ldots, v_n)$. n is called the* dimension *of $\mathbb{K}$ and is denoted by $\dim_{\mathbb{K}} V$. (Note that this is well-defined by 4.1.19).*

Lemma 4.1.21. [**finite span**] *Let $\mathbb{K}$ be a field and V an $\mathbb{K}$-space with a finite spanning list $\mathcal{S} = (v_1, v_2, \ldots, v_n)$. Then some sublist of $\mathcal{S}$ is a basis for V. In particular, V is finite dimensional and $\dim_{\mathbb{K}} V \leq n$.*

Proof. By 4.1.18 applied with $\mathcal{L}$ the empty list, some sublist of $\mathcal{S}$ is a basis. □

Corollary 4.1.22. [**extent independent**] *Let V be a finite dimensional vector space over the field $\mathbb{K}$ and $\mathcal{L} = (w_1, \ldots, w_k)$ be linearly independent list of vectors in V. Then $\mathcal{L}$ is contained in a basis of V and so*

$$k \leq \dim_{\mathbb{K}} V.$$

Proof. By 4.1.18 applied with $\mathcal{S}$ a basis for V, $\mathcal{L}$ is contained in a basis for V. □

The next lemma is the analogue of Lagrange's Theorem for vector spaces:

Theorem 4.1.23 (Dimension Formula)**.** [**dim formula**] *Let V be a vector space over the field $\mathbb{K}$. Let W be an $\mathbb{K}$-subspace of V. Then V is finite dimensional if and only if both W and V/W are finite dimensional. Moreover, if this is the case, then*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W.$$

Proof. Suppose first that V and V/W are finite dimensional. Let $(w_1, w_2 \ldots w_k)$ be basis for W and $(v_1 + W, \ldots v_l + W)$ a basis for V/W.

Then by 4.1.17 $(w_1, \ldots, w_l, v_1, \ldots, v_l)$ is basis for V.V Thus V is finite dimensional and

$$\dim_{\mathbb{K}} V = k + l = \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W.$$

Suppose next that V is finite dimensional. Let $\mathcal{L} = (w_1, \ldots, w_k)$ be a linear independent sublist of W. By 4.1.22 $k \leq \dim_{\mathbb{K}} V$. So we can choose $\mathcal{L}$ with k maximal. Then $\mathcal{L}$ is a maximal linearly independent list of vectors in W and so by 4.1.6, $\mathcal{L}$ is a basis of V. Thus W is finite dimensional. By 4.1.18 applied with $\mathcal{S}$ a basis for V, V/W is finite dimensional. □

Remark 4.1.24. [rm:iso and rank]

(a) [**1**] We will work out the connected between the Dimension Formula and Lagrange's Theorem. Let $\mathbb{K}$ be a field, V a finite dimensional $\mathbb{K}$ space, W a $\mathbb{K}$-subspace of V, $n = \dim_{\mathbb{K}} V, k = \dim_{\mathbb{K}} W$ and $l = \dim_{\mathbb{K}} V$. Then the dimension formula says that

$$n = k + l$$

By Theorem D on Homework 2, $V \cong_{\mathbb{K}} \mathbb{K}^n$ and so $|V| = |\mathbb{K}^n| = |\mathbb{K}|^n$, $|W||\mathbb{K}|^k$ and $|V/W| = |\mathbb{K}|^l$. Thus

$$|V| = |\mathbb{K}|^n = |\mathbb{K}|^{k+l} = |\mathbb{K}|^k \cdot |\mathbb{K}|^l = |W| \cdot |V/W|$$

So the Dimension formula implies Lagrange's Theorem (for vector spaces). If $|\mathbb{K}|$ is finite, the converse is true. But if $|\mathbb{K}|$ is infinite, $|\mathbb{K}|^n = |\mathbb{K}|$ for all $n \in \mathbb{Z}^+$, so $|\mathbb{K}|^n = |\mathbb{K}|^{k+l}$ does not imply $k = l$.

(b) [**2**] For those of you familiar with matrices you might have seen the Rank Theorem (see for example [Lay, Theorem 14, Chapter 4]):

$$\text{rank} A + \dim \operatorname{Nul} A = n$$

where A is an $m \times n$ matrix, rank$A$ is dimension of the column space $\operatorname{Col} A$ of A and $\operatorname{Nul} A = \{v \in \mathbb{K}^m \mid Av = \vec{0}\}$.

This formula essentially is equivalent to the the First Isomorphism Theorem for vector spaces (see Homework 3#2). Indeed let f be the $\mathbb{K}$-linear map $\mathbb{K}^n \to \mathbb{K}^m, v \to Av$. Then

$$\operatorname{Nul} A = \ker f \text{ and } \operatorname{Col} A = \operatorname{Im} f$$

The First Isomorphism Theorem for vector spaces says:

$$\mathbb{K}^n/\ker f \cong_{\mathbb{K}} \operatorname{Im} f.$$

By Theorem D on Homework 2, this is equivalent to

$$\dim_{\mathbb{K}}(\mathbb{K}^n/\ker f) = \dim_{\mathbb{K}} \operatorname{Im} f,$$

and so by the dimension formula to

$$\dim \mathbb{K}^n - \dim \ker f = \dim_K \operatorname{Im} f,$$

that is to

$$n - \dim \operatorname{Nul} A = \operatorname{rank} A$$

4.2 Field Extensions

Definition 4.2.1. [**def:subfield**] *Let $\mathbb{F}$ be a field and $\mathbb{K}$ a subset of $\mathbb{F}$. $\mathbb{K}$ is a called a* subfield *of $\mathbb{F}$ provided that*

(i) [**i**] $a + b \in \mathbb{K}$ *for all* $a, b \in \mathbb{K}$.

(ii) [**ii**] $0_{\mathbb{F}} \in \mathbb{K}$.

(iii) [**iii**] $-a \in \mathbb{K}$ *for all* $a \in \mathbb{K}$.

(iv) [**iv**] $ab \in \mathbb{K}$ *for all* $a, b \in \mathbb{K}$.

(v) [**v**] $1_{\mathbb{F}} \in \mathbb{K}$.

(vi) [**vi**] $a^{-1} \in \mathbb{K}$ *for all* $a \in \mathbb{K}$ *with* $a \neq 0_{\mathbb{F}}$.

If $\mathbb{K}$ is a subfield of $\mathbb{F}$ we also say that $\mathbb{F}$ is an extension field *of $\mathbb{K}$ and that $\mathbb{K} \leq \mathbb{F}$ is a field extension.*

Note that (i), (ii) and (iii) just say that $\mathbb{K}$ is subgroup of $\mathbb{F}$ with respect to addition and (iv),(v),(vi) say that $\mathbb{K} \setminus \{0_{\mathbb{F}}\}$ is a subgroup of $\mathbb{F} \setminus \{0_{\mathbb{F}}\}$ with respect to multiplication. Note also a subfield of $\mathbb{F}$ is a field.

Example 4.2.2. [**ex:extension**]

(a) [**1**] $\mathbb{Q} \leq \mathbb{R}$ and $\mathbb{R} \leq \mathbb{C}$ are field extensions.

(b) [**2**] Let $\mathbb{F}$ be a field. By 3.8.12 $\mathbb{F}[x]$ is an integral domain. We denote the field of fraction of $\mathbb{F}[x]$ by $\mathbb{F}(x)$. So

$$\mathbb{F}(x) = \left\{ \frac{f}{g} \middle| f, g \in \mathbb{F}[x], g \neq 0_{\mathbb{F}} \right\}$$

and $\mathbb{F} \leq \mathbb{F}(x)$ is a field extension.

Lemma 4.2.3. [**extension are spaces**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension. Then $\mathbb{F}$ is vector space over $\mathbb{K}$, where the scalar multiplication is given by*

$$\mathbb{K} \times \mathbb{F} \to \mathbb{F}, (f, k) \to fk$$

Proof. Using the axioms of a field it is easy to verify the axioms of a vector space. □

Definition 4.2.4. [**finite extensions**] *A field extension $\mathbb{K} \leq \mathbb{F}$ is called* finite *if $\mathbb{F}$ is a finite dimensional $\mathbb{K}$-space.* $\dim_{\mathbb{K}} \mathbb{F}$ *is called the* degree *of the extension $\mathbb{K} \leq \mathbb{F}$*

Example 4.2.5. [**ex:finite**]

(1) [**1**] $(1, i)$ is an $\mathbb{R}$-basis for $\mathbb{C}$ and so $\mathbb{R} \leq \mathbb{C}$ is a finite field extension of degree 2.

(2) [**2**] Let $\mathbb{K}$ be a field. Then $\mathbb{K} \leq \mathbb{K}(x)$ is not finite. Indeed by 4.1.5(2) $\mathbb{K}[x]$ is not finite dimensional over $\mathbb{K}$ and so by 4.1.23 also $\mathbb{F}(x)$ is not finite dimensional over $\mathbb{K}$.

Lemma 4.2.6. [**dim formula for extensions**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and V a $\mathbb{F}$-space. Then with respect to the restriction of the scalar multiplication to $\mathbb{K}$, V is an $\mathbb{K}$-space. If V is finite dimensional over $\mathbb{F}$ and $\mathbb{K} \leq \mathbb{F}$ is finite, then V is finite dimensional over $\mathbb{K}$ and*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} \mathbb{F} \cdot \dim_{\mathbb{F}} V.$$

Proof. It is readily verified that V is indeed on $\mathbb{K}$-space. Suppose now that V is finite dimensional over $\mathbb{F}$ and that $\mathbb{K} \leq \mathbb{F}$ is finite. Then there exist a $\mathbb{F}$-basis $(v_1, \dots, v_n)$ for V and an $\mathbb{K}$-basis $(k_1, \dots, k_m)$ for $\mathbb{F}$. We will show that

$$\mathcal{B} := (k_i v_j \mid 1 \leq i \leq m, 1 \leq j \leq n)$$

is an $\mathbb{K}$-basis for V.

To show that $\mathcal{B}$ spans V over $\mathbb{K}$, let $v \in V$. Then since $(v_1, \dots, v_n)$ spans V over $\mathbb{F}$ there exists $l_1, \dots, l_n \in \mathbb{F}$ with

$$v = \sum_{j=1}^{n} l_j v_j. \tag{1}$$

Let $1 \leq j \leq n$. Since $(k_1, \dots, k_m)$ spans $\mathbb{F}$ over $\mathbb{K}$ there exists $a_{1j}, \dots a_{mj} \in \mathbb{K}$ with

$$l_i = \sum_{i=1}^{m} a_{ij} k_i. \tag{2}$$

Substituting (2) into (1) gives

$$v = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} k_i \right) v_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} k_i v_j .$$

Thus $\mathcal{B}$ spans V.

To show that $\mathcal{B}$ is linearly independent over $\mathbb{K}$, let $a_{ij} \in \mathbb{K}$ for $1 \leq i \leq m$ and $i \leq j \leq n$ with

$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} k_i v_j = 0_V .$$

Then also

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} k_i \right) v_j = 0_V .$$

Since $\sum_{i=1}^{m} a_{ij} k_i \in \mathbb{F}$ and $(v_1, \ldots, v_n)$ is linearly independent over $\mathbb{F}$ we conclude that for all $1 \leq j \leq n$:

$$\sum_{i=1}^{m} a_{ij} k_i = 0_{\mathbb{F}} .$$

Since $(k_1, k_2, \ldots, k_m)$ is linearly independent over $\mathbb{K}$ this implies $a_{ij} = 0_{\mathbb{K}}$ for all $1 \leq i \leq m$ and all $1 \leq j \leq m$. Thus $\mathcal{B}$ is a basis for V over $\mathbb{K}$, V is finite dimensional over $\mathbb{K}$ and

$$\dim_{\mathbb{K}} V = mn = \dim_{\mathbb{K}} \mathbb{F} \cdot \dim_{\mathbb{F}} V.$$

□

Here is a second proof for the preceding lemma: By Lemma D on Homework 3, $V \cong_{\mathbb{F}} \mathbb{F}^n$ and $\mathbb{F} \cong_{\mathbb{K}} \mathbb{K}^m$. Hence $V \cong_{\mathbb{K}} (\mathbb{K}^m)^n \cong_{\mathbb{K}} \mathbb{K}^{mn}$. Thus $\dim_{\mathbb{K}} V = mn$.

Example 4.2.7. [**ex:dim formula extensions**] Since $(1,0)$ and $(0,1)$ is a $\mathbb{C}$-basis for $\mathbb{C}^2$ and $(1,i)$ is a $\mathbb{R}$ basis for $\mathbb{C}$. So $\big((1,0),(i,0),(0,1),(0,i)\big)$ is an $\mathbb{R}$-basis for $\mathbb{C}$. This can also be directly verified: Let $a,b,c,d \in \mathbb{R}$. Then

$$(a+bi, c+di) = a(1,0) + b(i,0) + c(0,1) + d(0,i)$$

So we see that there exists exactly one way to write $(a+bu, c+di)$ has a linear combination of $\big((1,0),(i,0),(0,1),(0,i)\big)$

Corollary 4.2.8. [**finite by finite**] *Let $\mathbb{K} \leq \mathbb{F}$ and $\mathbb{F} \leq \mathbb{E}$ be finite field extensions. Then also $\mathbb{K} \leq \mathbb{E}$ is a finite field extension and*

$$\dim_{\mathbb{K}} \mathbb{E} = \dim_{\mathbb{K}} \mathbb{F} \cdot \dim_{\mathbb{F}} \mathbb{E}.$$

Proof. By 4.2.3 $\mathbb{E}$ is a $\mathbb{F}$-space. So the Corollary follows from 4.2.6 applied with $V = \mathbb{E}$. □

Lemma 4.2.9. [**associate poly**] *Let $\mathbb{K}$ be a field and $f \in \mathbb{K}[x]^\sharp$. Then there exists unique monic polynomial $g \in \mathbb{K}[x]$ with $f \sim g$.*

Proof. Let l be the leading coefficient of f and put $g = l^{-1}f$. Then g is monic and $g \sim f$. Let h also be a monic polynomial with $f \sim h$. Then $g \sim h$ and so $g = kh$ for $k \in \mathbb{K}[x]$. By 3.6.4 k is a unit in $\mathbb{K}[x]$ and then by 3.8.12(e), $k \in \mathbb{K}$. Since both g and h are monic $k = 1_\mathbb{K}$ and $g = h$. □

Lemma 4.2.10. [**fx principal**] *Let $\mathbb{K}$ be a field and I a non-zero ideal in $\mathbb{K}[x]$.*

(a) [**a**] *There exists a unique monic polynomial $p \in \mathbb{K}[x]$ with $I = \mathbb{K}[x]p$.*

(b) [**b**] *$\mathbb{K}[x]/I$ is an integral domain if and only if p is irreducible and if and only if $\mathbb{K}[x]/I$ is field.*

Proof. (a) By 3.8.13(a), $\mathbb{K}[x]$ is a PID. Hence $I = \mathbb{K}[x]f$ for some polynomial $f \in \mathbb{K}[x]$. By 4.2.9 $f \sim p$ for unique polynomial $g \in \mathbb{K}[x]$. By 3.6.2(c) $f \sim p$ if and only if $I = \mathbb{K}[x]p$. So (a) holds.

(b) This follows from (a) and 3.8.13(b) □

Definition 4.2.11. [**def:fa**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $a \in \mathbb{F}$. If there exists a non-zero $f \in \mathbb{K}[x]$ with $f(a) = 0_\mathbb{K}$ then a is called* algebraic *over $\mathbb{K}$. Otherwise a is called transcendental over $\mathbb{K}$.*

Example 4.2.12. [**ex:algebraic**]

(1) [**1**] $\sqrt{2}$ is the a root of $x^2 - 2$ and so $\sqrt{2}$ is algebraic over $\mathbb{Q}$.

(2) [**2**] i is a root of $x^2 + 1$ so i is algebraic over $\mathbb{Q}$.

(3) [**3**] π is not the root of any non-zero polynomial with rational coefficients. So π is transcendental. The proof of this fact is highly non-trivial and beyond the scope of this lecture notes. For a proof see Appendix 1 in [Lan].

(4) [**4**] Let y be an indeterminate over $\mathbb{K}$ and $\mathbb{K}(y)$ the field of fraction of the polynomial ring $\mathbb{K}[y]$. The y is transcendental over $\mathbb{K}$. Indeed $f = \sum_{i=0}^n k_i x^i \in \mathbb{K}[x]^\sharp$. Then $k_i \neq 0_\mathbb{K}$ for some i and so also $f(y) = \sum_{i=0}^n k_i y^i \neq 0_\mathbb{K}$.

Although complex numbers which are transcendental over $\mathbb{Q}$ are hard to come by, there are many more transcendental number then algebraic numbers. To see we will have short look at the cardinality of sets.

4.2.13 (Cardinalities)**.** [**cardinality**] Let A and B be sets. We say that A and B have the same *cardinality* and write $|A| = |B|$ if there exists a bijection $:A \to B$. We write $|A| \geq |B|$ if either $B = \emptyset$ or there exists an onto map $f : A \to B$. We write $|A| \leq |B|$ if there exists a 1-1 map from A to B. It is easy to see that $|A| \geq |B|$ if and only if $|B| \leq |A|$. Indeed suppose $f : A \to B$ is onto. For each $b \in B$ pick $\tilde{b} \in A$ with $f(\tilde{b}) = b$. Define

$g : B \to A, b \to \tilde{B}$. If $\tilde{b} = \tilde{d}$, then $b = f(\tilde{b}) = f(\tilde{d}) = d$ and so g is 1-1. Suppose now that $g : B \to A$ is 1-1 and $B \neq \emptyset$. Pick $b_0 \in B$ and let $a \in A$. If $a = g(b)$ for some $b \in B$, define $\tilde{a} = b$. Note that $\tilde{a}$ is well defined since f is 1-1. If $a \notin g(B)$ define $\tilde{a} = b_0$. Then the map $f : A \to B, a \to \tilde{a}$ is onto, since $f(g(b)) = b$ for all $b \in B$.

A more difficult fact is that $|A| \leq |B|$ and $|B| \leq |A|$ implies $|A| = |B|$. This fact is called the Theorem of Schröder Bernstein. For a proof see for example [Hun, Theorem 0.8.6].

We write $|A| < |B|$ if $|A| \leq |B|$ but $|A| \neq |B|$.

We will know compare the cardinality of various infinite sets:

$|\mathbb{N}| = |\mathbb{Z}^+|$, since $\mathbb{N} \to \mathbb{Z}^+, n \to n+1$ is a bijection.

$|\mathbb{N}| = |\mathbb{Z}|$ since $\mathbb{Z} \to \mathbb{N}, n \to \begin{cases} 2n & \text{if } n \geq 0 \\ 2|n| - 1 & \text{if } n < 0 \end{cases}$ is a bijection.

We will now show that $|\mathbb{Z}^+| < |\mathbb{R}|$. Since $|\mathbb{Z}^+| \subseteq \mathbb{R}$, $|Q| \leq \mathbb{R}|$. Suppose that $|\mathbb{Z}^+| = |\mathbb{R}|$. Then $|\mathbb{Z}^+| \geq |[0,1)|$ where $[0,1) = \{r \in \mathbb{R}, 0 \leq r < 1)$. Thus there function an onto function $f : \mathbb{Z}_+ \to [0,1)$.

We have

$$\begin{array}{rcl} f(1) & = & 0.a_{11}a_{12}a_{13}a_{14}\ldots \\ f(2) & = & 0.a_{21}a_{22}a_{23}a_{24}\ldots \\ f(3) & = & 0.a_{31}a_{32}a_{33}a_{34}\ldots \\ \vdots & \vdots & \vdots \\ f(n) & = & 0.a_{n1}a_{n2}a_{n3}a_{n4}\ldots \\ \vdots & \vdots & \vdots \end{array}$$

where $a_{ij} \in \mathbb{N}$ with $0 \leq a_{ij} < 9$. Define $s = 0.s_1s_2s_3s_4\ldots \in [0,1)$ by $s_i = 5$ if $a_{ii} \neq 5$ and $s_i = 0$ if $a_{ii} = 5$. Then $s_i \neq a_{ii}$ for all $i \in \mathbb{Z}^+$. It follows that $s \neq f(i)$ for all $i \in \mathbb{Z}^+$, a contradiction to the assumption that f is onto.

Proposition 4.2.14. [**phia hom**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $a \in \mathbb{F}$.*

(a) [**a**] *The map $\phi_a : \mathbb{K}[x] \to \mathbb{F}, f \to f(a)$ is a ring homomorphism.*

(b) [**b**] $\operatorname{Im}\phi_a = \mathbb{K}[a]$ *and so* $\mathbb{K}[a] = \{f(a) \mid f \in \mathbb{K}[x]\}$.

(c) [**c**] ϕ_a *is 1-1 if and only if* $\ker\phi_a = \{0_{\mathbb{K}}\}$ *and if and only if a is transcendental.*

Proof. (a) See 3.4.2(a).

(b) By 3.3.5(a), $\operatorname{Im}\phi_a$ is a subring of $\mathbb{F}$. Since $\phi_a(k) = k$ and $\phi_a(x) = a$ for all $k \in \mathbb{K}$, $\mathbb{K} \cup a \subseteq \mathbb{K}[a]$ and so $\mathbb{K}[a] \subseteq \operatorname{Im}\phi_a$ be definition of $\mathbb{K}[a]$. Let $f = \sum_{i=0}^{i} k_i x \in \mathbb{K}[x]$. Then

$$\phi_a(f) = f(a) = \sum_{i=0}^{n} k_i a^i \in \mathbb{K}[a]$$

and so $\operatorname{Im}\phi_a \subseteq \mathbb{K}[a]$ and (b) holds,

(c) By 2.6.3(f) ϕ_a is 1-1 if and only if $\ker\phi_a = \{0_{\mathbb{K}}\}$. Now

$$\ker\phi_a = \{f \in \mathbb{K}[x] \mid \phi_a(f) = 0_{\mathbb{F}}\} = \{f \in \mathbb{K}[x] \mid f(a) = 0_{\mathbb{F}}\},$$

and so $\ker\phi_a = \{0_{\mathbb{K}}\}$ if and only if there does not exist a non-zero polynomial f with $f(a) = 0_{\mathbb{F}}$, that is if and only if a is transcendental. □

Proposition 4.2.15. [**transcendental**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $a \in \mathbb{F}$. Suppose that a is transcendental over $\mathbb{K}$. Then*

(a) [**a**] $\tilde{\phi}_a : \mathbb{K}[x] \to \mathbb{K}[a], f \to f(a)$ *is an isomorphism of rings.*

(b) [**b**] *For all $n \in \mathbb{N}$, $(1, a, a^2, \dots, a^n)$ is linearly independent over $\mathbb{K}$.*

(c) [**c**] $\mathbb{K}[a]$ *is not finite dimensional over $\mathbb{K}$ and $\mathbb{K} \leq \mathbb{F}$ is not finite.*

(d) [**d**] $a^{-1} \notin \mathbb{K}[a]$ *and $\mathbb{K}[a]$ is not a subfield of $\mathbb{F}$.*

Proof. (a) By 4.2.14(c), $\tilde{\phi}_a$ is 1-1 and by 4.2.14(b), $\tilde{\phi}_a$ is well-defined and onto.

(b) Let $b_0, b_1, \dots, b_n \in \mathbb{K}$ with $\sum_{i=0}^n b_i a^i = 0_{\mathbb{K}}$. Then $f(a) = 0_{\mathbb{K}}$ where $f = \sum_{i=0}^n b_i x^i$. Since a is transcendental $f = 0_{\mathbb{K}}$ and so $b_0 = b_1 = \ldots = b_n = 0_{\mathbb{K}}$. Thus $(1_{\mathbb{K}}, a, \dots, a^n)$ is linearly independent over $\mathbb{K}$.

(c) Suppose $\mathbb{K}[a]$ is finite dimensional over $\mathbb{K}$ and put $n = \dim_{\mathbb{K}}\mathbb{K}[a]$. Then by (b) $(1, a, a^2, \dots, a^n)$ is linearly independent over $\mathbb{K}$. This list has length $n+1$ and so by 4.1.22

$$n + 1 \leq \dim_F \mathbb{K}[a] = n,$$

a contradiction.

So $\mathbb{K}[a]$ is not finite dimensional over $\mathbb{K}$. Suppose $\mathbb{K} \leq \mathbb{F}$ is finite, then by 4.1.23 also $\mathbb{K}[a]$ is finite dimensional over $\mathbb{K}$, a contradiction.

(d) Suppose $a^{-1} \in \mathbb{K}[x]$. Then $a^{-1} = f(a)$ for some $f \in \mathbb{K}[x]$. Thus $af(a) - 1_{\mathbb{K}} = 0_{\mathbb{F}}$ and so a is root of the non-zero polynomial $xf - 1_{\mathbb{K}}$. But then a is algebraic, a contradiction. □

Theorem 4.2.16. [**algebraic**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $a \in \mathbb{F}$. Suppose that a is algebraic over $\mathbb{K}$. Then*

(a) [**z**] *There exists a unique monic polynomial $m_a = m_a^{\mathbb{K}} \in \mathbb{K}[x]$ with $\ker\phi_a = m_a\mathbb{K}[x]$.*

(b) [**a**] $\overline{\phi}_a : \quad \mathbb{K}[x]/(m_a) \to \mathbb{K}[a], \quad f + m_a\mathbb{K}[x] \to f(a)$ *is a well-defined isomorphism of rings.*

(c) [**b**] m_a *is irreducible.*

(d) [**c**] $\mathbb{K}[a]$ *is a subfield of $\mathbb{F}$.*

(e) [**d**] *Put $n = \deg m_a$. Then $(1, a, \dots, a^{n-1})$ is an $\mathbb{K}$-basis for $\mathbb{K}[a]$*

(f) [**e**] $\dim_{\mathbb{K}} \mathbb{K}[a] = \deg m_a$.

(g) [**f**] *Let* $g \in \mathbb{K}[x]$. *Then* $g(a) = 0_{\mathbb{F}}$ *if and only if* $m_a \mid g$ *in* $\mathbb{K}[x]$.

(h) [**g**] m_a *is the unique monic irreducible polynomial in* $\mathbb{K}[x]$ *with* a *as a root.*

Proof. (a) By 4.2.14(c), $\ker \phi_a \neq \{0_{\mathbb{K}}\}$. By 4.2.14(a) is a ring homomorphism and so 3.3.5(c) $\ker \phi_a$ is an ideal in $\mathbb{K}[x]$. Thus by 4.2.10, $\ker \phi_a = m_a\mathbb{K}[x]$ for a unique monic polynomial $m_a \in \mathbb{K}[x]$.

(b): By definition of m_a, $\ker \phi_a = m_a\mathbb{K}[x]$. By 4.2.14(a) ϕ_a is a ring homomorphism and so (b) follows from the Isomorphism Theorem of Rings 3.3.10.

(c) and (d): Since $\mathbb{F}$ is an integral domain, $\mathbb{K}[a]$ is an integral domain. So by (b), $\mathbb{K}[x]/(m_a)$ is an integral domain. Hence by 4.2.10(b), m_a is irreducible and $\mathbb{K}[x]/(m_a)$ is a field. By (b) also $\mathbb{K}[a]$ is a field. So (c) and (d) hold.

(d) Let $T \in \mathbb{K}[x]/m_a\mathbb{K}[x]$. Hence by 3.8.13(d) there exists unique polynomial $f \in \mathbb{K}[x]$ of degree less than n with $T = \overline{f}$, where $\overline{f} = f + m_a\mathbb{K}[x]$. Let $f = \sum_{i=0}^{n-1} k_i x^i$ with $k_i \in \mathbb{K}$. Then the k_i are unique in $\mathbb{K}$ with

$$T = \overline{\sum_{i=0}^{n-1} k_i x^i} = \sum_{i=0}^{n-1} k_i \overline{x^i}$$

Thus by 4.1.6

$$1, \overline{x}, \overline{x^2}, \ldots, \overline{x^i}$$

is a basis for $\mathbb{K}[x]/m_a\mathbb{K}[x]$. Since $\overline{\phi}_a(\overline{x^i}) = a^i$ and since $\overline{\phi}_a$ is an isomorphism we conclude from 4.1.11(e) that

$$(1, a, a^2, \ldots, a^{n-1})$$

is a basis for $\mathbb{K}[a]$.

(f) Follows from (e).

(g) $g(a) = 0_{\mathbb{F}}$ if and only if $\phi_a(a) = 0_{\mathbb{F}}$ if and only if $g \in \ker \phi_a$ if and only if $g \in m_a\mathbb{K}[x]$ and if and only if $m_a \mid g$ in $\mathbb{K}[x]$.

(h) By (c), m_a is irreducible. Also m_a is monic and has a as a root. Let $f \in \mathbb{K}[x]$ be monic and irreducible with $f(a) = 0_{\mathbb{K}}$. Then by (h), $m_a \mid f$. Since f is irreducible and m_a is not a unit, $m_a \sim f$. Thus by 4.2.9 $m_a = f$. □

Definition 4.2.17. [**def:minimal polynomial**] *Let* $\mathbb{K} \leq \mathbb{F}$ *be a field extension and let* $a \in \mathbb{K}$ *be algebraic over* $\mathbb{K}$. *The unique monic polynomial* $m_a \in \mathbb{K}[x]$ *with* $\ker \phi_a = (m_a)$ *is called the* minimal polynomial *of* a *over* $\mathbb{K}$.

Example 4.2.18. [**ex: minimal polynomial**]

(1) [**a**] It is easy to see that x^3-5 has no root on $\mathbb{Q}$. Thus x^3-2 is irreducible in $\mathbb{Q}[x]$ (see 3.8.16(c)). So 4.2.16(h) implies that x^3-5 is the minimal polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$. Hence by 4.2.16(e)

$$\left(1, \sqrt[3]{5}, (\sqrt[3]{5})^2\right) = \left(1, \sqrt[3]{2}), \sqrt[3]{25}\right)$$

is a basis for $\mathbb{Q}[\sqrt[3]{5}]$. Thus

$$\mathbb{Q}[\sqrt[3]{5}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{25} \mid a, b, c \in \mathbb{Q}\}.$$

(2) [**b**] Let $\xi = e^{\frac{2\pi}{3}i} = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3}) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Then $\xi^3 = 1$ and ξ is a root of x^3-1. x^3-1 is not irreducible, since $(x^3-1) = (x-1)(x^2+x+1)$. So ξ is a root of x^2+x+1. x^2+x+1 does not have a root in $\mathbb{Q}$ and so is irreducible in $\mathbb{Q}[x]$. Hence the minimal polynomial of ξ is x^2+x+1. Thus

$$\mathbb{Q}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Q}\}.$$

Lemma 4.2.19. [**iso transitive**]

(a) [**a**] *Let $\alpha : R \to S$ and $\beta : S \to T$ be ring isomorphisms. Then*

$$\beta \circ \alpha : R \to T, r \to \beta(\alpha(r))$$

and

$$\alpha^{-1} : S \to R, s \to \alpha^{-1}(s)$$

are ring isomorphism.

(b) [**b**] *Let R and S be rings, I an ideal in R and $\alpha : R \to S$ a ring isomorphism. Put $J = \alpha(I)$. Then*

(a) [**a**] *J is an ideal in S.*

(b) [**b**] *$\beta : I \to J, \quad i \to \alpha(i)$ is a ring isomorphism.*

(c) [**c**] *$\gamma : R/I \to S/J, \quad r + I \to \alpha(i) + J$ is a well-defined ring isomorphism.*

(d) [**d**] *$\alpha\big(aR\big) = \big(\alpha(a)S$ for all $a \in R$.*

(c) [**c**] *let $\sigma : R \to S$ a ring isomorphism. Then*

$$\tilde{\sigma} : R[x] \to S[x], \quad \sum_{i=1}^{n} f_i x^i \to \sum_{i=1}^{n} \sigma(i) x^i$$

is a ring isomorphism. In the following we will just write σ for $\tilde{\sigma}$.

Proof. Readily verified. □

Corollary 4.2.20. [**extending isomorphism**] *Let $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ be a field isomorphism. For $i = 1, 2$ let $\mathbb{F}_i \leq \mathbb{E}_i$ be a field extension and suppose $a_i \in \mathbb{F}_i$ is algebraic over $\mathbb{F}_i$ with minimal polynomial p_i. Suppose that $\sigma(p_1) = p_2$. Then there exists a field isomorphism*

$$\breve{\sigma} : \mathbb{F}_1[a_1] \to \mathbb{F}_2[a_2]$$

with

$$\rho(a_1) = a_2 \textit{ and } \rho\mid_{\mathbb{F}_1} = \sigma$$

Proof. By 4.2.19(c) $\sigma : \mathbb{F}_1[x] \to \mathbb{F}_2[x], f \to \sigma(f)$ is a ring isomorphism. By 4.2.19(b:a) $\sigma(p_1\mathbb{F}_1[x]) = \sigma(p_1)\mathbb{F}_2[x] = p_2\mathbb{F}_2[x]$ and so by 4.2.19(b:c)

$$\mathbb{F}_1[x]/p_1\mathbb{F}_1[x] \to \mathbb{F}_2[x]/p_2\mathbb{F}_2[x], f + p_1\mathbb{F}_1[x] \to \sigma(f) + p_2\mathbb{F}_2[x] \tag{1}$$

is a ring isomorphism. By 4.2.16(b) for $i = 1, 2$

$$\mathbb{F}_i[x]/p_i\mathbb{F}_i[x] \to \mathbb{F}_i[a_i], f + p_i\mathbb{F}_i[x], \to f(a_i)$$

is a ring isomorphism.

Composing the three isomorphism in (1) and (2) we obtain the isomorphism

$$\begin{array}{cccccccc} \rho : & \mathbb{F}_1[x] & \to & \mathbb{F}_1[x]/p_1\mathbb{F}_1[x] & \to & \mathbb{F}_2[x]/(p_2) & \to & \mathbb{F}_2[x] \\ & f(a_1) & \to & f + p_1\mathbb{F}_1[x] & \to & \sigma(f) + p_2\mathbb{F}_2[x] & \to & \sigma(f)(a_2) \end{array}$$

For $f = k \in \mathbb{F}_1$ (a constant polynomial) we have $\sigma(f) = \sigma(k)$, $f(a_1) = k$ and $\sigma(f)(a_2) = \sigma(k)$. So $\rho(k) = \sigma(k)$.

For $f = x$ we have $\sigma(x) = x$, $f(a_1) = a_1$ and $\sigma(x)(a_2) = a_2$. So $\rho(a_1) = a_2$. □

Example 4.2.21. [**ex:find auto**]

(1) [**1**] Let

$$\mathbb{K}_1 = \mathbb{K}_2 = \mathbb{R}, \quad \mathbb{F}_1 = \mathbb{F}_2 = \mathbb{C}, \quad \sigma = \mathrm{id}_{\mathbb{R}}, \quad p_1 == p_2 = x^2 + 1, \quad a_1 = i, \quad a_2 = -i.$$

Note that $\mathbb{C} = \mathbb{K}[i] = \mathbb{K}[-i]$, $x^2 + 1$ is the minimal polynomial of i and $-i$ over $\mathbb{R}$ and $\sigma(x^2 + 1) = x^2 + 1$. Hence the assumptions of 4.2.20 are fulfilled and we conclude that there exists a field isomorphism

$$\breve{\sigma} : \mathbb{C} \to \mathbb{C}, \quad r \to r \text{ for all } r \in \mathbb{R}, i \to -i$$

Let $a, b \in \mathbb{R}$. Then

$$\check{\sigma}(a+bi) = \check{\sigma}(a) + \check{\sigma}(b)\check{\sigma}(-i) = a + b(-i) = a - bi$$

This shows $\check{\sigma}$ is complex conjugation.

(2) [**2**] Let

$$\mathbb{K}_1 = \mathbb{K}_2 = \mathbb{Q}, \quad \mathbb{F}_1 = \mathbb{F}_2 = \mathbb{C}, \quad \sigma = \mathrm{id}_{\mathbb{Q}}, \quad p_1 = p_2 = x^3{-}2, \quad \xi = e^{2\pi i}3a_1 = \sqrt[3]{2}, \quad a_2 = \xi\sqrt[3]{2}.$$

Again the assumptions of 4.2.20 are fulfilled and we obtain a field isomorphism

$$\check{\sigma} : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\xi\sqrt[3]{2}, q \to q \text{ for all } q \in \mathbb{Q}, \sqrt[3]{2} \to \xi\sqrt[3]{2}$$

For $a, b, c \in \mathbb{Q}$ we have

$$\check{\sigma}(a + b\sqrt[3]{2} + c\sqrt[4]{4}) \to \sigma(a + b\xi\sqrt[3]{2} + c\xi^2\sqrt[3]{4})$$

4.3 Splitting Fields

Definition 4.3.1. [**def:algebraic**] *A field extension $\mathbb{K} \leq \mathbb{F}$ is called* algebraic *if each $k \in \mathbb{F}$ is algebraic over $\mathbb{K}$.*

Example 4.3.2. [**ex:algebraic 2**]

1. [**1**] Let $c = a{+}bi \in \mathbb{C}$. Then $(x{-}c)(x{-}\bar{c}) = x^2{+}(c{+}\bar{c})x{+}c\bar{c}) = x^2{+}2ax{+}(a^2{+}b^2) \in \mathbb{R}[x]$. So c is the root of non-zero polynomial. Hence c is algebraic and $\mathbb{R} \leq \mathbb{C}$ is algebraic.

2. [**2**] π is transcendental over $\mathbb{Q}$. So $\mathbb{Q} \leq \mathbb{R}$ is not algebraic.

3. [**3**] Let $\mathbb{K}$ be a field, then $\mathbb{K} \leq \mathbb{K}(x)$ is not algebraic since, x is transcendental over $\mathbb{K}$, see 4.2.12(4).

Lemma 4.3.3. [**finite imp algebraic**] *Any finite field extension is algebraic.*

Proof. Let $\mathbb{K} \leq \mathbb{F}$ be a finite field extension. Let $a \in \mathbb{F}$. Suppose that a is transcendental over $\mathbb{K}$. Then by 4.2.15(c), $\mathbb{K} \leq \mathbb{F}$ is not finite, a contradiction. □

Definition 4.3.4. [**def:splitting fields**] *Let $\mathbb{K} \leq \mathbb{F}$ be field extensions and $f \in \mathbb{K}[x]$. We say that f* splits *in $\mathbb{F}$ if there exists $a_0, a_1 \dots a_n \in \mathbb{F}$ with*

(i) [**i**] $f = a_0(x - a_1)(x - a_2)\dots(x - a_n)$.

We say that $\mathbb{F}$ is a splitting field *for f over $\mathbb{K}$ if f splits in $\mathbb{F}$ and*

(ii) [**ii**] $\mathbb{F} = \mathbb{K}[a_1, a_2, \dots, a_n]$.

Proposition 4.3.5. [**existence of splitting fields**] *Let $\mathbb{K}$ be a field and $f \in \mathbb{K}[x]$. Then there exists a splitting field $\mathbb{F}$ for f over $\mathbb{K}$. Moreover, $\mathbb{K} \leq \mathbb{F}$ is finite of degree at most $n!$.*

Proof. The proof is by induction on $\deg f$. If $\deg f \leq 0$, then $f = a_0$ for some $a_0 \in \mathbb{K}$ and so $\mathbb{K}$ is a splitting field for f over $\mathbb{K}$. Now suppose that $\deg f = k+1$ and that the proposition holds for all fields and all polynomials of degree k. Let p be a monic irreducible divisor of f and put $\mathbb{E} = \mathbb{K}[x]/p\mathbb{K}[x]$. By 4.2.10 $\mathbb{E}$ is a field. We identify $a \in \mathbb{K}$ with $a + p\mathbb{K}[x]$. Then $\mathbb{K}$ is a subfield of $\mathbb{E}$. Let $h \in \mathbb{K}[x]$. Put $\overline{h} = h + p\mathbb{K}[x] \in \mathbb{E}$ and $b := x + p\mathbb{K}[x] \in \mathbb{E}$. Then $h = \sum_{i=0}^{n} k_i x^i$ for some $k_i \in \mathbb{K}$ and so

$$h(b) = \sum_{i=0}^{n} k_i b^i = \sum_{i=0}^{n} \overline{k_i}\overline{x}^i = \overline{\sum_{i=0}^{n} k_i x^i} = \overline{h}$$

Thus

$$\mathbb{K}[b] \overset{4.2.14(b)}{=} \{h(b) \mid h \in \mathbb{K}[x]\} = \{\overline{h} \mid h \in \mathbb{K}[x]\} = \{h + p\mathbb{K}[x] \mid h \in \mathbb{K}[x]\} = \mathbb{E}$$

Since $p \mid f$, $f \in p\overline{K}[x]$. So $\overline{f} = f + p\mathbb{K}[x] = p\mathbb{K}[x]0_{\mathbb{E}}$. Hence $f(b) = \overline{f} = 0_{\mathbb{E}}$ and b is a root of f in $\mathbb{E}$. By 3.8.15 $f = (x-b) \cdot g$ for some $g \in \mathbb{E}[x]$ with $\deg g = k$. So by the induction assumption there exists a splitting field $\mathbb{F}$ for g over $\mathbb{E}$ with $\dim_{\mathbb{E}} \mathbb{F} \leq k!$. Hence exist $a_0, \ldots, a_k \in \mathbb{F}$ with

(i) [**a**] $g = a_0(x-a_1)(x-a_2)\ldots(x-a_k)$;

(ii) [**b**] $\mathbb{F} = \mathbb{E}[a_1, a_2, \ldots, a_k]$; and

(iii) [**c**] $\dim_{\mathbb{F}} \mathbb{E} \leq k!$

Since $f = g \cdot (x-b)$ and $\mathbb{E} = \mathbb{K}[b]$ we conclude that

(iv) [**d**] $f = a_0(x-a_1)(x-a_2)\ldots(x-a_k)(x-b)$, and

(v) [**e**] $\mathbb{F} = \mathbb{K}[b][a_1, a_2, \ldots, a_b] = \mathbb{K}[a_1, \ldots, a_n, b]$.

Thus $\mathbb{F}$ is a splitting field for f over $\mathbb{K}$. By 4.2.16(h), p is the minimal polynomial for b over $\mathbb{E}$ and $\dim_{\mathbb{K}} \mathbb{E} = \dim_{\mathbb{K}} \mathbb{K}[b] = \deg p \leq \deg f = k+1$ and so by 4.2.8 and (iii)

$$\dim_{\mathbb{K}} \mathbb{F} = \dim_{\mathbb{F}} \mathbb{E} \cdot \dim_{\mathbb{E}} \mathbb{F} \leq (k+1) \cdot k! = (k+1)!$$

So the theorem also holds for polynomials of degree $k+1$ and so for all polynomials. □

Theorem 4.3.6. [**unique splitting**] *Suppose that*

(i) [**i**] *$\sigma : \mathbb{K}_1 \to \mathbb{K}_2$ is an isomorphism of fields;*

(ii) [**ii**] *For $i = 1$ and 2, $f_i \in \mathbb{K}[x]$ and $\mathbb{F}_i$ a splitting field for f_i over $\mathbb{K}_i$; and*

(iii) [**iii**] $\sigma(f_1) = f_2$

Then there exists a field isomorphism

$$\breve{\sigma} : \mathbb{F}_1 \to \mathbb{F}_2 \textit{ with } \breve{\sigma} \mid_{\mathbb{K}_1} = \sigma.$$

Suppose in addition that

(iv) [**iv**] *For $i = 1$ and 2, p_i is an irreducible factor of f_i in $\mathbb{K}[x]$ and a_i is a root of p_i in $\mathbb{F}_i$; and*

(v) [**v**] $\sigma(p_1) = \sigma(p_2)$.

Then $\breve{\sigma}$ can be chosen such that

$$\sigma(a_1) = a_2.$$

Proof. The proof is by induction on $\deg f$. If $\deg f \leq 0$, then $\mathbb{F}_1 = \mathbb{K}_1$ and $\mathbb{F}_2 = \mathbb{K}_2$ and so the theorem holds with $\sigma = \breve{\sigma}$.

So suppose that $\deg f = k+1$ and that the lemma holds for all fields and all polynomials of degree k. If (iv) and (v) hold let p_i and a_i as there.

Otherwise let p_1 be any irreducible factor of f_1. Put $p_2 = \sigma(p_1)$. By 4.2.19(c), $\sigma : \mathbb{F}_1[x] \to \mathbb{F}_2[x]$ is a ring isomorphism. Thus p_2 is a irreducible factor of $\sigma(f_1) = f_2$. Since f_i splits over $\mathbb{F}$, there exists a root a_i for p_i in $\mathbb{F}_i$.

Put $\mathbb{E}_i = \mathbb{F}_i[a_i]$. By 4.2.20 there exists a field isomorphism $\rho : \mathbb{E}_1 \to \mathbb{E}_2$ with $\rho(a_1) = a_2$ and $\rho \mid_{\mathbb{K}_1} = \sigma$. By the factor theorem $f_i = (x - a_i) \cdot g_i$ for some $g_i \in \mathbb{E}_i[x]$. Since $\rho \mid_{\mathbb{K}_1} = \sigma$ and f_1 has coefficients in $\mathbb{K}_1$, $\rho(f_1) = \sigma(f_1) = f_2$. Thus

$$(x - a_2) \cdot g_2 = f_2 = \rho(f_1) = \rho\big((x - a_1) \cdot g_1\big) = big(x - \rho(a_2)\big) \cdot \rho(g_1) = (x - a_2) \cdot \rho(g_1),$$

and so by the Cancellation Law $g_2 = \rho(g_1)$. Since $\mathbb{F}_i$ is a splitting field for f_i over $\mathbb{F}_i$, $\mathbb{F}_i$ is also a splitting field for g_i over $\mathbb{E}_i$. So by the induction assumption there exists a field isomorphism $\breve{\sigma} : \mathbb{F}_1 \to \mathbb{F}_2$ with $\breve{\sigma} \mid_{\mathbb{E}_i} = \rho$. We have $\breve{\sigma}(a_1) = \rho(a_1) = a_2$ and $\breve{\sigma} \mid_{\mathbb{K}_1} = \rho \mid_{\mathbb{K}_1} = \sigma$.

Thus the Theorem holds for polynomials of degree $k + 1$ and so by induction for all polynomials. □

Example 4.3.7. [**ex:splitting field**] Let $\xi = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Then the roots of $x^3 - 2$ are $\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}$ and so

$$\mathbb{F} := \mathbb{Q}[\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, \xi]$$

is splitting field of $x^3 - 2$ over $\mathbb{Q}$. Let $\sigma = \mathrm{id}_{\mathbb{Q}}$. By 4.3.6 there exists a automorphism $\breve{\sigma}$ of $\mathbb{F}$ with $\breve{\sigma}|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ and $\breve{\sigma}(\sqrt[3]{2}) = \xi\sqrt[3]{2}$.

Put $\mathbb{K}_1 = \mathbb{Q}[\sqrt[2]{}]$ and $\mathbb{K}_2 = \mathbb{Q}[\xi\sqrt[2]{}]$. Then by Homework 4#5

$$\check{\sigma}(\mathbb{K}_1) = \check{\sigma}(\mathbb{Q}[\sqrt[3]{2}]) = \check{\sigma}(\mathbb{Q})[\check{\sigma}(\sqrt[3]{2})] = \mathbb{Q}[\xi\sqrt[3]{2}] = \mathbb{K}_2$$

and so we obtain a field isomorphism

$$\tau : \mathbb{K}_1 \to \mathbb{K}_2, a \to \check{\sigma}(a)$$

Note that $\tau(q) = q$ for all $q \in \mathbb{Q}$ and $\tau(\sqrt[3]{2}) = \xi\sqrt[3]{2}$.

Since x^3-2 has a root in $\mathbb{Q}[\sqrt[3]{2}]$, it is not irreducible over $\mathbb{Q}[\sqrt[3]{2}]$. We will now determine its irreducible factors. For this let α be any root of x^3-2. Then

$$\begin{array}{r|ccccccc}
\multicolumn{1}{r}{} & x^2 & + & \alpha x & + & \alpha^2 & & \\ \cline{2-8}
x-\alpha & x^3 & & & & & - & 2 \\ \cline{1-1}
\multicolumn{1}{r}{} & x^3 & - & \alpha x^2 & & & & \\ \cline{2-8}
\multicolumn{1}{r}{} & & & \alpha x^2 & & & - & 2 \\
\multicolumn{1}{r}{} & & & \alpha x^2 & - & \alpha^2 x & & \\ \cline{3-8}
\multicolumn{1}{r}{} & & & & & \alpha^2 x & - & 2 \\
\multicolumn{1}{r}{} & & & & & \alpha^2 x & - & \alpha^3 \\ \cline{5-8}
\multicolumn{1}{r}{} & & & & & & & 0
\end{array}$$

Thus $x^3-2 = (x-\alpha)(x^2+\alpha x+\alpha^2)$. Put $g_1 = x^2+\sqrt[3]{2}\,x+\sqrt[3]{4}$ and $g_2 = x^2+\xi\sqrt[3]{2}, x+\xi^2\sqrt[3]{4}$. Then $x^3-2 = (x-\sqrt[3]{2})g_1$ and $\tau(g_1) = g_2$. Also the roots of g_1 are $\xi\sqrt[3]{2}$ and $\xi^2\sqrt[3]{2}$. Note that that $\xi \notin \mathbb{R}$ and also $\xi^2 \notin \mathbb{R}$. Hence neither $\xi\sqrt[3]{2}$ nor $\xi^2\sqrt[3]{2}$ is in $\mathbb{K}_1 = \mathbb{Q}[\sqrt[3]{2}]$. Thus g_1 is irreducible over $\mathbb{K}_1$. It follows that also $g_2 = \tau(g_1)$ is irreducible over $\mathbb{K}_2 = \tau(\mathbb{K}_1)$. Note that $\mathbb{F}$ is a splitting field for $x^3 = 2$ over $\mathbb{K}_i$ and g_i is an irreducible factor of x^3-2. Since $\xi\sqrt[3]{2}$ is a root of g_1 and $\sqrt[3]{2}$ is a root of g_2 we conclude from 4.3.6 that there exists isomorphism $\check{\tau} : \mathbb{F} \to \mathbb{F}$ with $\check{\tau}|_{\mathbb{K}_1} = \tau$ and $\check{\tau}(\xi\sqrt[3]{2})\sqrt[3]{2}$. Since $\tau(\xi\sqrt[3]{4})$ is a root of g_2 we get $\check{\tau}(\xi\sqrt[3]{4}) = \xi\sqrt[3]{4}$.

Also

$$\check{\tau}(\xi) = \check{\tau}\left(\frac{\xi\sqrt[3]{2}}{\sqrt[3]{2}}\right) = \frac{\check{\tau}(\xi\sqrt[3]{2})}{\check{\tau}(\sqrt[3]{2})} = \frac{\sqrt[3]{2}}{\xi\sqrt[3]{2}} = \frac{1}{\xi} = \xi^2 = \overline{\xi}$$

4.4 Separable Extension

Definition 4.4.1. [**def:sep**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension.*

(a) [**a**] *Let $f \in \mathbb{K}[x]$. If f is irreducible, then f is called* separable *over $\mathbb{K}$ provided that f does not have a double root in its splitting field over $\mathbb{K}$. In general, f is called separable over $\mathbb{K}$ provided that all irreducible factors of f in $\mathbb{K}[x]$ are separable over $\mathbb{K}$.*

(b) [**b**] *$a \in \mathbb{F}$ is called separable over $\mathbb{F}$ if a is algebraic over $\mathbb{K}$ and the minimal polynomial of a over $\mathbb{K}$ is separable over $\mathbb{K}$.*

(c) [**c**] *$\mathbb{K} \leq \mathbb{F}$ is called separable over $\mathbb{K}$ if each $a \in \mathbb{F}$ is separable over $\mathbb{K}$.*

Example 4.4.2. [**ex:sep**]

(1) [**1**] Let $\mathbb{K}$ be any field. Then $x^2 = x \cdot x$, x is irreducible and x has not multiple roots. So x and x^2 are separable over $\mathbb{K}$.

(2) [**2**] Let $\mathbb{K}$ be any field. Let $f = x^2 + x + 1 \in \mathbb{K}[x]$. We will show that f is separable over $\mathbb{K}$. For this let a, b be elements in a splitting field for f over $\mathbb{K}$ with $f = (x-a)(x-b)$. Since $(x-a)(x-b) = x^2 + x + 1$ we have $a + b = -1$ and $ab = 1$.

If $a \neq b$, then f has not multiple roots and so f is separable.

Suppose that $a = b$. Then $2a = -1$. Thus $\operatorname{char} \mathbb{K} \neq 0$ and $a = -\frac{1}{2}$. Moreover $1 = ab = a^2 = \frac{1}{4}$ and so $4 = 1$ and $3 = 0$. Thus $\operatorname{char} K = 3$ and $a = -\frac{1}{2} == \frac{1}{-1} = 1$. If follows that $f = (x+1)^2$. Since $x + 1$ is separable, f is separable.

(3) [**3**] Let y be an indeterminate over $\mathbb{Z}_2$, that is $\mathbb{Z}_2 \leq \mathbb{Z}_2(y)$ is a transcendental field extension. Put

$$\mathbb{F} = \mathbb{Z}_2(y) = \{ab^{-1} \mid a, b \in \mathbb{Z}_2[y], b \neq 0_{\mathbb{Z}_2}\}$$

and

$$\mathbb{K} = \mathbb{Z}_2(y^2).$$

Note that $\mathbb{K}$ is a subfield of $\mathbb{F}$. It is not to difficult to see that $y \notin \mathbb{K}$. Since $-1_{\mathbb{Z}_2} = 1_{\mathbb{Z}_2}$,

$$x^2 - y^2 = (x-y)(x+y) = (x-y)^2.$$

So y is a double root of $x^2 - y^2$. Since $y \notin \mathbb{K}$, $x^2 - y^2$ has no root in $\mathbb{K}$ and so by 3.8.16(c) is irreducible in $\mathbb{K}[x]$. Hence by 4.2.16(h) $x^2 - y^2$ is the minimal polynomial of t over $\mathbb{K}$. Since y is a double root of $x^2 - y^2$, $x^2 - y^2$ is not separable. So also y is not separable over $\mathbb{K}$ and $\mathbb{F}$ is not separable over $\mathbb{K}$.

Lemma 4.4.3. [**sep**] *Let $\mathbb{E} \leq \mathbb{F}$ and $\mathbb{K} \leq \mathbb{E}$ be a field extensions.*

(a) [**a**] *Let $a \in \mathbb{F}$ be algebraic over $\mathbb{K}$. Then a is algebraic over $\mathbb{E}$. Moreover, if $m_a^{\mathbb{E}}$ is the minimal polynomial of a over $\mathbb{E}$, and $m_a^{\mathbb{K}}$ is the minimal polynomial of a over $\mathbb{K}$, then $m_a^{\mathbb{E}}$ divides $m_a^{\mathbb{K}}$ in $\mathbb{E}[x]$.*

(b) [**b**] *If $f \in \mathbb{K}[x]$ is separable over $\mathbb{K}$, then f is separable over $\mathbb{E}$.*

(c) [**c**] *If $a \in \mathbb{F}$ is separable over $\mathbb{K}$, then a is separable over $\mathbb{E}$.*

(d) [**d**] *If $\mathbb{K} \leq \mathbb{F}$ is separable, then also $\mathbb{E} \leq \mathbb{F}$ and $\mathbb{F} \leq \mathbb{E}$ are separable.*

Proof. (a) Since $m_a^{\mathbb{K}}(a) = 0_{\mathbb{K}}$ and $m_a^{\mathbb{E}} \in \mathbb{K}[x] \subseteq \mathbb{E}[x]$, a is algebraic over $\mathbb{E}$. Moreover, by 4.2.16(g), $m_\alpha^{\mathbb{E}}$ divides $m_\alpha^{\mathbb{K}}$ in $\mathbb{E}[x]$.

(b) Let $f \in \mathbb{K}[x]$ be separable over $\mathbb{K}$. Then $f = p_1 p_2 \ldots p_k$ for some irreducible $p_i \in \mathbb{K}[x]$. Moreover, $p_i = q_{i1} q_{i2} \ldots q_{il_i}$ for some irreducible $q_{ij} \in \mathbb{E}[x]$. Since f is separable, p_i has no double roots. Since q_{ij} divides p_i also q_{ij} has no double roots. Hence q_{ij} is separable over $\mathbb{E}$ and so also f is separable over $\mathbb{E}$.

(c) Since a is separable over $\mathbb{E}$, $m_a^{\mathbb{K}}$ has no double roots. By (a) $m_a^{\mathbb{E}}$ divides $m_a^{\mathbb{K}}$ and so also $m_a^{\mathbb{E}}$ has no double roots. Hence a is separable over $\mathbb{E}$.

(d) Let $a \in \mathbb{F}$. Since $\mathbb{K} \leq \mathbb{F}$ is separable, a is separable over $\mathbb{K}$. So by (c), a is separable over $\mathbb{E}$. Thus $\mathbb{E} \leq \mathbb{F}$ is separable. Let $a \in \mathbb{E}$. Then $a \in \mathbb{F}$ and so a is separable over $\mathbb{K}$. Hence $\mathbb{K} \leq \mathbb{E}$ is separable. □

4.5 Galois Theory

Definition 4.5.1. [**def:aut fk**] *Let $\mathbb{K} \leq \mathbb{F}$ be field extension.* $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ *is the set of all field isomorphism $\alpha : \mathbb{F} \to \mathbb{F}$ with $\alpha \mid_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$.*

Lemma 4.5.2. [autfk] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension. Then* $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ *is a subgroup of* $\mathrm{Sym}(\mathbb{F})$*.*

Proof. Clearly $\mathrm{id}_{\mathbb{F}} \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Let $\alpha, \beta \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then by 4.2.19(a) $\alpha \circ \beta$ is a field isomorphism. If $a \in \mathbb{K}$, then $\alpha(\beta(a)) = \alpha(a) = a$ and so $(\alpha \circ \beta) \mid_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$. So $\alpha \circ \beta \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. By 4.2.19(a) α^{-1} is a field isomorphism. Since $\alpha \mid_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$ also $\alpha^{-1} \mid_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$ and so $\alpha^{-1} \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Hence by 2.3.3, $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ is a subgroup of $\mathrm{Sym}(\mathbb{F})$. □

Example 4.5.3. [**ex:aut fk**] What is $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$?

Let $\sigma \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ and $a, b \in \mathbb{R}$. Since $\sigma_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$ we have $\sigma(a) = a$ and $\sigma(b) = b$. Thus

$$(*) \qquad \sigma(a + bi) = \sigma(a) = \sigma(b)\sigma(i) = a + b\sigma(i).$$

So we need to determine $\sigma(i)$. Since $i^2 = -1$, we get

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1.$$

Thus $\sigma(i) = i$ or $-i$. If $\sigma(i) = i$, then (*) shows that $\sigma = \mathrm{id}_{\mathbb{C}}$ and if $\sigma(i) = -i$, (*) shows that σ is complex conjugation. By Example 4.2.21, complex conjugation is indeed an automorphism of $\mathbb{C}$ and thus

$$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_C, \text{complex conjugation}\}.$$

Note here that $|\mathrm{Aut})\mathbb{R}(\mathbb{C})| = 2 = \dim_{\mathbb{R}} \mathbb{C}$.

Definition 4.5.4. [**def: fix kh**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $H \subseteq \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Then*

$$\mathrm{Fix}_{\mathbb{F}}(H) := \{k \in \mathbb{F} \mid \sigma(k) = k \textit{ for all } \sigma \in H\}.$$

$\mathrm{Fix}_{\mathbb{F}}(H)$ is called the fixed-field *of H in $\mathbb{F}$.*

Lemma 4.5.5. [**fix h**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and H a subset of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then $\mathrm{Fix}_{\mathbb{F}}(H)$ is subfield of $\mathbb{F}$ containing $\mathbb{K}$.*

Proof. By definition of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$, $\sigma(a) = a$ for all $a \in \mathbb{K}$, $\sigma \in H$. Thus $\mathbb{K} \subseteq \mathrm{Fix}_{\mathbb{F}}(H)$. In particular, $0_{\mathbb{K}}, 1_{\mathbb{K}} \in \mathrm{Fix}_{\mathbb{F}}(H)$.

Let $a, b \in \mathrm{Fix}_{\mathbb{F}}(H)$ and $\sigma \in H$. Then

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a + b,$$

and so $a + b \in \mathrm{Fix}_{\mathbb{F}}(H)$.

$$\sigma(-a) = -\sigma(a) = -a,$$

and so $-a \in \mathrm{Fix}_{\mathbb{F}}(H)$.

$$\sigma(ab) = \sigma(a)\sigma(b) = ab,$$

and so $ab \in \mathrm{Fix}_{\mathbb{F}}(H)$. Finally if $a \neq 0_{\mathbb{K}}$, then

$$\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1},$$

and so $a^{-1} \in \mathrm{Fix}_{\mathbb{F}}(H)$.

Hence $\mathrm{Fix}_{\mathbb{F}}(H)$ is a subfield of $\mathbb{F}$. □

Example 4.5.6. [**ex:fix h**] By Example 4.5.3, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$, where σ is complex conjugation. Thus $\mathrm{Aut}_{\mathbb{R}}\mathbb{C}$ has two subgroups namely, $\{\mathrm{id}_{\mathbb{C}}\}$ and $\{\mathrm{id}_{\mathbb{C}}, \sigma\}$. We will compute the fixed field for both this subgroups. Clearly

$$\mathrm{Fix}_{\mathbb{C}}(\{\mathrm{id}_{\mathbb{C}}\}) = \mathbb{C}.$$

Also $a + bi$ is fixed by σ if and only if $a + bi = a - bi$, if and only if $b = 0$, that if and only if $a + bi \in \mathbb{R}$.

$$\mathrm{Fix}_{\mathbb{C}}(\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})) = \mathbb{R}.$$

Let $\mathbb{E}$ be a field with $\mathbb{R} \leq \mathbb{E} \leq \mathbb{C}$. Then by 4.2.8

$$2 = \dim_{\mathbb{R}} \mathbb{C} = \dim_{\mathbb{R}} \mathbb{E} \cdot \dim_{\mathbb{E}} \mathbb{C}$$

and so either $\dim_{\mathbb{R}} \mathbb{E} = 1$ or $\dim_{\mathbb{E}} \mathbb{C} = 1$. Thus $\mathbb{E} = \mathbb{R}$ or $\mathbb{E} = \mathbb{C}$. So see that the is a 1-1 correspondence between the subgroup of $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ and the fields between $\mathbb{R}$ and $\mathbb{C}$.

Proposition 4.5.7. [**acts on roots**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and $0_{\mathbb{K}} \neq f \in \mathbb{K}[x]$.*

(a) [**a**] *Let $a \in \mathbb{F}$ and $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then $\sigma(f(a)) = f(\sigma(a))$.*

(b) [**b**] *The set of roots of f in $\mathbb{F}$ is invariant under $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. That is if a is a root of f in $\mathbb{F}$ and $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$, then $\sigma(a)$ is also a root of f in $\mathbb{F}$.*

(c) [**c**] *Let $a \in \mathbb{F}$. Then $\mathrm{Stab}_{\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})}(a) = \mathrm{Aut}_{\mathbb{K}(a)}(\mathbb{F})$.*

(d) [**d**] *Let a be root of f in $\mathbb{F}$. Then*

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})/\mathrm{Aut}_{\mathbb{K}[a]}(\mathbb{F})| = |\{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})\}|.$$

Proof. (a) Let $f = \sum_{i=0}^{n} f_i x^i$. Then

$$\sigma(f(a)) = \sigma\left(\sum_{i=0}^{n} f_i a^i\right) = \sum_{i=0}^{n} \sigma(f_i)\sigma(a)^i = \sum_{i=0}^{n} f_i \sigma(a)^i = f(\sigma(a)).$$

(b) Let a be a root of f in $\mathbb{F}$ then $f(a) = 0_{\mathbb{F}}$ and so by (a)

$$f(\sigma(a)) = \sigma(f(a)) = \sigma(0_{\mathbb{F}}) = 0_{\mathbb{F}}.$$

(c) Put $H = \mathrm{Stab}_{\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})}(a) = \{\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F}) \mid \sigma(a) = a\}$. Then clearly $\mathrm{Aut}_{\mathbb{K}[a]}(\mathbb{F}) \subseteq H$. Note that $a \in \mathrm{Fix}_{\mathbb{F}}(H)$ and by 4.5.5 $\mathrm{Fix}_{\mathbb{F}}(H)$ is a subfield of $\mathbb{F}$ containing $\mathbb{K}$. So $\mathbb{K}(a) \subseteq \mathrm{Fix}_{\mathbb{F}}(H)$ and thus $H \subseteq \mathrm{Aut}_{\mathbb{K}(a)}(\mathbb{F})$. Therefore $H = \mathrm{Aut}_{\mathbb{K}(a)}(\mathbb{F})$.

(d) By 2.7.17(d)

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})/\mathrm{Stab}_{\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})}(a)| = |\{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})\}|,$$

and so (d) follows from (c). □

Theorem 4.5.8. [**ftg i**] *Let $\mathbb{K}$ be a field and $\mathbb{F}$ the splitting field of a separable polynomial over $\mathbb{K}$. Then*

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})| = \dim_{\mathbb{K}} \mathbb{F}.$$

Proof. The proof is by induction on $\dim_{\mathbb{K}} \mathbb{F}$. If $\dim_{\mathbb{K}} \mathbb{F} = 1$, then $\mathbb{F} = \mathbb{K}$ and $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F}) = \{\mathrm{id}_{\mathbb{K}}\}$. So the theorem holds in this case. Suppose now that theorem holds for all finite field extensions of degree less than $\dim_{\mathbb{K}} \mathbb{F}$. Let $f \in \mathbb{K}[x]$ be separable polynomial with $\mathbb{F}$ as splitting field and let a be a root of f with $a \notin \mathbb{K}$. Let R be the set of roots of f in $\mathbb{F}$. Since m_a has no double roots, $|R| = \deg m_a$ and so by 4.2.16(f),

$$|R| = \dim_{\mathbb{K}} \mathbb{K}[a]. \tag{1}$$

Put

$$S = \{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})\}.$$

We will show that $S = R$. Let $b \in R$. Then by 4.3.6 applied with $\mathbb{K}_1 = \mathbb{K}_2 = \mathbb{K}, \mathbb{F}_1 = \mathbb{F}_2 = \mathbb{F}$, $\sigma = \mathrm{id}_{\mathbb{K}}$, $f_1 = f_2 = f$, $p_1 = p_2 = m_a$, $a_1 = a$ and $a_2 = b$, there exists a field isomorphism $\breve{\sigma} : \mathbb{F} \to \mathbb{F}$ with

$$\breve{\sigma} \mid_{\mathbb{K}} = \sigma = \mathrm{id}_{\mathbb{K}} \text{ and } \breve{\sigma}(a) = b.$$

Then $\breve{\sigma} \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ and so $b = \breve{\sigma}(a) \in S$. Hence

$$R \subseteq S.$$

By 4.5.7(b), $\sigma(a)$ is a root of f for each $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Thus $S \subseteq R$ and

$$R = S. \tag{2}$$

By 4.5.7(d)

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})/\mathrm{Aut}_{\mathbb{K}[a]}(\mathbb{F})| = |\{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})\}| = |S|,$$

and so by (1) and (2)

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})/\mathrm{Aut}_{\mathbb{K}[a]}(\mathbb{F})| = \dim_{\mathbb{K}} \mathbb{K}[a]. \tag{3}$$

Observe that $\mathbb{F}$ is a splitting field for f over $\mathbb{K}[a]$ and that by 4.4.3(b), f is separable over $\mathbb{K}[a]$. Moreover, by 4.2.8

$$\dim_{\mathbb{K}[a]} \mathbb{F} = \frac{\dim_{\mathbb{K}} \mathbb{F}}{\dim_{\mathbb{K}[a]}(\mathbb{F})} < \dim_{\mathbb{K}} \mathbb{F},$$

and so by induction

$$|\mathrm{Aut}_{\mathbb{K}[a]}(\mathbb{F})| = \dim_{\mathbb{K}[a]} \mathbb{F}. \tag{4}$$

Multiplying (3) with (4) gives

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})/\mathrm{Aut}_{\mathbb{K}[a]}(\mathbb{F})| \cdot |\mathrm{Aut}_{\mathbb{K}[a]}(\mathbb{F})| = \dim_{\mathbb{K}} \mathbb{K}[a] \cdot \dim_{\mathbb{K}[a]} \mathbb{F}. \tag{5}$$

So by Lagrange's Theorem and Corollary 4.2.8,

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})| = \dim_{\mathbb{K}} \mathbb{F}.$$

□

Example 4.5.9. [**ex:ftg i**] By Example 4.2.18 x^3-2 is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ and $\dim_{\mathbb{Q}} \mathbb{Q}\left[\sqrt[3]{2}\right]=3$. The other roots of x^3-2 are $\xi\sqrt[3]{2}$ and $\xi^2\sqrt[3]{2}$, where $\xi=e^{\frac{2\pi}{3}i}$. Also by Example 4.2.18 ξ is a root of x^2+x+1. Since $\xi\notin\mathbb{R}$, $\xi\notin\mathbb{Q}\left[\sqrt[2]{2}\right]$. Thus x^2+x+1 is the minimal polynomial of ξ over $\mathbb{Q}\left[\sqrt[3]{2}\right]$. Put $\mathbb{F}=\mathbb{Q}\left[\sqrt[3]{2},\xi\right]$. Then $\dim_{\mathbb{Q}\left[\sqrt[3]{2}\right]}\mathbb{F}=2$ and so

$$\dim_{\mathbb{Q}}\mathbb{F}=\dim_{\mathbb{Q}}\mathbb{Q}\left[\sqrt[3]{2}\right]\cdot\dim_{\mathbb{Q}\left[\sqrt[3]{2}\right]}\mathbb{F}=3\cdot 2=6$$

Note that

$$\mathbb{F}=\mathbb{Q}\left[\sqrt[3]{2},\xi\sqrt[3]{2},\xi^2\sqrt[3]{2}\right],$$

and so $\mathbb{F}$ is the splitting field of x^3-2 over $\mathbb{Q}$. Let $R=\left\{\sqrt[3]{2},\xi\sqrt[3]{2},\xi^2\sqrt[3]{2}\right\}$, the set of roots of x^3-2. By 4.5.7, R is $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{F})$-invariant and so by 2.7.8(d), $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{F})$ acts on R. The homomorphism associated to this action is

$$\alpha:\operatorname{Aut}_{\mathbb{K}}(\mathbb{F})\to\operatorname{Sym}(R),\sigma\to\sigma\mid_R.$$

Let $\sigma\in\ker\alpha$. Then $R\subseteq\operatorname{Fix}_{\mathbb{F}}(\sigma)$. Since $\operatorname{Fix}_{\mathbb{F}}(\sigma)$ is a subfield of $\mathbb{F}$ containing $\mathbb{Q}$, this implies $\operatorname{Fix}_{\mathbb{F}}(\sigma)=\mathbb{F}$ and so $\sigma=\mathrm{id}_{\mathbb{F}}$. Thus by 2.6.3(f) α is 1-1. By 4.5.8 $|\operatorname{Aut}_{\mathbb{K}}(\mathbb{F})|=\dim_{\mathbb{Q}}\mathbb{F}=6$. Since also $|\operatorname{Sym}(R)|=6$ we conclude that α is a bijection and so

$$\operatorname{Aut}_{\mathbb{K}}(\mathbb{F})\cong\operatorname{Sym}(R)\cong\operatorname{Sym}(3).$$

Lemma 4.5.10. [**bounded deg**] *Let $\mathbb{K}\le\mathbb{F}$ be a field extension and G a finite subgroup of $\operatorname{Aut}_{\mathbb{K}}(\mathbb{F})$ with $\operatorname{Fix}_{\mathbb{F}}(G)=\mathbb{K}$. Then $\mathbb{K}\le\mathbb{F}$ is finite and $\dim_{\mathbb{K}}\mathbb{F}\le|G|$.*

Proof. Put $m=|G|$ and let $G=\{\sigma_1,\sigma_2,\dots,\sigma_m\}$ with $\sigma_1=\mathrm{id}_{\mathbb{F}}$.

Let $(a_1,a_2,\dots,a_n)$ be $\mathbb{K}$-linearly independent list in $\mathbb{F}$ and let $C_1,C_2,\dots,C_n$ be the columns of the matrix

$$(\sigma_i(a_j))=\begin{pmatrix} a_1 & a_2 & \dots & a_n\\ \sigma_2(a_1) & \sigma_2(a_2) & \dots & \sigma_2(a_n)\\ \vdots & \vdots & \vdots & \vdots\\ \sigma_m(a_1) & \sigma_m(a_2) & \dots & \sigma_m(a_n)\end{pmatrix}.$$

Claim: $(C_1,C_2,\dots,C_n)$ is linearly independent over $\mathbb{F}$.

Before we prove the Claim we will show that Lemma follows from the Claim. Since $\mathbb{F}^m$ has dimension m over $\mathbb{F}$, 4.1.22 implies that any $\mathbb{F}$-linear independent list in $\mathbb{F}^m$ has length at most m. So if $(C_1,C_2,\dots,C_n)$ is linearly independent, then $n\le m$ and $\dim_{\mathbb{K}}\mathbb{F}\le|G|$.

Suppose now that the Claim is false and under all the $\mathbb{K}$ linearly independent list $(a_1,\dots,a_n)$ for which $(C_1,C_2\dots,C_n)$ is linearly dependent over $\mathbb{F}$ choose one with n as small as possible. Then there exist $l_1,l_2\dots l_n\in\mathbb{F}$ not all zero with

(1) $$\sum_{j=1}^{n} l_k C_j = \vec{0}.$$

If $l_1 = 0_{\mathbb{F}}$, then $\sum_{j=2}^{n} l_j C_j = \vec{0}$ and so also $(a_2, \ldots, a_n)$ is a counterexample. This contradicts the minimal choice of n.

Hence $l_1 \neq 0_{\mathbb{F}}$. Note that also $\sum_{j=1}^{n} l_1^{-1} l_j C_j = \vec{0}$. So we may assume that $l_1 = 1_{\mathbb{K}}$.

Suppose that $l_j \in \mathbb{K}$ for all $1 \leq j \leq n$. Considering the first coordinate in the equation (1) we conclude

$$\sum_{j=1}^{n} l_j a_j = 0_{\mathbb{K}},$$

a contradiction since $(a_1, \ldots, a_n)$ is linearly independent over $\mathbb{K}$. So there exists $1 \leq k \leq n$ with $l_k \notin \mathbb{K}$. Note that $l_1 = 1_{\mathbb{K}} \in \mathbb{K}$ and so $k > 1$. Without loss $k = 2$. So $l_2 \notin \mathbb{K}$. Since $\mathrm{Fix}_{\mathbb{F}}(G) = \mathbb{K}$, $l_2 \notin \mathrm{Fix}_{\mathbb{F}}(G)$ and so there exists $\rho \in G$ with $\rho(l_2) \neq l_2$. Note that (1) is equivalent to the system of equation

$$\sum_{j=1}^{n} l_j \sigma(a_j) = 0_{\mathbb{K}} \text{ for all } \sigma \in G.$$

Applying ρ to each of these equation we conclude

$$\sum_{j=1}^{n} \rho(l_k)(\rho \circ \sigma)(a_j) = 0_{\mathbb{K}} \text{ for all } \sigma \in G.$$

Since $\sigma = \rho \circ (\rho^{-1} \circ \sigma)$ these equations with $\rho^{-1} \circ \sigma$ in place of σ give

$$\sum_{j=1}^{n} \rho(l_j)\sigma(a_j) = 0_{\mathbb{K}} \text{ for all } \sigma \in G,$$

and so

(2) $$\sum_{j=1}^{n} \rho(l_j) C_j = \vec{0}.$$

Subtracting (1) from (2) gives

$$\sum_{j=1}^{n} (\rho(l_j) - l_j) C_j = \vec{0}.$$

Since $l_1 = 1_{\mathbb{K}} = \rho(1_{\mathbb{K}})$, $\rho(l_1) - l_1 = 0_{\mathbb{K}}$ and so

$$(3) \qquad \sum_{j=2}^{n}(\rho(l_j) - l_j)C_j = \vec{0}.$$

Since $\rho(l_2) \neq l_2$, $\rho(l_2) - l_2 \neq 0_{\mathbb{K}}$. So not all the coefficient in (3) are zero, a contradiction to the minimal choice of n. □

Proposition 4.5.11. [**compute min poly**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension and G a finite subgroup of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ with $\mathrm{Fix}_{\mathbb{F}}(G) = \mathbb{K}$. Let $a \in \mathbb{F}$. Then a is algebraic over $\mathbb{K}$. Let $a_1, a_2, \dots a_n$ be the distinct elements of $Ga = \{\sigma(a) \mid \sigma \in G\}$. Then*

$$m_a = (x - a_1)(x - a_2) \dots (x - a_n).$$

In particular, m_a splits over $\mathbb{F}$ and $\mathbb{F}$ is separable over $\mathbb{K}$.

Proof. Put $q = (x - a_1)(x - a_2) \dots (x - a_n)$. Then $q \in \mathbb{F}[x]$. We will show that $q \in \mathbb{K}[x]$.

Let $\sigma \in G$. Then

$$(1) \qquad \sigma(q) = \sigma\big((x - a_1)(x - a_2) \dots (x - a_n)\big) = \big(x - \sigma(a_1)\big)\big(x - \sigma(a_2)\big) \dots \big(x - \sigma(a_n)\big).$$

Let $b \in Ga$. Then $b = \rho(a)$ for some $\rho \in G$ and so $\sigma(b) = \sigma(\rho(a)) = (\sigma \circ \rho)(a) \in Ga$. Thus the map $Ga \to Ga$, $b \to \sigma(b)$ is a bijection with inverse $b \to \sigma^{-1}(b)$. Hence

$$\big(x - \sigma(a_1)\big)\big(x - \sigma(a_2)\big) \dots \big(x - \sigma(a_n)\big) = (x - a_1)(x - a_2) \dots (x - a_n) = q.$$

Thus by (1)

$$(2) \qquad \sigma(q) = q.$$

Let $q = \sum_{i=0}^{n} q_i x^i$ with $q_i \in \mathbb{F}$. Then

$$\sum_{i=0}^{n} q_i x^i = q \overset{(2)}{=} \sigma(q) = \sigma\left(\sum_{i=0}^{n} q_i x^i\right) = \sum_{i=0}^{n} \sigma(q_i),$$

and so

$$q_i = \sigma(q_i) \text{ for all } 0 \leq i \leq n, \sigma \in G.$$

It follows that for all $0 \leq i \leq n$,

$$q_i \in \mathrm{Fix}_{\mathbb{F}}(G) = \mathbb{K}.$$

Hence $q \in \mathbb{K}[x]$.

Since $a = \mathrm{id}_{\mathbb{F}}(a)$ is one of the a_i's we have $q(a) = 0_{\mathbb{K}}$. Thus 4.2.16(g) implies that $m_a \mid q$. By 4.5.7 each a_i is a root of m_a and so q divides m_a in $\mathbb{F}[x]$. Since m_a and q both are monic we conclude that $m_a = q$. So

$$m_a = (x - a_1)(x - a_2) \dots (x - a_n).$$

Since each $a_i \in \mathbb{F}$, m_a splits over $\mathbb{F}$. Since the a_i's are pairwise distinct, m_a is separable. So a is separable over $\mathbb{F}$. Since $a \in \mathbb{F}$ was arbitrary, $\mathbb{K} \leq \mathbb{F}$ is separable. □

Example 4.5.12. [**ex:min poly**] Let σ be complex conjugation and $G = \langle \sigma \rangle = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$. Then by Example 4.5.6, $\mathrm{Fix}_{\mathbb{C}}(G) = \mathbb{R}$ and so we can apply 4.5.11 to the extension $\mathbb{R} \leq \mathbb{C}$. Let $d \in \mathbb{C}$, then $d = a + bi$ for some $a, b \in \mathbb{R}$. Thus

$$Gd = \{\mathrm{id}_{\mathbb{C}}(a + bi), \sigma(a + bi) =\} = \{a + bi, a - bi\}$$

Suppose that $d \in \mathbb{R}$, then $b = 0$, $d = a + bi = a - bi$ and so by 4.5.11

$$m_d = x - d$$

Suppose next that $d \notin \mathbb{R}$. Then $b \neq 0$, $a + bi \neq a - bi$ and by 4.5.11

$$m_d = (x - (a + bi))(x - (a - bi) = x^2 - 2ax + (a^2 + b^2)$$

Definition 4.5.13. [**def:normal ext**] *let A $\mathbb{K} \leq \mathbb{F}$ be a field extension.*

(a) [**a**] *$\mathbb{K} \leq \mathbb{F}$ is called* normal *if $\mathbb{K} \leq \mathbb{F}$ is algebraic and m_a splits over $\mathbb{F}$ over each $a \in \mathbb{F}$.*

(b) [**b**] *$\mathbb{K} \leq \mathbb{F}$ is called* Galois *if $\mathbb{K} \leq \mathbb{F}$ is finite, separable and normal.*

(c) [**c**] *An* intermediate *field of $\mathbb{K} \leq \mathbb{F}$ is a subfield $\mathbb{E}$ of $\mathbb{F}$ with $\mathbb{K} \subseteq \mathbb{E}$.*

Theorem 4.5.14. [**galois**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension. Then the following statements are equivalent.*

(a) [**a**] *$\mathbb{F}$ is the splitting field of a separable polynomial over $\mathbb{K}$.*

(b) [**b**] *$\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ is finite and $\mathbb{K} = \mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{F}))$.*

(c) [**c**] *$\mathbb{K} = \mathrm{Fix}_{\mathbb{F}}(G)$ for some finite subgroup G of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$.*

(d) [**d**] *$\mathbb{K} \leq \mathbb{F}$ is Galois.*

Proof. (a) $\Longrightarrow$ (b): By 4.5.8 $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ is finite of order $\dim_{\mathbb{K}} \mathbb{F}$. Put $\mathbb{E} := \mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{F}))$. Then $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F}) \subseteq \mathrm{Aut}_{\mathbb{E}}(\mathbb{F}) \subseteq \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ and so

$$(1) \qquad \mathrm{Aut}_{\mathbb{K}}(\mathbb{F}) = \mathrm{Aut}_{\mathbb{E}}(\mathbb{F}).$$

Since $\mathbb{F}$ is the splitting field of a separable polynomial f over $\mathbb{K}$, $\mathbb{F}$ is also the splitting field of f over $\mathbb{E}$. By 4.4.3 f is separable over $\mathbb{E}$ and so we can apply 4.5.8 to $\mathbb{E} \leq \mathbb{F}$ and $\mathbb{K} \leq \mathbb{F}$. Hence

$$\dim_{\mathbb{E}} \mathbb{F} \leq \dim_{\mathbb{K}} \mathbb{E} \cdot \dim_{\mathbb{E}} \mathbb{F} \overset{4.2.8}{=} \dim_{\mathbb{K}} \mathbb{F} \overset{4.5.8}{=} |\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})| \overset{(1)}{=} |\mathrm{Aut}_{\mathbb{E}}(\mathbb{F})| \overset{4.5.8}{=} \dim_{\mathbb{E}} \mathbb{F}.$$

Hence equality must hold everywhere in the above inequalities. Thus $\dim_{\mathbb{E}} \mathbb{F} = \dim_{\mathbb{K}} \mathbb{F}$ and so $\dim_{\mathbb{K}} \mathbb{E} = 1$ and $\mathbb{E} = \mathbb{K}$.

(b) $\Longrightarrow$ (c): Just put $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$.

(c) $\Longrightarrow$ (d): By 4.5.10 $\mathbb{K} \leq \mathbb{F}$ is finite and by 4.5.11, m_a splits over $\mathbb{F}$ and is separable. Thus $\mathbb{K} \leq \mathbb{F}$ is finite, normal and separable.

(d) $\Longrightarrow$ (a): Since $\mathbb{K} \leq \mathbb{F}$ is finite there exists a basis $(k_1, k_2, \ldots, k_n)$ for $\mathbb{F}$ over $\mathbb{K}$. Then $\mathbb{F} \subseteq \mathbb{K}[a_1, a_2 \ldots, a_n] \subseteq \mathbb{F}$ and

$$\mathbb{F} = \mathbb{K}[a_1, a_2 \ldots, a_n]. \tag{2}$$

Let m_i be the minimal polynomial of a_i over $\mathbb{K}$. Since $\mathbb{K} \leq \mathbb{F}$ is separable, m_i is separable over $\mathbb{K}$. Since $\mathbb{K} \leq \mathbb{F}$ is normal, p_i splits over $\mathbb{K}$. Put $m = m_1 m_2 \ldots m_n$. Then m is separable and splits over $\mathbb{F}$. Let $a_1, a_2, \ldots, a_n, a_{n+1}, \ldots, a_k$ be the roots of f in $\mathbb{F}$ then by (1), $\mathbb{F} \subseteq \mathbb{K}[a_1, a_2 \ldots, a_k] \subseteq \mathbb{F}$ and so

$$\mathbb{F} = \mathbb{K}[a_1, a_2 \ldots, a_k].$$

Thus $\mathbb{F}$ is a splitting field of m over $\mathbb{K}$. Since m is separable, (a) holds. □

Lemma 4.5.15. [**fix and conjugation**] *Let $\mathbb{K} \leq \mathbb{F}$ be a field extension. Let $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ and let $\mathbb{E}$ be subfield of $\mathbb{F}$ containing $\mathbb{K}$. Then*

$$\sigma \mathrm{Aut}_{\mathbb{E}}(\mathbb{F}) \sigma^{-1} = \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{F})$$

Proof. Let $\rho \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then

$$\begin{array}{rcll}
& \rho \in \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{F}) & & \\
\Longleftrightarrow & \rho(k) = k \text{ for all } k \in \sigma(\mathbb{E}) & - & \text{Definition of } \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{F}) \\
\Longleftrightarrow & \rho(\sigma(e)) = \sigma(e) \text{ for all } e \in \mathbb{E} & - & \text{Definition of } \sigma(\mathbb{E}) \\
\Longleftrightarrow & \sigma^{-1}(\rho(\sigma(e)) = e \text{ for all } e \in \mathbb{E} & - & \sigma \text{ is a bijection} \\
\Longleftrightarrow & (\sigma^{-1}\rho\sigma)(e) \text{ for all } e \in \mathbb{E} & - & \text{Definition of } \sigma^{-1}\rho\sigma \\
\Longleftrightarrow & \sigma^{-1}\rho\sigma \in \mathrm{Aut}_{\mathbb{E}}(\mathbb{F}) & - & \text{Definition of } \mathrm{Aut}_{\mathbb{E}}(\mathbb{F}) \\
\Longleftrightarrow & \rho \in \sigma \mathrm{Aut}_{\mathbb{E}}(\mathbb{F}) \sigma^{-1} & - & 2.4.12(c)
\end{array}$$

□

Lemma 4.5.16. [**char normal extension**] *Let $\mathbb{K} \leq \mathbb{F}$ be a Galois extension and $\mathbb{E}$ an intermediate field of $\mathbb{K} \leq \mathbb{F}$. The following are equivalent:*

(a) [**a**] *$\mathbb{K} \leq \mathbb{E}$ is normal.*

(b) [**b**] *$\mathbb{K} \leq \mathbb{E}$ is Galois.*

(c) [**c**] *$\mathbb{E}$ is invariant under $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$, that is $\sigma(\mathbb{E}) = \mathbb{E}$ for all $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$.*

Proof. (a) $\Longrightarrow$ (b): Suppose $\mathbb{K} \leq \mathbb{E}$ is normal. Since $\mathbb{K} \leq \mathbb{F}$ is separable, 4.4.3(d) implies that $\mathbb{K} \leq \mathbb{E}$ is separable. Since $\mathbb{K} \leq \mathbb{F}$ is finite, 4.1.23 implies that $\mathbb{K} \leq \mathbb{E}$ is finite. Thus $\mathbb{K} \leq \mathbb{E}$ is Galois.

(b) $\Longrightarrow$ (c): Suppose $\mathbb{K} \leq \mathbb{E}$ is Galois. Let $a \in \mathbb{E}$ and $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. By 4.5.7 $\sigma(a)$ is a root of m_a. Since $\mathbb{K} \leq \mathbb{E}$ is normal, m_a splits over $\mathbb{E}$. Hence all roots of m_a are contained in $\mathbb{E}$ and so $\sigma(a) \in \mathbb{E}$. Thus $\sigma(\mathbb{E}) \subseteq \mathbb{E}$ and also $\sigma^{-1}(\mathbb{E}) \subseteq \mathbb{E}$. Therefore $\mathbb{E} \subseteq \sigma(\mathbb{E})$ and $\sigma(\mathbb{E}) = \mathbb{E}$.

(c) $\Longrightarrow$ (a): Suppose that $\mathbb{E}$ is invariant under $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ and let $a \in \mathbb{E}$. Put $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. By 4.5.14 $\mathbb{K} = \mathrm{Fix}_{\mathbb{F}}(G)$ and G is finite. So by 4.5.11 m_a splits over $\mathbb{F}$ and if b is a root of m_a, then $b = \sigma(a)$ for some $\sigma \in G$. Since $\mathbb{E}$ is invariant under $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$, $b = \sigma(a) \in \mathbb{E}$. So m_a splits over $\mathbb{E}$ and $\mathbb{K} \leq \mathbb{E}$ is normal. □

Theorem 4.5.17 (Fundamental Theorem of Galois Theory)**.** [**ftg**] *Let $\mathbb{K} \leq \mathbb{F}$ be a Galois extension. Let $\mathbb{E}$ be an intermediate field of $\mathbb{K} \leq \mathbb{F}$ and $G \leq \mathrm{Aut}_{\mathbb{K}}(K)$.*

(a) [**e**] *$\mathbb{E} \leq \mathbb{F}$ is Galois.*

(b) [**a**] *The map*

$$\mathcal{G} : \quad \mathbb{E} \to \mathrm{Aut}_{\mathbb{E}}(\mathbb{F})$$

is a inclusion reversing bijection between to intermediate fields of $\mathbb{K} \leq \mathbb{F}$ and the subgroups of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. The inverse of $\mathcal{G}$ is given by

$$\mathcal{F} : \quad G \to \mathrm{Fix}_{\mathbb{F}}(G).$$

(c) [**b**] *$|G| = \dim_{\mathrm{Fix}_{\mathbb{F}}(G)} \mathbb{F}$ and $\dim_{\mathbb{E}} \mathbb{F} = |\mathrm{Aut}_{\mathbb{E}}(\mathbb{F})|$.*

(d) [**c**] *$\mathbb{K} \leq \mathbb{E}$ is normal if and only if $\mathrm{Aut}_{\mathbb{E}}(\mathbb{F})$ is normal in $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$.*

(e) [**d**] *If $\mathbb{K} \leq \mathbb{E}$ is normal, then the map*

$$\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})/\mathrm{Aut}_{\mathbb{E}}(\mathbb{F}) \to \mathrm{Aut}_{\mathbb{K}}(\mathbb{E}), \quad \sigma\mathrm{Aut}_{\mathbb{E}}(\mathbb{F}) \to \sigma|_{\mathbb{E}}$$

is a well-defined isomorphism of groups.

Proof. (a) Since $\mathbb{F}$ is the splitting field of a separable polynomial f over $\mathbb{K}$, $\mathbb{F}$ is also the splitting field of f over $\mathbb{E}$. By 4.4.3(b), f is separable over $\mathbb{E}$ and so

(*) $\mathbb{F}$ is the splitting field of a separable polynomial over E.

Thus by 4.5.14 $\mathbb{E} \leq \mathbb{F}$ is Galois.

(b) We will show that the two maps are inverses to each other. By (a) and 4.5.14

$$\text{Fix}_{\mathbb{F}}(\text{Aut}_{\mathbb{E}}(\mathbb{F})) = \mathbb{E}, \text{ that is } \mathcal{F}(\mathcal{G}(\mathbb{E})) = \mathbb{E} \tag{1}$$

Put $\mathbb{L} = \text{Fix}_{\mathbb{F}}(G)$. Then $G \leq \text{Aut}_{\mathbb{L}}(\mathbb{F})$. By (*) applied to $\mathbb{L}$ in place of $\mathbb{E}$, $\mathbb{F}$ is the splitting field of a separable polynomial over $\mathbb{L}$. So we can apply 4.5.8 and get

$$|\text{Aut}_{\mathbb{L}}(\mathbb{F})| \overset{4.5.8}{=} \dim_{\mathbb{L}} \mathbb{F} \overset{4.5.10}{\leq} |G| \leq |\text{Aut}_{\mathbb{L}}(\mathbb{F})|, \tag{2}$$

It follows that equality holds everywhere in (2). In particular, $|G| = |\text{Aut}_{\mathbb{L}}(\mathbb{F})|$ and $G = \text{Aut}_{\mathbb{L}}(\mathbb{F})$, that is

$$\text{Aut}_{\text{Fix}_{\mathbb{F}}(G)}(\mathbb{F}) = G, \text{ that is } \mathcal{G}(\mathcal{F}(G)) = G \tag{3}$$

By (1) and (3) $\mathcal{G}$ and $\mathcal{F}$ are inverse to each other. If $\mathbb{D}$ is a field with $\mathbb{E} \leq \mathbb{D} \leq \mathbb{F}$, then clearly $\text{Aut}_{\mathbb{D}}(\mathbb{K}) \subseteq \text{Aut}_{\mathbb{E}}(\mathbb{F})$ and so $\mathcal{G}$ is inclusion reversing.

(c) Since equality holds in (2), $\dim_{\mathbb{L}} \mathbb{F} = |G|$ and the first statement in (c) holds. Put $H = \text{Aut}_{\mathbb{E}}(\mathbb{F})$. By (b), $\mathbb{E} = \text{Fix}_{\mathbb{F}}(H)$ and so the first statement in (c) applies to H in place of G gibes the second statement in (c).

(d) We have

$$\begin{array}{rccc} & \mathbb{K} \leq \mathbb{E} \text{ is normal} & & \\ \iff & \sigma(\mathbb{E}) = \mathbb{E} \text{ for all } \sigma \in \text{Aut}_{\mathbb{K}}(\mathbb{F}) & - & 4.5.16 \\ \iff & \text{Aut}_{\sigma(\mathbb{E})}(\mathbb{F}) = \text{Aut}_{\mathbb{E}}(\mathbb{F}) \text{ for all } \sigma \in \text{Aut}_{\mathbb{K}}(\mathbb{F}) & - & (b) \\ \iff & \sigma\text{Aut}_{\mathbb{E}}(\mathbb{F})\sigma^{-1} = \text{Aut}_{\mathbb{E}}(\mathbb{F}) \text{ for all } \sigma \in \text{Aut}_{\mathbb{K}}(\mathbb{F}) & - & 4.5.15 \\ \iff & \text{Aut}_{\mathbb{E}}(\mathbb{F}) \trianglelefteq \text{Aut}_{\mathbb{K}}(\mathbb{F}) & & \end{array}$$

(e) Since $\mathbb{K} \leq \mathbb{E}$ is normal 4.5.16 implies that $\mathbb{E}$ is $\text{Aut}_{\mathbb{K}}(\mathbb{F})$-invariant. So by 2.7.8(d) $\text{Aut}_{\mathbb{K}}(\mathbb{F})$ acts on $\mathbb{E}$. The homomorphism associated to this action is

$$\alpha : \text{Aut}_{\mathbb{K}}(\mathbb{F}) \to \text{Sym}(\mathbb{E}), \sigma \to \sigma \mid_{\mathbb{E}} .$$

In particular, $\sigma|_{\mathbb{E}}$ is a bijection from $\mathbb{E}$ to $\mathbb{E}$. Clearly $\sigma|_{\mathbb{E}}$ is a homomorphism. Thus $\sigma|_{\mathbb{E}}$ is a field isomorphism. Moreover, $(\sigma|_{\mathbb{E}})|_{\mathbb{K}} = \sigma|_{\mathbb{K}} = \text{id}_{\mathbb{K}}$ and so $\sigma|_{\mathbb{E}} \in \text{Aut}_{\mathbb{K}}(\mathbb{F})$. Thus

$\operatorname{Im}\alpha \subseteq \operatorname{Aut}_{\mathbb{E}}(\mathbb{F})$. Let $\rho \in \operatorname{Aut}_{\mathbb{E}}(\mathbb{F})$. By (*) $\mathbb{F}$ is splitting field of some polynomial over $\mathbb{E}$. Then by 4.3.6 (applied with $\mathbb{K}_1 = \mathbb{K}_2 = \mathbb{E}$, $\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{F}$, $f_1 = f_2 = f$ and $\sigma = \rho$) there exists a field isomorphism $\check{\rho} : \mathbb{F} \to \mathbb{F}$ with $\check{\rho}|_{\mathbb{E}} = \rho$. Since $\check{\rho}|_{\mathbb{K}} = \rho|_{\mathbb{E}} = \mathrm{id}_{\mathbb{K}}$, $\check{\rho} \in \operatorname{Aut}_{\mathbb{K}}(\mathbb{F})$. Then $\rho = \alpha(\check{\rho})$ and so $\rho \in \operatorname{Im}\alpha$ and $\operatorname{Im}\alpha = \operatorname{Aut}_{\mathbb{K}}(\mathbb{E})$.

Note that $\sigma \in \ker\alpha$ if and only if $\alpha|_{\mathbb{E}} = \mathrm{id}_{\mathbb{E}}$. So $\ker\alpha = \operatorname{Aut}_{\mathbb{E}}(\mathbb{F})$. Hence (e) follows from the First Isomorphism Theorem. □

Example 4.5.18. [**ex:ftg**] Let $\mathbb{F}$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}$ in $\mathbb{C}$. Put

$$\xi = e^{\frac{2\pi}{3}i}, \quad a = \sqrt[3]{2}, \quad b = \xi\sqrt[3]{2}, \quad \text{and } c = \xi^2\sqrt[3]{2}.$$

By Example 4.5.9

$$\mathbb{F} = \mathbb{Q}[a,\xi], \quad \dim_{\mathbb{Q}}\mathbb{F} = 6 \text{ and } \operatorname{Aut}_{\mathbb{Q}}(\mathbb{F}) \cong \operatorname{Sym}(R) \cong \operatorname{Sym}(3),$$

where $R = \{a,b,c\}$ is the set of roots of $x^3 - 2$. For $(x_1,\ldots,x_n)$ a cycle in $\operatorname{Sym}(R)$ let $\sigma_{x_1\ldots x_n}$ be the corresponding element in $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{F})$. So for example σ_{ab} is the unique element of $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{F})$ with $\sigma_{ab}(a) = b, \sigma_{ab}(b) = a$ and $\sigma_{ab}(c) = c$. Then by Example 2.6.13 the subgroup of $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{F})$ are

$$\{\mathrm{id}_{\mathbb{F}}\}, \langle\sigma_{ab}\rangle, \langle\sigma_{ac}\rangle, \langle\sigma_{bc}\rangle, \langle\sigma_{ac}\rangle, \langle\sigma_{abc}\rangle, \operatorname{Aut}_{\mathbb{Q}}(\mathbb{F})$$

We now compute the corresponding intermediate fields:

Observe that

$$\operatorname{Fix}_{\mathbb{F}}(\{\mathrm{id}_{\mathbb{F}}\}) = \mathbb{F}.$$

$\langle\sigma_{ab}\rangle$ has order 2. Hence by the FTGT 4.5.17(c), $\dim_{\operatorname{Fix}_{\mathbb{F}}(\langle\sigma_{ab}\rangle)}\mathbb{F} = 2$. Since $\dim_{\mathbb{Q}}\mathbb{F} = 6$, 4.2.8 implies that $\dim_{\mathbb{Q}}\operatorname{Fix}_{\mathbb{F}}(\langle\sigma_{ab}\rangle) = 3$. Since c is fixed by σ_{ab} and $\dim_{\mathbb{Q}}\mathbb{Q}[c] = \deg p_c = \deg(x^3 - 2) = 3$ we have

$$\operatorname{Fix}_{\mathbb{F}}(\langle\sigma_{ab}\rangle) = \mathbb{Q}[c] = \mathbb{Q}\left[\xi^2\sqrt[3]{2}\right].$$

Similarly,

$$\operatorname{Fix}_{\mathbb{F}}(\langle\sigma_{ac}\rangle) = \mathbb{Q}[b] = \mathbb{Q}\left[\xi\sqrt[3]{2}\right]$$

and

$$\operatorname{Fix}_{\mathbb{F}}(\langle\sigma_{bc}\rangle) = \mathbb{Q}[a] = \mathbb{Q}\left[\sqrt[3]{2}\right].$$

Note that $\dim_{\mathbb{Q}}\mathbb{Q}[\xi] = 2$ and so $\dim_{\mathbb{Q}[\xi]}\mathbb{F} = 3$. Hence $|\operatorname{Aut}_{\mathbb{Q}[\xi]}(\mathbb{F})| = 3$. Since $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{F})$ has a unique subgroup of order 3 we get $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{F}) = \langle\sigma_{abc}\rangle$ and so

$$\operatorname{Fix}_{\mathbb{F}}(\langle\sigma_{abc}\rangle) = \mathbb{Q}[\xi].$$

Let us verify that σ_{abc} indeed fixes ξ. From $b = a\xi$ we have $\xi = a^{-1}b$ and so

$$\sigma_{abc}(\xi) = \sigma_{abc}(a^{-1}b) = (\sigma_{abc}(a))^{-1}\sigma_{abc}(b) = b^{-1}c = \xi.$$

Finally by 4.5.14

$$\mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{Q}}(\mathbb{F})) = \mathbb{Q}.$$

Note that the roots of x^2+x+1 are ξ and ξ^2. So $\mathbb{Q}[\xi]$ is the splitting field of x^2+x+1 and $\mathbb{Q} \leq \mathbb{Q}[\xi]$ is a normal extension, corresponding to the fact that $\langle \sigma_{abc} \rangle$ is normal in $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$.

Since $m_a = x^3 - 2$ and neither b or c are in $\mathbb{Q}[a]$, m_a does not split over $\mathbb{Q}[a]$. Hence $\mathbb{Q} \leq \mathbb{Q}[a]$ is not normal, corresponding to the fact that $\langle \sigma_{bc} \rangle$ is not normal in $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$.

4.6 Fundamental theorem of Algebra

Definition 4.6.1. [**def:algebraic closed**] *Let $\mathbb{K}$ be a field. $\mathbb{K}$ is called algebraically closed if every polynomial in $\mathbb{K}[x]$ splits over $\mathbb{K}$.*

The goal of this section is to show that $\mathbb{C}$ is algebraically closed. This proof is based on the following properties of $\mathbb{R}$ and $\mathbb{C}$:

Lemma 4.6.2. [**real props**]

(a) [**a**] *Let $f \in \mathbb{R}[x]$ be a polynomial of odd degree. Then f has root in $\mathbb{R}$.*

(b) [**b**] *Let $u \in \mathbb{C}$. Then $u = v^2$ for some $v \in \mathbb{C}$.*

Proof. (a) This follows from the Intermediate Value Theorem from Calculus.

(b) Let $u = a + ib$ with $a, b \in \mathbb{R}$. Put

$$c := \sqrt{\frac{1}{2}\left(a + \sqrt{a^2+b^2}\right)}, \quad d := \mathrm{sgn}(b)\sqrt{\frac{1}{2}\left(-a + \sqrt{a^2+b^2}\right)} \text{ and } v := c + di.$$

Then

$$v^2 = (c+di)^2 = (c^2 - d^2) + 2cd$$

$$c^2 - d^2 = \frac{1}{2}\big((a + \sqrt{a^2+b^2}) - (-a + \sqrt{a^2+b^2})\big) = \frac{1}{2}2a = a$$

and

$$\begin{aligned} 2cd &= \mathrm{sgn}(b)2\sqrt{\tfrac{1}{2}}^2\sqrt{\left(a + \sqrt{a^2+b^2}\right)\left(-a + \sqrt{a^2+b^2}\right)} \\ &= \mathrm{sgn}(b)\sqrt{-a^2 + (a^2+b^2)} = \mathrm{sgn}(b)|b| = b \end{aligned}$$

So indeed $v^2 = u$. □

Corollary 4.6.3. [**real extensions**]

(a) [**a**] *Let $\mathbb{R} \leq \mathbb{F}$ be a finite field extension with* $\dim_{\mathbb{R}} \mathbb{F}$ *odd. Then $\mathbb{R} = \mathbb{F}$.*

(b) [**b**] *There does not exist a field extension $\mathbb{C} \leq \mathbb{F}$ with* $\dim_{\mathbb{C}} \mathbb{F} = 2$*.*

Proof. (a) Let $a \in \mathbb{K}$. Then $\mathbb{R}[a]$ is a subfield of $\mathbb{K}$ and so by the dimension formula 4.2.8

$$\dim_{\mathbb{R}} \mathbb{F} = \dim_{\mathbb{R}} \mathbb{R}[a] \cdot \dim_{\mathbb{R}[a]} \mathbb{F}$$

Since $\dim_{\mathbb{R}} \mathbb{F}$ is odd, we conclude that $\dim_{\mathbb{R}} \mathbb{R}[a]$ is odd. Hence by 4.2.16 the minimal polynomial m_a for a over $\mathbb{R}$ has odd degree (namely $\dim_{\mathbb{R}} \mathbb{R}[a]$)). Thus by 4.6.2(a), m_a has a root $b \in \mathbb{R}$. Since m_a is irreducible over $\mathbb{R}$ we get $m_a = x - b$ and $a = b \in \mathbb{R}$. Since this holds for all $a \in \mathbb{F}$, $\mathbb{F} = \mathbb{R}$.

(b) Suppose for a contradiction that $\mathbb{C} \leq \mathbb{F}$ is a field extension with $\dim_{\mathbb{F}} \mathbb{C} = 2$. Let $a \in \mathbb{F} \setminus \mathbb{C}$. Then $\mathbb{F} = \mathbb{C}[a]$ and so $m_a^{\mathbb{C}}$ has degree two. By 4.6.2(b) and the quadratic formula, $m_a^{\mathbb{C}}$ has a root in $\mathbb{C}$, a contradiction since $m_a^{\mathbb{C}}$ is irreducible. □

Definition 4.6.4. [**def:derivative**] *Let $\mathbb{K}$ be a field and $f = \sum_{i=0}^{n} k_i x^i \in \mathbb{K}[x]$. then $f' := \sum_{i=1}^{n} i k_i x^{i-1}$. f' is called the* derivative *of f.*

Lemma 4.6.5. [**diru**] *Let $\mathbb{K}$ be a field and $f, g \in \mathbb{K}[x]$*

(a) [**a**] *The derivative function $\mathbb{K}[x] \to \mathbb{K}[x], f \to f'$ is $\mathbb{K}$-linear.*

(b) [**c**] *$(fg)' = f'g + fg'$.*

Proof. (a) is obvious. (b) By (a) we may assume that $f = x^m$ and $g = x^n$

$$(fg)' = (x^{n+m})' = (n+m)x^{n+m-1}$$

$$f'g + fg' = mx^{m-1}x^n + x^m nsx^{n-1} = (n+m)x^{m+n-1}$$

Thus (b) holds. □

Lemma 4.6.6. [**mroots**] *Let $\mathbb{K}$ be a field, $f \in \mathbb{K}[x]$ with $f \neq 0_{\mathbb{K}}$ and $c \in \mathbb{K}$. Then c is a double root of f if and only if $f(c) = 0_K$ and $f'(c) = 0$.*

Proof. In both cases c is a root of f and so $f = g \cdot (x - c)$ for some $g \in \mathbb{K}[x]$. Thus $f' = g' \cdot (x - c) + g \cdot (x - c)$ and so $f'(c) = g(c)$. Thus c is a root of f' if and only if c is a root of g and if and only if c is a double root. □

Lemma 4.6.7. [**char sep**] *Let $\mathbb{K}$ be a field and f an irreducible polynomial over $\mathbb{K}$. Then f is separable if and only if $f' \neq 0_{\mathbb{K}}$.*

Proof. Without loss f is monic. Let $\mathbb{E}$ be a splitting field of f over $\mathbb{K}$ and a a root of f in $\mathbb{E}$. Note that f is the minimal polynomial of a over $\mathbb{K}$. Then

$$\begin{array}{cccc} & a \text{ is a double root of } f & & \\ \iff & f'(a) = 0_{\mathbb{K}} & - & 4.6.6 \\ \iff & f \Big| f' \text{ in } \mathbb{K}[x] & - & 4.2.16(g) \\ \iff & f' = 0_{\mathbb{K}} & - & \deg f' < \deg f \end{array}$$

Thus f has a double root if and only if $f' = 0_{\mathbb{K}}$. □

Example 4.6.8. [**ex:char sep**] Let y be an indeterminate over $\mathbb{Z}_2$. Put $\mathbb{K} = \mathbb{Z}_2(y)$. By Example 4.4.2(3), $f := x^2 - y^2$ is irreducible over $\mathbb{K}$. Note that $f' = 2x = 0_{\mathbb{Z}_2}$. So by 4.6.7 $x^2 - y^2$ is not separable over $\mathbb{K}$, which of course we already proved in 4.4.2(3) by showing that y is the only root of $x^2 - t^2$.

Definition 4.6.9. [**def:chr**] *Let R be a ring. If there exists $n \in \mathbb{Z}^+$ with $nr = 0_R$ for all $n \in R$, then* $\operatorname{char} R$ *is the minimal such that n. Otherwise* $\operatorname{char} R = 0$. $\operatorname{char} R$ *is called the* characteristic *of R.*

Lemma 4.6.10. [**basic chr**] *Let R be a ring with identity and put $p = \operatorname{char} \mathbb{F}$.*

(a) [**a**] *The map $\alpha : \mathbb{Z} \to R, n \to n1_R$ is a ring homomorphism with* $\ker \alpha = p\mathbb{Z}$.

(b) [**d**] *Let $n \in \mathbb{Z}$. Then $n1_R = 0_R$ if and only if $p \mid n$ in $\mathbb{Z}$.*

(c) [**b**] *If R is an integral domain, then $p = 0$ or p is prime integer.*

(d) [**c**] *If R is an integral domain, $n \in \mathbb{Z}$ and $r \in R^\sharp$, then $nr = 0_R$ if and only if $p \mid n$ in $\mathbb{Z}$.*

Proof. (a) By Lemma B(e) on the Solutions of Homework 2, α is ring homomorphism. Let $n \in \mathbb{Z}$. If $nr = 0_R$ for all $r \in R$, then $n1_R = 0_R$. If $n1_R = 0_R$, then $nr = n(1_R r) = (n1_R)r = 0_R r = 0_R$. So $n \in \ker \alpha$ if and only if $n1_R = 0_R$ and if and only if $nr = 0_R$ for all $r \in R$. Since $\ker \alpha$ is an ideal $\mathbb{Z}$, $\ker \alpha = m\mathbb{Z}$ for some $m \in \mathbb{N}$. If $m = 0$, then there does not exists $n \in \mathbb{Z}^+$ with $nr = 0_R$ for all $r \in R$ and so $\operatorname{char} \mathbb{R} = 0$. If $m \neq 0$, then m is the smallest positive integer in $\ker \alpha$ and again $m = \operatorname{char} R$.

(b) follows immediately from (a).

(c) By (a) and the First Isomorphism Theorem of Rings, $\mathbb{Z}_p$ is isomorphic to subring of R. Since R is an integral domain, we conclude that $\mathbb{Z}_p$ is an integral domain. Hence by Example 3.2.4(3), $p = 0$ or p is a prime.

(d) We have

$$\begin{aligned} & nr = 0_R \\ \iff\ & n(1_R r) = 0_R \\ \iff\ & (n1_R)r = 0_R \\ \iff\ & n1_R = 0_R \quad - \quad r \neq 0_R, R \text{ is an Integral domain} \\ \iff\ & p \mid n \text{ in } \mathbb{Z} \quad - \quad (a) \end{aligned}$$

□

Corollary 4.6.11. [**sep chr 0**] *Let $\mathbb{K}$ be a field with* $\operatorname{char}\mathbb{K} = 0$.

(a) [**a**] *Let $f \in \mathbb{K}[x]$. Then $f' = 0_{\mathbb{K}}$ if and only if $f \in \mathbb{K}$.*

(b) [**b**] *All polynomials over $\mathbb{K}$ are separable.*

Proof. (a) If $f \in \mathbb{K}$ then clearly $f' = 0_{\mathbb{K}}$. So suppose $f \notin \mathbb{K}$. Then $f = \sum_{i=0}^n k_i x^i \in \mathbb{K}[x]$ with $k_n \neq 0$ and $n \geq 1$. By 4.6.10(d), $na_n \neq 0_{\mathbb{K}}$ and so $f' = \sum_{i=1}^n i a_i x^{i-1}$ has degree $n-1$. Thus $f' \neq 0_{\mathbb{K}}$

(b) Let $f \in \mathbb{K}[z]$ be irreducible. Then $f \notin \mathbb{K}$ and by (a), $f' \neq 0_{\mathbb{K}}$. Thus by 4.6.7, f is separable. So all irreducible polynomial over $\mathbb{K}$. By definition of separable an arbitrary polynomial is separable, if all its irreducible divisors are separable. So (b) holds. □

Theorem 4.6.12 (Fundamental Theorem of Algebra)**.** [**fta**] $\mathbb{C}$ *is algebraically closed.*

Proof. Let $f \in \mathbb{C}[x]$ and let $\mathbb{D}$ be a splitting field of f over $\mathbb{C}$. We need to show that $\mathbb{D} = \mathbb{C}$. Note that $\mathbb{R} \leq \mathbb{D}$ is finite and so there exists a $\mathbb{R}$-basis $(b_1, b_2, \ldots, b_n)$ for $\mathbb{D}$. It follows that $\mathbb{D} = \mathbb{R}[b_1, b_2, \ldots, b_n]$. Let m_i be the minimal polynomial of b_i over $\mathbb{R}$ and put $g = \prod_{i=1}^n m_i$. Let $\mathbb{F}$ be a splitting field of g over $\mathbb{D}$. We claim that $\mathbb{F}$ is also a splitting field for g over $\mathbb{R}$. Indeed let U be the set of roots of g in $\mathbb{F}$. Then $\mathbb{F} = \mathbb{D}[U]$. Since $b_i \in U$ for all i we conclude that $\mathbb{D} = \mathbb{R}[b_1, \ldots, b_n] \subseteq \mathbb{R}[U]$. Thus both $\mathbb{D}$ and U are contained in $\mathbb{R}[U]$ and so $\mathbb{F} = \mathbb{D}[U] \leq \mathbb{R}[U] \leq \mathbb{F}$. Hence $\mathbb{F} = \mathbb{R}[U]$ and $\mathbb{F}$ is a splitting field of g over $\mathbb{R}$. By 4.6.11, g is separable over $\mathbb{R}$ and so by 4.5.14, $\mathbb{R} \leq \mathbb{F}$ is Galois. Let $G = \operatorname{Aut}_{\mathbb{R}}(\mathbb{F})$ and let S be a Sylow 2-subgroup of G. Put $\mathbb{E} = \operatorname{Fix}_{\mathbb{F}}(S)$. By the Fundamental Theorem of Galois Theory 4.5.17 $\dim_{\mathbb{E}} \mathbb{F} = |S|$ and so by the dimension formula,

$$\dim_{\mathbb{R}} \mathbb{E} = \frac{\dim_{\mathbb{R}} \mathbb{F}}{\dim_{\mathbb{E}} \mathbb{F}} = \frac{|G|}{|S|}$$

By Sylow's Theorem 2.8.10 $\frac{|G|}{|S|}$ is odd. Hence $\dim_{\mathbb{R}} \mathbb{E}$ is odd and by 4.6.3(a), $\mathbb{R} = \mathbb{E}$. Hence by the FTGT,

$$S = \operatorname{Aut}_{\mathbb{E}}(F) = \operatorname{Aut}_{\mathbb{R}}(\mathbb{F}) = G$$

Hence G is a 2-group. Put $H = \mathrm{Aut}_{\mathbb{C}}(\mathbb{F})$. Suppose for a contradiction that $|H| \neq \{\mathrm{id}_{\mathbb{F}}\}$. Then by 2.8.8, H has a subgroup P of order $\frac{|H|}{2}$. Put $\mathbb{L} = \mathrm{Fix}_{\mathbb{F}}(P)$. By the FTGT and the dimension formula

$$\dim_{\mathbb{C}}\ \mathbb{L} = \frac{|H|}{|P|} = 2,$$

a contradiction to 4.6.3(b). Thus $H = \{id_{\mathbb{F}}\}$ and so

$$\mathbb{C} = \mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{C}}(\mathbb{F}) = \mathbb{F}.$$

Since $\mathbb{C} \leq \mathrm{D} \leq \mathbb{F}$ also $\mathbb{C} = \mathrm{D}$ and so $\mathbb{C}$ is algebraically closed. □

4.7 Geometric Construction

Definition 4.7.1. [**def:plane**]

(a) [**a**] *$E := \mathbb{R}^2$. E is called the* plane *and the elements of E are called* points.

(b) [**b**] *For $e = (a, b) \in E$, $||e|| := \sqrt{a^2 + b^2}$. $\leq (e)$ is called the length of e.*

(c) [**c**] *For $\in \mathbb{E}$* $\mathrm{dist}(e, d) := ||e - d||$. $\mathrm{dist}(e, d)$ *is called the distance of d from e.*

(d) [**d**] *Let $e \in E$ and $r \in \mathbb{R}^+_0$. Put $C_r(e) = \{d \in \mathbb{R} \mid \mathrm{dist}(d, e) = r\}$. Then $C_r(e)$ is called* circle *of radius r and center e.*

(e) [**e**] *Let $a, b \in E$ with $a \neq b$. Put $L(a, b) := \{a + r(b - a) \mid r \in \mathbb{R}$. Then $L(a, b)$ is called the line through a and b.*

(f) [**f**] *Let $a, b, c \in \mathbb{E}$ with $b \neq a \neq c$. We say that the line $L(a, b)$ is perpendicular to the line $L(a, c)$, if $d_1e_1 + d_2 = 0$, where $b - a = (d_1, d_2)$ and $c - a = (e_1, e_2)$ with $d_i, e_i \in \mathbb{R}$.*

Definition 4.7.2. [**def:construction**] *Let $T \subseteq E$.*

(a) [**a**] $D^+_T := \{\mathrm{dist}(s, t) \mid s, t \in T\}$

(b) [**b**] $C_T := C_r(e) \mid e \in E, r \in D^+_T\}$.

(c) [**c**] $L_T := \{L(s, t) \mid s, t \in T \mid s \neq t$.

(d) [**d**] *T^* consists of all $s \in T$ such that there exists $A \neq B \in C_T \cup L_I$ with $s \in A \cup B$.*

(e) [**e**] *$S_0 := \{(0, 0), (0, 1)\}$ and inductively define $S_{i+1} := S_{i+1}$.*

(f) [**f**] *$S := \bigcup_{i=0}^{\infty} S_i$, $D^+ := D_S$, $\mathbb{D} := D^+_S \cup D^-_S$ and $C := C_S, L := L_S$. The elements of S are called constructable points, the elements of D constructable numbers, the elements of C constructable circles and the elements of L are called constructable lines.*

This definition can be summarized as follows: $(0,0),(0,1)$ are constructable points. Let s,t be constructable points and r non-negative constructable numbers. The the distance between s and t is a constructable number. If $s \neq t$, the line through s and t is constructable. The circle with radius r and center s is constructable. Finally the intersection points of a constructable line or circle with a distinct constructable line or circle are constructable points.

Lemma 4.7.3. [**perp line**] *Let A be a constructable point and l a constructable line. Then the unique line through A and perpendicular to l is constructable.*

Lemma 4.7.4. [**points numbers**] *A point is constructable if and only if both its coordinates are constructable. A number r in $\mathbb{R}$ is constructable if and only if $(0,r)$ is constructable.*

Lemma 4.7.5. [**const field**] *$\mathbb{D}$ is a subfield of $\mathbb{R}$ and $\sqrt{d} \in \mathbb{D}$ for all $d \in \mathbb{D}$ with $d \geq 0$.*

Lemma 4.7.6. [**quadratic extensions**] *Let $\mathbb{K}$ subfield of $\mathbb{R}$ and $(u,v) \in E$. If $(u,v) \in (\mathbb{E}^2)^*$ then $\dim_{\mathbb{E}} \mathbb{E}[u,v]] \leq 2$.*

Proof. Suppose first that $(a,b) \in \mathbb{E}^2$. The (a,b) in $F_1 \cap F_2$, there F_i is a line through two points in $\mathbb{E}^2$ or F_i is a circle with center in $\mathbb{E}^2$ and radius in $\mathbb{E}$.

Suppose first that F_1 and F_2 are both lines. The the points on $F_1 \cap F_2$ are the solutions of a system of linear equation

$$a_1x + b_1y = c_1 \text{ and } a_2x + b_2y + c_2$$

with $a_i, b_i, c_i \in \mathbb{E}$. It follows that $u, v \in \mathbb{E}$ and so $\dim_{\mathbb{E}} \mathbb{E}[u,v] = 1$

Suppose next that F_1 is line and F_2 is a circle. Then the points in $F_1 \cap F_2$ are the solution of the system of equation

$$ax + by = c \text{ and } (x-d)^2 + (y-e)^2 = f$$

with $a,b,c,d,e,f \in \mathbb{E}$ and $(a,b) \neq (0,0)$. Without loss $b \neq 0$ and so $y = (c-ax)b^{-1}$. In particular, $v \in \mathbb{E}[u]$ and $\mathbb{E}[u,v] = \mathbb{E}[u]$. Moreover, u is a root of degree two polynomial $(x-d)^2((c-ax)b^{-1}-e)^2 = f$. Thus $\dim_{\mathbb{E}} \mathbb{E}[u] \leq 2$.

Suppose finally that both F_1 and F_2 are circles. The the points on in $F_1 \cap F_2$ are the solutions of

$$(x-a)^2 + (y-b)^2 = c \text{ and } (x-d)^2 + (y-e)^2 = f$$

That is of

$$(x^2 - 2xa - 2yb + y^2 = c - a^2 - b^2 \text{ and } x^2 - 2xd - 2ye + y^2 = f - d^2 - e^2$$

Subtracting this two equations gives

$$(2d - 2a)x + (2e - 2b)y = c + d^2 + e^2 - a^2 - b^2 - f$$

Note that $(a,d) \neq (b,e)$ otherwise either $F_1 = F_2$ or $F_1 \cap F_2 = \emptyset$. So this last equation is the equation of a line L through two points in $\mathbb{E}^2$. Hence $F_1 \cap F_2 = \mathbb{F}_1 \cup L$ and we are done by the previous case. □

Lemma 4.7.7. [**subnormal series**] *Let p a positive prime integer, G a finite p-group and $H \leq G$. The there exists a chain of subgroups*

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

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

Proof. The proof is by induction on $|G| \cdot |G/H|$. If $|G/H| = 1$, then $G = H$ and the lemma holds.

So we assume that $G \neq H$. In particular, $|G| \neq 1$ and so by 2.7.29 $|\operatorname{Z}(G)| \neq 1$. Thus by 2.8.8 there exists $T \leq \operatorname{Z}(G)$ with $|T| = p$. Note that $T \trianglelefteq G$.

Suppose first $T \leq H$. Then since $|G/T| < |G|$ and $|G/T|\big/|H/T| = |G/H$ we conclude by induction that there exists a chain of subgroups

$$H/T = \overline{H_0} \trianglelefteq \overline{H_1} \trianglelefteq \overline{H_2} \ldots \trianglelefteq \overline{H_{n-1}} \trianglelefteq \overline{H_n} = G/T$$

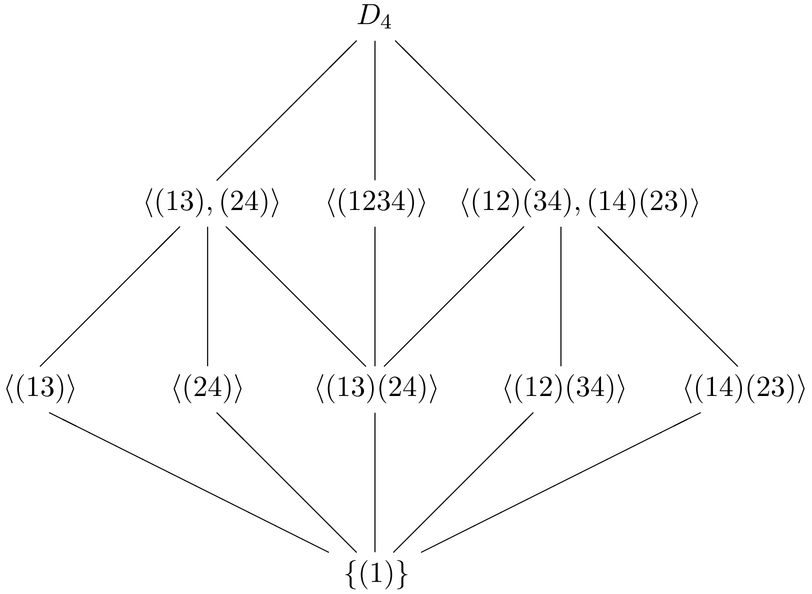
By the Correspondence Theorem 2.6.12 $\overline{H_i} = H_i/T$ for some $H_i \leq G$ and the lemma holds in this case.

Suppose next that $T \not\leq H$. Then $H \leq HT \leq G$ and $|HT/H| = |T/T \cap H| = |T| = p$. Moreover $G/HT| < |G|$ and so by induction there exists a chain of subgroups

$$HT = H_1 \trianglelefteq H_2 \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

with $|H_i/H_{i-1}| = p$ for all $2 \leq i \leq n$. Again the lemma holds. □

Example 4.7.8. [**ex:subnormal**] Let $G = D_4 = \langle (13), (12)(34) \rangle \leq \operatorname{Sym}(4)$ and $p = 2$. Since $|D_4| = 8$, D_4 is a 2-group. If $A \leq B \leq D_4$ with $|A/B| = 2$, then by $A \trianglelefteq B$ since A and $B \setminus A$ are the left cosets and also the right cosets of A in B.



Theorem 4.7.9. [**char constructable**] *Let $a \in \mathbb{R}$ and $\mathbb{K}$ a subfield of $\mathbb{D}$. The the following are equivalent.*

(a) [**a**] *a is constructable*

(b) [**b**] *There exist $n \in \mathbb{N}$ and finite sequence of field extensions*

$$\mathbb{K} = \mathbb{K}_0 \leq \mathbb{K}_1 \leq \mathbb{K}_2 \leq \mathbb{K}_n \leq \mathbb{R}$$

with $\dim_{\mathbb{K}_{i-1}} \mathbb{K}_i = 2$ for all $1 \leq i \leq n$ and $a \in \mathbb{K}_n$.

(c) [**e**] *a is algebraic over $\mathbb{K}$ and if $\mathbb{F}$ is the splitting field for $m_a^{\mathbb{K}}$ over $\mathbb{K}$ in $\mathbb{C}$, then $\dim_{\mathbb{K}} \mathbb{F} = 2^n$ for some $n \in \mathbb{N}$.*

(d) [**d**] *a is algebraic over $\mathbb{K}$ and if $\mathbb{F}$ is the splitting field for $m_a^{\mathbb{K}}$ over $\mathbb{K}$ in $\mathbb{C}$, then $\mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ is a 2-group.*

(e) [**c**] *There exists $n \in \mathbb{N}$ and a finite sequence of field extensions*

$$\mathbb{K} = \mathbb{K}_0 \leq \mathbb{K}_1 \leq \mathbb{K}_2 \leq \mathbb{K}_n = \mathbb{K}[a]$$

with $\dim_{\mathbb{K}_{i-1}} \mathbb{K}_i = 2$ for all $1 \leq i \leq n$.

Proof. (a) $\Longrightarrow$ (b): Suppose a is constructable. Then $(0, a)$ is constructable. Hence there exists a finite sequence of elements $e_0 = (0,0), e_1 = (1,0), e_2, e_3 \ldots e_n = (0,a)$ in R^2 such that for each $2 \leq j \leq n$ a_j there exists $F_1(j), F_2(j)$ such that $e_j \in F_1(j) \cup F_2(j)$ and $F_i(j)$

is either a line through two points of $E_{j-1} := \{e_0, e_1, \ldots, e_{j-1}$ or a circle with center in E_j and radius the distance of between two points of E_{j-1}. Let $e_i = (a_i, b_i)$ and define $\mathbb{K}_0 = \mathbb{K}$ and for $i > 0$, $\mathbb{K}_i = \mathbb{K}_{i=1}[a_i, b_i]$. Then by 4.7.6 $\dim_{\mathbb{K}_{j-1}} \mathbb{K}_j \leq 2$. Removing all $\mathbb{K}_i$ with $\mathbb{K}_i = \mathbb{K}_{i-1}$ we see that (b) holds.

(b) $\Longrightarrow$ (c): Suppose (b) holds. Let $a_i \in \mathbb{K}_i \setminus \mathbb{K}_i i - 1$. Then $\mathbb{K}_i = \mathbb{K}_i[i-1][a_i]$. Put $f = \prod_{j=1}^n m_{a_j}^Q$ and let $\mathbb{E}$ be a splitting field of f over $\mathbb{K}$ in $\mathbb{C}$. Note that $\mathbb{K} \leq \mathbb{E}$ and $a_i \in \mathbb{E}$ so by induction $\mathbb{K}_i = \mathbb{K}_{i-1}[a_i] \leq \mathbb{E}$ for all $1 \leq i \leq n$. By 4.6.11, f is separable and so by 4.5.14 $\mathbb{K} \leq \mathbb{E}$ is Galois. Put $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$ and let $H = \langle T \leq G \mid |T| \text{ is an odd} prime\}$. Then H is a normal subgroup of G. Put $\mathbb{L} = \mathrm{Fix}_{\mathbb{E}}(H)$. We we show by induction on i that $\mathbb{K}_i \leq \mathbb{L}$ for all $0 \leq i \leq n$. For $n = 0$, $\mathbb{K}_0 = \mathbb{K} \leq \mathbb{L}$. Suppose now that $i > 0$ and $\mathbb{K}_{i-1} \leq \mathbb{E}$. Since $\dim_{\mathbb{K}_{i-1}} \mathbb{K}_i = 2$, $a_i$is the root of a polynomial of degree 2 over $\mathbb{K}_{i-1}$. Thus $\deg m_{a_i}^{\mathbb{L}} = 2$. let R be the set roots of $m_{a_i}^{\mathbb{L}}$ in $\mathbb{E}$. Then $|R| \leq 2$. and by 4.5.7 H acts R. Let $T \leq G$ such that $|T| = p$, p an odd prime. The all the non-trivial orbits of T on R have length p. But $p \geq |R|$ and so T acts trivially on R. Thus $a_i \in \mathrm{Fix}_{\mathbb{E}}(T)$ for all such T. Thus $a_i \in \mathbb{L}$ and $\mathbb{K}_i = \mathbb{K}_{i-1}[a_i] \leq \mathbb{L}$.

Hence $a_i \in \mathbb{L}$ for all $1 \leq i \leq n$. Note that H is a normal subgroup of G and by the FTGT 4.5.17(d), $\mathbb{K} \leq \mathbb{L}$ is normal. Thus each $m^Q m_{a_i}$ splits over $\mathbb{L}$. Hence f splits over $\mathbb{L}$ and since $\mathbb{L} \leq \mathbb{E}$ and $\mathbb{E}$ is a splitting field for f over $\mathbb{K}$ we conclude that $\mathbb{L} = \mathbb{E}$. Hence $H = \{id_{\mathbb{E}}\}$. So G contains no subgroup of odd prime order. Thus by 2.8.8 implies that G is a 2-group. The FTGT 4.5.17 shows that $\dim_{\mathbb{K}} \mathbb{F} = |G| = 2^k$ for some $k \in \mathbb{N}$. Note that $a \in \mathbb{K}_n \leq q\mathbb{E}$ and since $\mathbb{K} \leq \mathbb{E}$ is normal, $m_a^{\mathbb{K}}$ splits over $\mathbb{E}$. Thus $\mathbb{F} \leq \mathbb{E}$ and by the dimension formula 4.2.8 $\dim_{\mathbb{K}} \mathbb{F}$ divides $\dim_{\mathbb{K}} \mathbb{E}$. So (c) holds.

For the remaining parts note that by 4.6.11 $m_a^{\mathbb{K}}$ is separable and so by 4.5.14 $\mathbb{K} \leq \mathbb{F}$ is Galois.

(c) $\Longrightarrow$ (d): This follows immediately immediately from FTGT.

(d) $\Longrightarrow$ (e): Put $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ and $H = \mathrm{Aut}_{\mathbb{K}[a]}(\mathbb{F})$. Then G is a 2-group and so by 4.7.7 there exists a chain of subgroups

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

with $|H_i/H_{i-1}| = 1$ for all $1 \leq i \leq n$. Put $\mathbb{K}_i = \mathrm{Fix}_{\mathbb{F}}(H_{n-i}$. Then by the FTGT 4.5.17, $\mathbb{K}_0 = \mathrm{Fix}_{\mathbb{F}}(H_n) = \mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{F}) = \mathbb{K}$, $\mathbb{K}_n = \mathrm{Fix}_{\mathbb{F}}(H_0) = \mathrm{Fix}_{\mathbb{F}}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[a]) = \mathbb{K}[a]$.

$$\mathbb{K} = \mathbb{K}_0 \leq \mathbb{K}_1 \leq \ldots \mathbb{K}_{n-1} \leq \mathbb{K}_n = \mathbb{F}$$

and $\dim_{\mathbb{K}_{i-1}} \mathbb{K}_i = |H_{n-i+1}/H_{n-i}| = 2$. So (e) holds.

(e) $\Longrightarrow$ (a): We will show by induction on i that all elements in $\mathbb{K}_i$ are constructable.

By assumption $\mathbb{K}_0 = \mathbb{K} \leq \mathbb{D}$. Suppose now that $0 \leq i < n$ and $\mathbb{K}_i \leq \mathbb{D}$. let $a \in \mathbb{K}_{i+1}$. If $a \in \mathbb{K}_i$, then $a \in \mathbb{D}$. If $a \notin \mathbb{K}_i$, then since $\dim_{\mathbb{K}_i} \mathbb{K}_{i+1} = 2$, $m_a^{\mathbb{K}_i}$ has degree 2. So a is the root of polynomial of degree two with coefficients in $\mathbb{K}_i$. By the quadratic formula, $a = b + c\sqrt{d}$ for some $b, c, d \in \mathbb{K}_i$. Since $b, c, d \in \mathbb{D}$ we conclude from 4.7.5 $\sqrt{d} \in \mathbb{D}$ and since $\mathbb{D}$ is a field $a = b + c\sqrt{d} \in \mathbb{D}$. Thus $\mathbb{K}_{i+1} \leq \mathbb{D}$. This shows that $\mathbb{K}_n \subseteq \mathbb{D}$ and since $a \in \mathbb{K}_n$, a is constructable. □

Lemma 4.7.10. [**q in d**] *$\mathbb{Q} \leq \mathbb{D}$ and so 4.7.9 can be applied to $\mathbb{K} = \mathbb{Q}$.*

Proof. We have $0, 1 \in \mathbb{D}$. If $n \in \mathbb{D} \cap \mathbb{Z}$ then also $n+1 \in \mathbb{D} \cap Z$ and $-n \in \mathbb{D} \cap \mathbb{Z}$. So $\mathbb{Z} \leq \mathbb{D}$. Finally if $n, m \in \mathbb{Z}$ with $m \neq 0$, then $\frac{n}{m} = nm^{-1} \in \mathbb{Z}$. □

Example 4.7.11. [**ex:constructable**]

(1) [**1**] We have $\mathbb{Q} \leq \mathbb{Q}[\sqrt{2}] \leq \mathbb{Q}[\sqrt[4]{2}]$ and both of these extension have degree 2. So by 4.7.9(e), $\sqrt[4]{2}$ is constructable. Also by Homework 4#8, the splitting field of $x^4 - 2$ has degree 8 over $\mathbb{Q}$ and so by 4.7.9(c), $\sqrt[4]{2}$ is constructable.

(2) [**2**] Let $\mathbb{F}$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. By Example 4.5.9i $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{F}) \cong \mathrm{Sym}(3)$. So $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{F})$ is not a 2-group and thus by 4.7.9(d), $\sqrt[3]{2}$ is not constructable. In particular, it is impossible to double a cube, that is to construct a cube whose volumes is twice the volume of a given cube.

(3) [**3**] π is transcendental and so not constructable. Thus it is impossibly to square a circle, that is to construct a square whose area is the same is the are of a given circle.

(4) [**4**] Let $0 \leq \alpha \leq \pi$. We say that α is a constructable angle if the exists a triangle consisting of constructable points and α as one of the angles. It is easy to see α constructable angle if and only if $\cos\alpha$ is a constructable number. We will now investigate the question whether an angle α can be trisected, that is given an constructable angle is also $\beta := \frac{\alpha}{3}$ constructable? For this the first sort out the connection between $\cos\alpha$ and $\cos\beta$.

Recall from your favorite trig class:

$$\sin(\alpha+\beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta)$$

and

$$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$$

Thus $\cos(2\beta) = \cos^2(\beta) - \sin^2(\beta) = 2\cos^2(\beta) - 1$ and $\sin(2\beta) = 2\sin(\beta)\cos(\beta)$ hence

$$\begin{aligned}
&\cos(3\beta) = \cos(\beta+2\beta) = \cos(\beta)\cos(2\beta) - \sin(\beta)\sin(2\beta) \\
&= \cos(\beta)(2\cos^2(\beta) - 1) - 2\sin^2(\beta)\cos(\beta) = 2\cos^3(\beta) - \cos(\beta) - 2(1-\cos^2(\beta))\cos(\beta) \\
&= 2\cos^3(\beta) - \cos(\beta) - 2\cos(\beta) + 2\cos^3(\beta) = 4\cos^3(\beta) - 3\cos(\beta)
\end{aligned}$$

Thus $\cos(\alpha) = 4\cos^3(\beta) + 3\cos(\beta)$. Multiplication by 2 gives:

$$8\cos^3(\beta) + 6\cos(\beta) - 2\cos(\alpha) = 0$$

Put $a = 2\cos(\alpha)$, $b = 2\cos(\beta)$ and $\mathbb{K} = \mathbb{Q}[a]$. Then a is constructable, $\mathbb{K} \leq \mathbb{D}$, β is constructable angle if and only if b is a constructable number. Moreover, b is root of the polynomial

$$x^3 + 3x - a$$

over $\mathbb{K}$.

Suppose that $x^3 - 2x - a$ has no root on $\mathbb{K}$. Then $x^3 + 2x - a$ is irreducible over $\mathbb{K}$ and so $\dim_{\mathbb{K}} \mathbb{K}[a] = 3$. Thus by 4.7.9(e), a is not constructable.

Suppose that $x^3 - 2x - a$ has a root in $\mathbb{K}$. Then the irreducible factors of $x^3 - 2x - a$ over $\mathbb{K}$ have degree 1 or 2 and so $\dim_{\mathbb{K}} \mathbb{K}[a] \leq 2$. Thus 4.7.9(e), a constructable. We proved

(*) Let α be a constructable angle and put $a = 2\cos\alpha$. Then α can be trisected if and only if $f := x^3 - 2x - a$ has a root in $\mathbb{Q}[a]$.

Let $\alpha = \pi$. Then $\cos\alpha = -1$, $a = -2$, $f = x^3 - 3x + 2$ and $\mathbb{Q}[a] = \mathbb{Q}$. Since $f(1) = 0$, $\frac{\pi}{3}$ is constructable. (Which is obvious since $\cos\frac{\pi}{3} = \frac{1}{2}$.

Let $\alpha = \frac{\pi}{2}$. Then $\cos\alpha = 0$, $a = 0$, $f = x^3 - 3x$ and $\mathbb{Q}[a] = \mathbb{Q}$. Since $f(0) = 0$, $\frac{\pi}{6}$ is constructable. (Which is again obvious since $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$.)

Let $\alpha = \frac{\pi}{3}$. Then $\cos\alpha = \frac{1}{[}2]$, $a = 1$, $f = x^3 - 3x - 1$ and $\mathbb{Q}[a] = \mathbb{Q}$. Suppose f has a root $q \in \mathbb{Q}$. Let $q = \frac{n}{m}$ where $n, m \in \mathbb{Z}$, $m > 0$ and $\gcd nm = 1$. Then

$$\frac{n}{m}^3 - 3\frac{n}{m} - 1 = 0 \text{ and } n^3 = 3nm^2 + 3m^3$$

Thus $m \mid n$ and since $\gcd nm = 1$, $m = 1$. Thus $n^3 - n - 1 = 0$, $n(n^2 - 1) = 1$. So $n \mid 1$, $n = \pm 1$ and $n(n^2 - 1) = 0$, a contradiction. Thus f has no root in $\mathbb{Q}$ and so $\frac{\pi}{3}$ cannot be trisected.

Our next goal is to determine for which $n \in \mathbb{Z}^+$, the angle $\frac{2\pi}{n}$ is constructable. Note that this is the case if and only if regular n-gon can be constructed. To do this we will have to develop quit a bit of theory first.

Lemma 4.7.12. [**ideals and poly**] *Let R be a commutative ring and I an ideal in R. Let $\overline{R} = R/I$. For $r \in R$ put $\overline{r} = r = I$ and for $f = \sum_{i=0}^n r_i x^i$ put $\overline{f} = \sum_{i=0}^n \overline{r_i} x \in \overline{R}[x]$. Then*

$$\pi_x : R[x] \to \overline{R}[x], \quad f \to \overline{f}$$

is an onto ring homomorphism with kernel $I[x] = \{\sum_{i=0}^n a_i x^i \mid a_i \in I\}$.

Proof. Let $\pi : R \to R/I, r \to \overline{r}$. Then by 3.3.9(c), π is an onto ring homomorphism with $\ker \pi = I$. Thus by 3.4.2(a), the map

$$\pi_x : R[x] \to \overline{R}[x], \sum_{i=0}^{n} r_i x^i \to \sum_{i=0}^{n} \pi(r_i) x^i$$

is a well-defined ring homomorphism. Note that $\pi_x(f) = \overline{f}$. We have

$$\begin{array}{cc} & f \in \ker \pi_x \\ \iff & \pi_x(f) = 0_{\overline{R}} \\ \iff & \sum_{i=0}^{n} \pi(r_i) x^i = 0_{\overline{R}} \\ \iff & \pi_(r_i) = 0_{\overline{R}} \text{ for all } 0 \leq i \leq n \\ \iff & r_i \in \ker \pi \text{ for all } 0 \leq i \leq n \\ \iff & r_i \in I \text{ for all } 0 \leq i \leq n \\ \iff & f \in I[x] \end{array}$$

So $\ker \pi_x = I[x]$.

Let $g = \sum_{i=0}^{n} a_i x^i \in \overline{R}[x]$. Then $a_i = r_i + I$ for some $r_i \in R$. Put $f = \sum_{i=0}^{n} r_i x^i$. Then $f \in \mathbb{R}[x]$, $\overline{f} = g$ and π_s is onto. □

Definition 4.7.13. [**def:content**] *Let R be a PID and $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. Then* $\operatorname{cont}(f) = \gcd(a_0, a_1, \ldots, a_n)$. $\operatorname{cont}(f)$ *is called the* content *of f. (Note here that* $\operatorname{cont} f$ *is only defined up to associates). f is called* primitive *if* $\operatorname{cont}(f) = 1_R$.

Example 4.7.14. [**ex:content**] Let $R = \mathbb{Z}$ and $f = 12x^2 + 9x + 15$. Then

$$\operatorname{cont}(f) = \gcd(12, 9, 15) = 3$$

and so f is not primitive.

Let $g = 12x^3 + 9x^2 + 4x + 6$. Then

$$\operatorname{cont}(g) = \gcd(12, 9, 4, 6) = 1$$

and so g is primitive.

Lemma 4.7.15. [**primitive poly**] *Let R be a PID and $f \in R[x]^\sharp$. Then there exists $c \in R$ and a primitive polynomial $g \in R[x]$ with $g = cg$. Moreover, c and g are unique up to associates and $c \sim \operatorname{cont}(f)$.*

Proof. Put $c := \operatorname{cont} f$ and let $f = \sum_{i=0}^{n} a_i x^i$. Then $c \mid a_i$ for all i and so there exists $b_i \in R$ with $a_i = cb_i$. Put $g = \sum_{i=0}^{n} b_i x_i$. Then clearly $cg = f$. Let $d = \operatorname{cont}(g)$. Then $d \mid b_i$ and so $dc \mid a_i$ for all $i \in I$. Thus by definition of cont and gcd, $dc \mid c$. Since $c \mid dc$ we conclude $c \sim dc$ and so by 3.6.4 d is a unit in R. Thus g is primitive.

Now suppose that $f = eh$ with $e \in R, h \in R[x]$ with h primitive. Let $h = \sum_{i-0}^{n} h_i x^i$. Then $a_i = eh_i$. So $e \mid a_i$ for all i and so $e \mid c$. Hence $c = er$ for some $r \in R$. Thus $eh = f = erg$ so since $R[x]$ is an integral domain, $h = rg$. Thus $r \mid h_i$ for all i. Since h is primitive we conclude that r is a unit. Thus $h \sim g$ and $e \sim c = \mathrm{cont}(f)$. □

Lemma 4.7.16 (Gauss)**.** [**gauss primitive**] *Let R be a PID and f and g primitive polynomials in $R[x]^\sharp$. Then fg is primitive.*

Proof. We will show the contrapositive. So let $f, g \in R[x]^\sharp$ such that fg is not primitive. Then $\mathrm{cont}(fg) \nsim 1_R$. Since R is a PID and so a UFD there exists prime p in R with $p \mid \mathrm{cont} fg = 0$. So p divides all coefficients of fg. We apply 4.7.12 with $I = Rp$. Then $\overline{fg} = 0_{\overline{R}}$. Hence also $\phi f\overline{g} = 0_{\overline{R}}$. Since p is a prime we conclude from 3.8.11 that $\overline{R}$ is an integral domain. Thus by 3.8.12(c), $\overline{R}[x]$ is an integral domain. Thus $\overline{f} = 0_{\overline{R}}$ or $\overline{g} = 0_{\overline{R}}$. Hence $f \in Rp[x]$ or $g \in Rp[x]$. Thus p divides all the coefficients of f or of g and so f or g is not primitive. □

Lemma 4.7.17. [**irreducible**] *Let R be a PID with field of fractions $\mathbb{F}$. Let $f \in R[x]$ be primitive. Then f is irreducible in $R[x]$ if and only if f is irreducible in $\mathbb{F}[x]$.*

Proof. Suppose first that f is irreducible in $\mathbb{F}[x]$ and let $f = gh$ with $g, h \in \mathbb{R}[x]$. then g or h is a unit in $\mathbb{F}[x]$. Say g is unit in $\mathbb{F}[x]$. Then by 3.8.12(e), $g \in \mathbb{F}$, that is $\deg g = 0$ and $g \in R$. Since f is primitive we conclude that $g \sim 1$ in R. So g is a unit in R and f is irreducible in $R[x]$.

Suppose next that f is irreducible in $R[x]$ and let $f = gh$ with $g, h \in \mathbb{F}[x]$. Note that there exists a such that $a \in R$ with $ag \in R[x]$. By 4.7.15 $ag\tilde{a}\tilde{g}$ with $\tilde{a} \in R, \tilde{g} \in R[x]$ and $\tilde{g}$ primitive. Similarly $bh \in R[x]$ and $bh = \tilde{b}\tilde{h}$ with $\tilde{b} \in R, \tilde{h} \in R[x]$ and $\tilde{h}$ primitive. Then

$$abf = abfg = (\tilde{a}\tilde{g})(\tilde{b}\tilde{h}) = \tilde{a}\tilde{b}\tilde{g}\tilde{h}$$

By Gauss' Lemma 4.7.16 $\tilde{g}\tilde{h}$ is primitive. 4.7.15 now shows that $f \sim \tilde{g}\tilde{h}$. Since f is irreducible in $R[x]$ we conclude that $\tilde{g}$ or $\tilde{h}$ is a unit in $R[x]$. So $\tilde{g}$ or $\tilde{h}$ has degree 0 and so g or h has degree 0. Thus f is irreducible in $R[x]$. □

Example 4.7.18. [ex:gauss]

(1) [**1**] Put $f = 3x^2 + 6x + 9$. Then $f = 3(x^2 + 2x + 3)$. Since neither 3 nor $x^2 + 2x + 3$ is a unit in $\mathbb{Z}[x]$, f is not irreducible over $\mathbb{Z}[x]$] (Note here that by 3.8.12(e) the units in $\mathbb{Z}[x]$ are the units in $\mathbb{Z}$. So 1 and -1 are the only units in $\mathbb{Z}[x]$.)

We claim that f is irreducible in $\mathbb{Q}[x]$. Bu 3.8.16(c), f is irreducible in $\mathbb{Q}[x]$ if and only if f has a root in $\mathbb{Q}$. Since

$$f = 3(x^2 + 2x + 3) = 3((x + 1)^2 + 2)$$

$f(a) > 0$ for all $a \in \mathbb{Q}$ and f has not root. So f is irreducible in $\mathbb{Q}[x]$ by not irreducible in $\mathbb{Z}[x]$. This shows that the assumption that f is primitive in 4.7.17 is necessary.

(2) [**2**] Is $f = x^4 + x^3 + x^2 + x + 1$ irreducible in $\mathbb{Q}[x]$? Since f is primitive, this is the case if and only if f is irreducible in $\mathbb{Q}[x]$. Suppose $f = gh$ with $g, h \in \mathbb{Z}[x]$ with neither g nor a h a unit in $\mathbb{Z}[x]$ and $\deg g \leq \deg h$. We have $1 = \text{lead}(f) = \text{lead}(g)\text{lead}(h)$ and so $\text{lead}(g) = \text{lead}(h) = \pm 1$. Replacing g by $\text{lead}(g)g$ and h be $\text{lead}(h)h$ we may assume that g and h are monic. Since g is not a unit we get $\deg g \geq 1$.

Since $1 = f(0) = g(0)h(0)$ we have $g(0) = h(0) = \pm 1$.

Suppose $\deg g = 1$. Then $g = x + g(0)$ and $-g(0) = \pm 1$ is a root of f. But $f(1) = 5$ and $f(-1) = 1$, a contradiction. Hence $2 \leq \deg g \leq \deg h$. Since $\deg g + \deg h = \deg f = 4$ we get $\deg g = \deg h = 2$. Thus $g = x^2 + ax + b$ and $h = x^2 + cx + b$ for some $a, b, c \in \mathbb{Z}$. Hence

$$x^4 + x^3 + x^2 + x + 1 = f = gh = x^4 + (a+c)x^3 + (b + ac + b)x^2 + (bc + ba)x + b^2$$

Thus $a + c = 1$, $2b + ac = 1$ and $b(a+c) = 1$. Thus $b = 1$, $2 + ac = 1$, $ac = -1$, $a = -c = \pm 1$ and $1 = a + c = a - a = 0$, a contradiction.

Thus contradiction shows that f is irreducible in $\mathbb{Z}[x]$ and so also in $\mathbb{Q}[x]$.

Corollary 4.7.19 (Eisenstein's Criterion)**.** [**eisenstein**] *Let R be a PID with field of fraction $\mathbb{F}$, p a prime in R and $f = \sum_{i=0}^{n} a_n x^n \in \mathbb{R}[x]$. Suppose that $a_n = 1_R$, $p \mid a_i$ for all $0 \leq i < n$ and $p^2 \nmid a_0$. Then f is irreducible in $R[x]$ and $\mathbb{F}[x]$.*

Proof. Since $a_n = 1_{\mathbb{F}}$, f is primitive. So by 4.7.17 it suffices to show that f is irreducible in $R[x]$. Suppose for a contradiction that $f = gh$ with $g, h \in R[x]$ neither g nor h a unit. Since $\text{lead}(g)\text{lead}(h) = \text{lead}(f) = 1_R$ we may assume that both g and h are monic. In particular, $\deg g \leq 1$ and $\deg h \geq 1$. Let $I = pR$ and define $\overline{R}, \overline{r}$ and $\overline{f}$ has in 4.7.12. Since $p \mid a_i$ for all $0 \leq i < n$ we have $\overline{a_0} = 0_{\overline{R}}$ for all $0 \leq i < n$. Thus $\overline{f} = x^n$. By 3.8.11, $\overline{R}$ is a field. Thus by Example 3.5.2(2), $\overline{R}[x]$ is Euclidean and by 3.6.20, $\overline{R}[x]$ is a UFD. Since x is irreducible in $\overline{R}[x]$, we conclude that $\overline{g} = x^k$ and $\overline{h} = x^l$ where $k, l \in \mathbb{Z}^+$ with $n = k + l$. It follows that $\overline{g}(\overline{0_R}) = \overline{0_R}$, $\overline{h}(\overline{0_R}) = \overline{0_R}$ and so p divides $g(0_R)$ and $h(0_R)$. Hence p^2 divides $f(0_R) = g(0_R)h(0_R)$, a contradiction to $f(0_R) = a_0$ and the assumptions. □

Definition 4.7.20. [**def:euler**] *Let $n \in \mathbb{Z}^+$.*

(a) [**a**] *$\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n \mid |a| = n\}$, where $|a|$ is the order of a in $(\mathbb{Z}_n, +)$.*

(b) [**b**] *$\phi(n) := |\mathbb{Z}_n^*|$.*

(c) [**c**] *The function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is called the* Euler function*.*

Lemma 4.7.21. [**subgroups of zn**] *Let $n \in \mathbb{Z}^+$.*

(a) [**a**] *The subgroups of $\mathbb{Z}_n$ are $k\mathbb{Z}_m = k\mathbb{Z}/n\mathbb{Z}, 1 \leq k \leq n$, $k \mid n$.*

(b) [**b**] *$k\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{k}}$ and $\mathbb{Z}_n/kZ_n \cong \mathbb{Z}_k$ for all $1 \leq k \leq n$, $k \mid n$. Here the first isomorphism is an isomorphism of abelian groups and the second an isomorphism of rings.*

(c) [**c**] *Let $a, b \in Z^+$ with $\gcd(a, b) = 1$. Then the map $\mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$, $k + ab\mathbb{Z} \to k + a\mathbb{Z}, k + b\mathbb{Z})$ is a well-defined isomorphism of rings.*

Proof. (a) See Homework 2#2 in MTH 418.

(b) The map $\alpha : \mathbb{Z} \to Z_n$, $m \to km + n\mathbb{Z}$ is a homomorphism of abelian group. Clearly $\operatorname{Im}\alpha = k\mathbb{Z}_n$. We have $m \in \ker\alpha$ if and only if $km + n\mathbb{Z} = 0_{\mathbb{Z}_n}$ and so if and only if $n \mid km$. Since $k \mid n$, this is the case if and only if $\frac{n}{k} \mid m$ and $m \in \frac{n}{k}\mathbb{Z}$. So $\ker\alpha = \frac{n}{k}\mathbb{Z}$ and so by the first Isomorphism Theorem for Groups:

$$\mathbb{Z}/\frac{k}{n}\mathbb{Z} = \mathbb{Z}/\ker\alpha \cong \operatorname{Im}\alpha = k\mathbb{Z}_n$$

So the first statement in (b) holds. By the Third Isomorphism Theorem for Rings:

$$\mathbb{Z}_n/k\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}/\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z} = \mathbb{Z}_k$$

(c) Define $\beta : \mathbb{Z} \to \mathbb{Z}_\alpha \times \mathbb{Z}_b, k \to (k + a\mathbb{Z}, k + \beta\mathbb{Z})$. Then β is a homomorphism of rings. $k \in \ker\alpha$ if and only if $a \mid k$ and $b \mid k$. Since $\gcd ab = 1$, this is the case if and only if $ab \mid k$. So $\ker\alpha = ab\mathbb{Z}$. Thus by the First Isomorphism Theorem of Rings, $\mathbb{Z}_{ab} = \mathbb{Z}/ab\mathbb{Z} \cong \operatorname{Im}\alpha$. Thus $|\operatorname{Im}\alpha| = ab$ and since $\mathbb{Z}_a \times \mathbb{Z}_b| = ab$ we get $\operatorname{Im}\alpha = \mathbb{Z}_a \times \mathbb{Z}_b$ and so (c) holds. □

Lemma 4.7.22. [**euler**] *Let $n \in \mathbb{Z}^+$.*

(a) [**a**] *$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid Z_n = \langle a \rangle\} = \{m + n\mathbb{Z} \mid 0 \leq m < n, \gcd(n, m) = 1\}$.*

(b) [**z**] *$\phi(n) = |\{m \mid 0 \leq m < n, \gcd(n, m) = 1\}|$.*

(c) [**b**] *$n = \sum_{1 \leq d \leq n, d|n} \phi(d)$.*

(d) [**c**] *$\phi(n) = n - \sum_{1 \leq d < n, d|n} \phi(d)$.*

(e) [**d**] *Suppose $a, b \in Z^+$ with $\gcd(a, b) = 1$. Then $\phi(ab) = \phi(a)\phi(b)$.*

(f) [**e**] *Let $k, p \in \mathbb{N}$, p a prime. Then $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$.*

(g) [**f**] *Let $n = \prod_{i=1}^t p_i^{k_i}$, where $p_1, p_2 \ldots p_t$ are distinct positive prime integers and $k_i \in \mathbb{N}$. Then*

$$\phi(n) = \prod_{i=1}^{t} p_i^{k_i - 1}(p_i - 1) = n\prod_{i=1}^{t}(1 - \frac{1}{p_i})$$

Proof. (a) Let $a \in Z_n$. Then by definition $|a| = \langle a \rangle$. Since $\langle a \rangle = \mathbb{Z}_n$ if snd only if $\langle a \rangle = |\mathbb{Z}_n|$ we get $|a| = n$ if and only if $\langle a \rangle = \mathbb{Z}_n$. So the first equality in (a) holds.

Let $a = m + n\mathbb{Z}$ where $m \in \mathbb{Z}$ with $0 \leq m < n$. Then by 4.7.21(a) $\langle a \rangle \neq \mathbb{Z}_n$ if and only if $\langle a \rangle = k\mathbb{Z}/n\mathbb{Z}$ for some $1 < k \leq n$ with $k \mid n$; if and only if $k \mid m$ for some $1 < k \leq n$ with

$k \mid n$ and so if and only if $\gcd(k,m) \neq 1$. Thus $\langle a \rangle = \mathbb{Z}_n$ if and only if $\gcd mn = 1$. This gives the second equality.

(b) follows immediately from (a).

(c) For $1 \leq d \leq n$ with $d \mid n$ define $\mathbb{Z}_{n,d} = \{a \in \mathbb{Z}_n \mid |a| = d\}$. Let $a \in \mathbb{Z}_n$, $a \in \mathbb{Z}_{n,d}$ if and only if $|\langle a \rangle| = d$ and so by 4.7.21(a) if and only if $a \in \frac{n}{d}\mathbb{Z}_n$ and $|a| = d$. By 4.7.21(b), $\frac{n}{d}\mathbb{Z}_n \cong \mathbb{Z}_d$ and so

$$|Z_{n,d}| = \{a \in \in \frac{n}{d}\mathbb{Z}_n, |a| = |\{b \in \mathbb{Z}_d \mid |b| = d\}| = |\mathbb{Z}_m^*| = \phi(d).$$

Since each $a \in \mathbb{Z}_n$ lies in a unique $\mathbb{Z}_{n,d}$ namely $\mathbb{Z}_{n,|a|}$ we conclude

$$n = |\mathbb{Z}_n| = \sum_{1 \leq d \leq n, d \mid n} |Z_{n.d}| = \sum_{1 \leq d \leq n, d \mid n} \phi(d)$$

and so (c) holds.

(d) follows immediately from (c).

(e) By 4.7.21(c), $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$. Hence

$$(*) \qquad \phi(ab) = \{k \in Z_{ab} \mid |k| = ab\}| = |\{e \in \mathbb{Z}_a \times \mathbb{Z}_b \mid |e| = ab\}|.$$

Let $e = (s,t) \in \mathbb{Z}_a \times \mathbb{Z}_b$ and $k \in \mathbb{Z}^+$. Put $u = |s|, v = |t|$. Then $u \mid a, v \mid b$. Since $\gcd(a,b) = 1$ we conclude that $gcd(u,v) = 1$. Note that $ke = (0_{\mathbb{Z}_a}, 0_{\mathbb{Z}_b})$ if and only if $ks = 0_{\mathbb{Z}_a}$ and $kt = 0_{\mathbb{Z}_b}$; if and only if $u \mid l$ and $v \mid k$ and if and only if $uv \mid k$. Thus $|e| = uv$. It follows that $|e| = ab$ if and only if $|s| = |a|$ and $|t| = a, b$. Thus

$$\{e \in \mathbb{Z}_a \times \mathbb{Z}_b \mid |e| = ab\} = \{(s,t) \mid s \in \mathbb{Z}_a, |s| = a, t \in \mathbb{Z}_b, |t| = b\} = \mathbb{Z}_a^* \times Z_b^*$$

Together with (*)

$$\phi(ab) = |\mathbb{Z}_a^* \times \mathbb{Z}_b^*| = |Z_a^*||Z_b^*| = \phi(a)\phi(b)$$

(f) The subgroups of $\mathbb{Z}_{p^k}$ are $p^l\mathbb{Z}_{p^k}$, $0 \leq l \leq k$ and so every proper subgroup of $\mathbb{Z}_{p^k}$ is contained in $p\mathbb{Z}_p$. Let $a \in \mathbb{Z}_{p^k}$. It follows that $\langle a \rangle = \mathbb{Z}_{p^k}$ if and only if $a \notin p\mathbb{Z}_{p^k}$. By 4.7.21(b), $p\mathbb{Z}_{p^k} \cong \mathbb{Z}_{p^{k-1}}$ and so $p\mathbb{Z}_{p^k}| = p^{k-1}$. Thus by (a)

$$\phi(p^k) = |\{a \in \mathbb{Z}_{p^k} \mid \langle a \rangle = \mathbb{Z}_{p^k}\}| = |\mathbb{Z}_{p^k} \setminus p\mathbb{Z}_{p^k}| = p^k - p^{k-1} = p^{k-1}(p-1)$$

(g) follows from (f), (e) and induction on k. □

Example 4.7.23. [**ex:euler**] We have $\phi(24) = \phi(2^3 3) = 2^2(2-1)3^0(3-1) = 4 \cdot 2 = 8$. Lets us verify this by determining integers $0 \leq k < 24$ with $\gcd(k, 24)$. Note that $\gcd(k, 24) = 1$ if and only if $2 \nmid k$ and $3 \nmid k$.

$$\not 0, 1, \not 2, \not 3, \not 4, 5, \not 6, 7, \not 8, \not 9, \not 10, 11, \not 12, 13, \not 14, \not 15, \not 16, 17, \not 18, 19, \not 20, \not 21, \not 22, 23$$

So there are indeed 8 such numbers.

Definition 4.7.24. [**root of unity**] *Let $n \in \mathbb{Z}^+$ and $\mathbb{K}$ a field.*

(a) [**a**] *$\xi \in \mathbb{K}^\sharp$ is an n'th -root of unity if $\xi^n = 1_\mathbb{K}$ and a primitive n'th root of unity if $|\xi| = n$, where $|\xi|$ is the multiplicative order of n.*

(b) [**b**] *$U_n\mathbb{K})$ is the set of n-root of unities in $\mathbb{K}$ and $U_n^*(\mathbb{K})$ is the set of primitive n-roots of unities in $\mathbb{K}$.*

(c) [**c**] *Let $\mathbb{F}$ be a splitting field for $x^n - 1_\mathbb{K}$ over $\mathbb{K}$. Then*

$$\Phi_n^\mathbb{K} := \prod_{\xi \in U_n^*(\mathbb{F})} x - \xi \in \mathbb{F}[x]$$

*is called the n-*cyclotomic *polynomial over $\mathbb{K}$.*

(d) [**e**] $\Phi_n := \Phi_n^\mathbb{Q}$

Lemma 4.7.25. [**freshman**]*Let R be a commutative ring and p a positive prime integer with $pa = 0_R$ for all $a \in R$. Then*

(a) [**a**] *The map $\alpha : R \to R, a \to a^p$ is a ring homomorphism. In particular, $a+b)^p = a^p + b^p$ and $(a-b)^p = a^p - b^p$ for all $a, b \in R$.*

(b) [**b**] *$a^p = a$ for all $a \in \mathbb{Z}_p$.*

(c) [**c**] *Let $f \in \mathbb{Z}_p[x]$. Then $f(x^p) = f^p$.*

Proof. (a) Let i be an integer with $0 < i < p$. Then p divides neither $i!$ nor $(p-i)!$ and so p divides $\binom{p}{i} = \frac{p!}{i!(p-i)}!$. Since $pa = 0_R$ for all $a \in R$ we conclude that $\binom{p}{i}a = 0_R$ for all a in R. Thus by the Binomial Theorem A.1.3 we conclude

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p.$$

Clearly also $(ab)^p = a^p b^p$ and so α is a ring homomorphism. It follows that $(a-b)^p = \alpha(a-b) = \alpha(a) - \alpha(b) = a^p - b^p$.

(b) Since $\mathbb{Z}_p$ is a field, $(\mathbb{Z}_p^\sharp, \cdot)$ is a group of order $p-1$. Thus $a^{p-1} = 1_{\mathbb{Z}_p}$ for all $a \in \mathbb{Z}_p$. Thus $a^p = a$ for all $a \in \mathbb{Z}_p$.

(c) Let $f = \sum_{i=0}^n a_i x^i$ with $a_i \in \mathbb{Z}_p$. Then

$$f^p \overset{\text{(a)}}{=} \sum +i = 0^n a_i^p x^{pi} = \overset{\text{(b)}}{=} \sum_{i=0}^{n} a_i (x^p)^i = f(x^p)$$

□

Lemma 4.7.26. [**not coprime cyclotomic**] *Let $\mathbb{K}$ be a field and $n \in \mathbb{Z}^+$. Suppose $p :=$* $\operatorname{char}\mathbb{K} \neq 0$ *let $n = p^k n_{p'}$ for some $k, n' \in \mathbb{N}$ with $p \nmid n_{p'}$.*

(a) [**a**] $U_n^*(\mathbb{K}) = U_{n'}(\mathbb{K})$.

(b) [**b**] *If* $p \mid n$, *then* $U_n^*(\mathbb{K}) = \emptyset$.

Proof. (a) Let $\xi \in \mathbb{Z}_n^*$ and put $m = |\xi|$. Let $m = p^r l$ with $r, l \in \mathbb{N}$ and $p \nmid l$. Then

$$0_{\mathbb{K}} = \xi^{p^r l} - 1_{\mathbb{K}} = (\xi^l - 1)^{p^r}$$

Thus $\xi^l = 1_{\mathbb{F}}$ and $|\xi| = l$. Since $m \mid n$, $l \mid n'$ and so $\xi \in U_{n'}(\mathbb{K})$.

(b) follows immediately from (a). □

Proposition 4.7.27. [**cyclotomic**] *Let* $\mathbb{K}$ *be a field,* $n \in \mathbb{Z}^+$ *and suppose that* $\operatorname{char}\mathbb{K} \nmid n$. *Put* $\mathbb{Z}_{\mathbb{K}} = \{n1_{\mathbb{K}} \mid n \in \mathbb{Z}^+\}$ *and let* $\mathbb{F}$ *be a splitting field for* $x^n - 1_{\mathbb{K}}$ *over* $\mathbb{K}$.

(a) [**a**] $x^n - 1_{\mathbb{K}} = \prod_{d \in \mathbb{Z}^+, d \mid n}, \Phi_n^{\mathbb{K}}$.

(b) [**b**] $\Phi_n^{\mathbb{K}} = \frac{x^n - 1}{\prod_{d \mid n, 1 \leq n < d} \Phi_n^{\mathbb{K}}}$.

(c) [**c**] $|U_n^*(\mathbb{F})| = \deg \Phi^{\mathbb{K}} = \phi(n)$. *In particular there exists a primitive n-root of unity in* $\mathbb{F}$. *with* $|\xi| = n$

(d) [**d**] $\Phi_n^{\mathbb{K}} \in \mathbb{Z}_{\mathbb{K}}[x] \subseteq \mathbb{K}[x]$.

(e) [**e**] *For* $n \in \mathbb{Z}$ *let* $\overline{n} = n1_{\mathbb{K}} \in \mathbb{Z}_{\mathbb{K}}$. *For* $f = \sum_{i=0}^n z_i x^i \in \mathbb{Z}[x]$ *let* $\overline{f} = \sum_{i=0}^n \overline{z_i} x^i \in \mathbb{Z}_{\mathbb{F}}[x]$. *Then* $\overline{\Phi_n} = \Phi_n^{\mathbb{K}}$.

Proof. (a) Since $\operatorname{char}\mathbb{K} \nmid n$, $n1_K \neq 0_{\mathbb{K}}$. Also $(x^n - 1_{\mathbb{K}})' = nx^{n-1}$ and $n1_K \neq 0_{\mathbb{K}}$. So $0_{\mathbb{K}}$ is the only root of $(x^n - 1)'$. Since $0_{\mathbb{K}}$ is not a root of $x^n - 1_{\mathbb{K}}$ we conclude from 4.6.6 that $x^n - 1_{\mathbb{K}}$ has not double roots. Thus

$$x^n - 1_{\mathbb{K}} = \prod_{\xi \in U_n(\mathbb{F})} x - \xi.$$

Since $U_n(\mathbb{F})$ is the disjoint union of the $U_d^*(\mathbb{F})$, $1 \leq d \leq n$, $d \nmid n$ we conclude that (a) holds.

(b) follows from (a) and the division algorithm.

(c) Follows from (b) and 4.7.22(d) and induction on n.

(d) Note that each $\Phi_d^{\mathbb{K}}$, $1 \leq d < n, d \nmid n$ is a monic. By induction we may assume that $\Phi_d \in \mathbb{Z}_{\mathbb{F}}[x]$. Thus (d) follows from (b) and the division algorithm.

(e) Again this follows from (b) and induction on n. □

Example 4.7.28. [**ex:cyclotomic**]

1. [**1**] We will compute Φ_n for all $1 \leq n \leq 8$.

   $\Phi_1 = x - 1$.

   $\Phi_2 = \frac{x^2 - 1}{x - 1} = x + 1$.

$\Phi_3 = \frac{x^3-1}{x-1} = x^2+x+1.$

$\Phi_4 = \frac{x^4-1}{(x-1)(x+1)} = \frac{x^4-1}{x^2-1} = x^2+1.$

$\Phi_5 = \frac{x^5-1}{(x-1)} = x^4+x^3+x^2+x+1.$

$\Phi_6 = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = \frac{x^6-1}{(x^3-1)(x+1)} = \frac{x^3=1}{x+1} = x^2-x+1$

$\Phi_7 = \frac{x^7-1}{(x-1)} = x^6+x^5x^4+x^3+x^2+x+1.$

$\phi_8 = \frac{x^8-1}{(x-1)(+1)(x^2+1)} = \frac{x^8-1}{x^4-1} = x^4+1.$

2. [**2**] We compute Φ_{p^k} where $p,k \in \mathbb{Z}^+$, p a prime.

We have

$$\Phi_p = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+x+1$$

The divisors of p^{k+1} are p^i, $0 \leq i \leq k+1$. Also

$$\prod_{i=0}^{k} \Phi_{p^i} = x^{p^k}-1$$

and so

$$\Phi_{p^{k+1}} = \frac{x^{p^{k+1}-1}}{x^{p^k}-1} = \frac{(x^{p^k})^p-1}{x^{p^k}-1} = \Phi_p(x^{p^k}) = x^{p^k(p-1)}+x^{p^k(p-2)}+\ldots+x^{p^k}+1.$$

For example $\Phi_{27} = \Phi_3(x^9) = x^{18}+x^9+1.$

Lemma 4.7.29. [**zn and un**] *Let $n \in \mathbb{Z}^+$ and $\mathbb{K}$ a field and suppose $\xi \in \mathbb{K}$ is a primitive n-th root of unity.*

(a) [**a**] *$U_n(\mathbb{K}) = \langle \xi \rangle$ and so $U_n(\mathbb{K})$ is a cyclic group of order n.*

(b) [**b**] *The map $\tau : (\mathbb{Z}_n, +) \to (U_n(\mathbb{K}), \cdot), k+n\mathbb{Z} \to \xi^k$ is isomorphism of groups.*

(c) [**c**] *$U_n(\mathbb{K})^* = \tau(\mathbb{Z}_n^*) = \{\xi^k \mid 0 \leq k < n, \gcd(k,n) = 0\}$.*

Proof. (a) Since each $a \in U_n(\mathbb{K})$ is a root of $x^n - 1_{\mathbb{K}}$ in $\mathbb{K}$, $|U_n| \leq n$. Since $|\xi| = n$ and $\xi \in U_n(\mathbb{K})$, $U_n(\mathbb{K}) = \langle \xi \rangle$.

(b) Follows from (a) and Example 2.6.9.

(c) We have

$$\begin{array}{lcccc} U_n(\mathbb{K})^* & = & \{\mu \in U_n(\mathbb{K}) \mid |\mu| = n\} & \overset{(b)}{=} & \{\tau(a) \mid a \in \mathbb{Z}_n, |a| = n\} \\ & \overset{4.7.22(a)}{=} & \{\tau(k+n\mathbb{Z}) \mid 0 \leq k < n, \gcd(k,n) = 1\} & = & \{\xi^k \mid 0 \leq k < n, \gcd(k,n) = 1\} \end{array}$$

□

Example 4.7.30. [**ex:all primitive**] Let ξ be a primitive 24th root if unity in a field $\mathbb{F}$. Then by 4.7.29(c)

$$\xi, \xi^5, \xi^7, \xi^{11}, \xi^{13}, \xi^{17}, \xi^{19}, \xi^{23}$$

are all the primitive 24th roots of unities in $\mathbb{F}$.

Corollary 4.7.31. [**finite in field**] *Let $\mathbb{F}$ be a field and G a finite subgroup of order n of $(\mathbb{F}^\sharp, \cdot)$. Then $G = U_n(\mathbb{F})$ and G is cyclic.*

Proof. Since $|G| = n$ we have $g^n = e_G = 1_\mathbb{F}$ for all $g \in G$. Thus $G \subseteq U_n(\mathbb{F})$. Note that

$$n = |G| \leq |U_n(\mathbb{F})| = \sum_{1 \leq d \leq n, d|n} |U_d^*(\mathbb{F})| \leq \sum_{1 \leq d \leq n, d|n} \phi(d) = n$$

So equality holds everywhere and so $G = U_n(\mathbb{F})$ and $|U_n^*(\mathbb{F})| = \phi(n) \geq 1$. Thus $\mathbb{F}$ has a primitive roots of unity ξ and by 4.7.29 $U_n(\mathbb{F}) = \langle \xi \rangle$. □

Proposition 4.7.32. [**phin irr**] *Let $n \in \mathbb{Z}^+$. Then Φ_n is irreducible in $\mathbb{Q}[x]$.*

Proof. Since Φ_n is monic, Φ_n is a primitive polynomial in $\mathbb{Z}[x]$. So by 4.7.17 it suffices to show that Φ_n is irreducible in $\mathbb{Z}[x]$. Let g be an irreducible factor of Φ_n in $\mathbb{Z}[x]$. Then $\Phi_n = gh$ for some $h \in Z[x]$. Since $\mathrm{lead} g \cdot \mathrm{lead} h = \mathrm{lead} \Phi_n = 1$ we may assume that g and h are monic. Let $\mathbb{F}$ be a splitting field of $x^n - 1$ over $\mathbb{Q}$. Let U be the set of roots of g in $\mathbb{F}$. Since $\Phi_n = \prod_{\xi \in U_n^*(\mathbb{F})} x - \xi$, $U \subseteq U_n^*(\mathbb{F})$ and $g = \prod_{\xi \in U} x - \xi$. We will show that $U = U_n^*(\mathbb{F})$. Note that this will implies that $g = \Phi_n$ and so Φ_n is irreducible.

Let $\xi \in U$ and let p prime integer with $1 < p < n$, Then $\gcd(p, n) = 1$ and so by 4.7.29(c), ξ^p is a primitive n-root of unity. Suppose for a contradiction that ξ^p is not a root of g. Then ξ^p is a root of h. Then $h(\xi^p) = 0$ and so ξ is a root of $h(x^p)$. Since g is a monic irreducible polynomial with ξ as a root, g is the minimal polynomial of ξ over $\mathbb{Q}$. Hence g divides $h(x^p)$ in $\mathbb{Q}[x]$. Since g and $h(x^p)$ are in $\mathbb{Z}[x]$ and g is monic, the Division algorithm shows that g divides $h(x^p)$ in $\mathbb{Z}[x]$. Thus $h(x^p) = gk$ for some $k \in \mathbb{Z}[x]$. Let $I = Rp$ and define $\overline{R}, \overline{r}$ and $\overline{f}$ has before. Using 4.7.25(c) we conclude

$$\overline{h}^p = \overline{h}(x^p) = \overline{g}\overline{k}$$

Let $\bar{l}$ be an irreducible factor of γ. Since $\overline{R}[x]$ is a PID we conclude $\bar{l}$ divides $\overline{h}$ in $\overline{R}[x]$. Since Φ_n divides $x^n - 1$ in $\mathbb{Z}[x]$, $\overline{g}\overline{h} = \overline{\Phi_n}$ divides $x^n - \overline{1}$ in $\overline{R}[x]$. It follows that $\bar{l}^2$ divides $x^n - \overline{1}$ in $\overline{R}[x]$. Thus $x^n - \overline{1}$ has a double root. But since $p \nmid n$, $(x^n - \overline{1})' = \overline{n}x^{n-1} \neq \overline{0}$ and so $x^n - \overline{1}$ does not have a double root.

This contradiction shows that ξ^p is a root of g and so $\xi^p \in U$. We proved:

(*) If $\xi \in U$ and p is prime integer with $1 \leq p < n$, then $\xi^p \in U$.

Now let $\eta \in U_n^*(|F)$. Then by 4.7.29, $\eta = \xi^k$ for some $k \in \mathbb{N}$ with $k \leq n$ and $\gcd(k, n) = 1$. We will show by complete induction on k that $\eta \in U$. Suppose $k = 0$. Then $\gcd(0, n) = 1$ shows that $n = 1$. Thus $\eta = \xi^0 = 1 = \xi \in U$. If $k = 1$, then $\eta = \xi \in U$. So suppose $k > 1$.

The there exists a prime $p \in \mathbb{Z}^+$ with $p \mid k$. Since $k < n$, $p < n$. Let $k = pl$ with $l \in \mathbb{Z}^+$. Then $l > k$ and so by induction $\xi^l \in U$. By (*) applied to ξ^l in place of ξ we conclude that $(\xi^l)^p \in U$ and so $\eta = \xi^k = \xi^{pl} = (\xi^l)^p \in U$.

Thus shows that $U = U_n^*(F)$ and so $g = \Phi_n$. Thus Φ_n is irreducible in $\mathbb{Z}[x]$ and so also in $\mathbb{Q}[x]$. □

Lemma 4.7.33. [**aut xn-1**] *Let* $\mathbb{K}$ *be a field and* $n \in \mathbb{Z}^+$ *such that* $\operatorname{char} p \nmid \mathbb{Z}$. *Let* $\mathbb{F}$ *be a splitting field of* $x^n - 1_{\mathbb{K}}$ *over* $\mathbb{K}$. *Then*

(a) [**a**] $\mathbb{F} = \mathbb{K}[\xi]$ *for any* $\xi \in U_n^*(\mathbb{F})$.

(b) [**b**] $K \leq \mathbb{F}$ *is Galois.*

(c) [**c**] $\operatorname{Aut}_{\mathbb{K}}(\mathbb{F})$ *is isomorphic to a subgroup of* $(\mathbb{Z}_n^*, \cdot)$. *In particular,* $\operatorname{Aut}_{\mathbb{K}}(\mathbb{F})$ *is abelian.*

(d) [**d**] *If* $\mathbb{K} = \mathbb{Q}$, *then* $\dim_{\mathbb{K}} \mathbb{F} = \phi(n)$ *and* $\operatorname{Aut}_{\mathbb{K}}(\mathbb{F}) \cong (\mathbb{Z}_n^*, \cdot)$.

Proof. (a) By 4.7.29(a), $U_n(\mathbb{F}) = \langle \xi \rangle \subseteq \mathbb{K}[\xi]$. Thus

$$F = \mathbb{K}[U_n(\mathbb{F})] \subseteq \mathbb{K}[\xi] \subseteq \mathbb{F}$$

So (a) holds.

(b) Since $\operatorname{char} \mathbb{F} \nmid n$, $x^n - 1_{\mathbb{F}}$ is separable. Thus by 4.5.14, $\mathbb{K} \leq \mathbb{F}$ is Galois.

(c) Let $\sigma \in \operatorname{Aut}_{\mathbb{K}}(\mathbb{F})$. Then $|\sigma(\xi)| = |xi| = n$ and $\sigma(\xi) \in U_n^{(}\mathbb{K})$. Let τ be as in 4.7.29 and define $f(\sigma) = \tau^{-1}(\sigma(\xi)$. The $f(\alpha) \in \mathbb{Z}_n^*$ and $f(\sigma) = k + n\mathbb{Z}$ if and only if $\sigma(\xi) = \xi^n$. We will show that $f : \operatorname{Aut}_{\mathbb{K}}(\mathbb{F}) \to (\mathbb{Z}_n^*, \cdot)$ is a homomorphism. So let $\sigma, \mu \in \operatorname{Aut})\mathbb{K}(\mathbb{F})$ and $f(\sigma) = k + n\mathbb{Z}$ and $f(\mu) = l + n\mathbb{Z}$ for some $k, l \in \mathbb{Z}$. Then

$$(\sigma \circ \mu)(\xi) = \sigma(\mu(\xi)) = \sigma(\xi^l)) = \sigma(\xi)^k = (\xi^k)^l = \xi^{kl}$$

and so

$$f(\sigma \circ \mu) = kl + n\mathbb{Z} = (k + n\mathbb{Z})(l + n\mathbb{Z}) = f(\sigma)f(\mu).$$

Thus f is a homomorphism. Let $\sigma \in \ker f$. Then $f(\sigma) = 1 + n\mathbb{Z}$ and $\sigma(\xi) = \xi^1 = \xi$. Thus $\operatorname{Fix}_{\mathbb{F}}(\sigma)$ is a subfield of $\mathbb{F}$ containing $\mathbb{K}$ and ξ. Hence by (a), $\sigma = \mathrm{id}_{\mathbb{F}}$ and so f is 1-1.

(d) By 4.7.32, Φ_n is irreducible over $\mathbb{Q}$. Thus Φ_n is an irreducible monic polynomial with ξ as a root. Hence Φ_n is the minimal polynomial of ξ over $\mathbb{Q}$ and

$$\dim_{\mathbb{K}} \mathbb{F} = \dim_{\mathbb{K}} \mathbb{K}[\xi] = \deg \Phi_n = \phi(n).$$

So by 4.5.8, $|\operatorname{Aut}_{\mathbb{K}}(\mathbb{F})| = \phi(n) = |\mathbb{Z}_n^*|$ and so f must be onto. Hence f is an isomorphism and (d) holds. □

Lemma 4.7.34. [**n root constructable**] *Let* $n \in \mathbb{Z}^+$. *Then* $\frac{2\pi}{n}$ *is an constructable angle if and only if* $n = 2^k p_1 p_2 p_3 \dots p_m$, *where* $k \in \mathbb{N}$ *and* $p_1, p_2, \dots, p_m$ *are pairwise distinct Fermat primes. Here a prime* p *is called a Fermat prime, if* $p = 2^t + 1$, *for some* $t \in \mathbb{Z}^+$.

Proof. Let $\xi = e^{\frac{2\pi}{n}}$. Then ξ is a primitive n-root of unity in $\mathbb{C}$. Put $\mathbb{F} = \mathbb{Q}[\xi]$. Then by 4.7.33 $\mathbb{F}$ is a splitting field for $x^n - 1$ over $\mathbb{Q}$, $\mathbb{Q} \leq \mathbb{F}$ is Galois and $\dim_{\mathbb{Q}} \mathbb{F} = \phi(n)$. Put $a = \cos(\frac{2\pi}{n}$ and $b = \sin(\frac{2\pi}{n}$. Then $\xi = a + bi$ and so $a = \frac{1}{2}(\xi + \overline{\xi})$. Since $\overline{x}i$ is also a n-root of unity, $\overline{\xi} \in \mathbb{F}$ and so also $a \in \mathbb{F}$. Put $\mathbb{E} = \mathbb{Q}[a]$. By 4.7.33 $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{F})$ is abelian and so all subgroups of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{F})$ are normal. Thus by the FTGT, $\mathbb{K} \leq \mathbb{E}$ is normal. Thus $m_a^{\mathbb{Q}}$ splits over $\mathbb{E}$ and so $\mathbb{E}$ is a splitting field for a over $\mathbb{Q}$. Note that $\xi\overline{\xi} = a^2 + b^2 = 1$. Thus $(x - \xi)(x - \overline{\xi}) = x^2 - 2ax + 1 \in \mathbb{E}[x]$. Hence either $\xi \in \mathbb{E}$ or $\dim_{\mathbb{E}} \mathbb{E}[xi] = 2$. Thus $\dim_{\mathbb{E}} \mathbb{F} \leq 2$. Thus

$$\dim_{\mathbb{Q}} \mathbb{F} = \dim_{\mathbb{Q}} \mathbb{F} \text{ or } \dim_{\mathbb{Q}} \mathbb{F} = 2\dim_{\mathbb{Q}} \mathbb{E}$$

We have

$$\begin{array}{lcl}
 & \frac{2\pi}{n} \text{ is a constructable angle} & \\
\iff & a \text{ is a constructable} & \\
\iff & \dim_{\mathbb{Q}} \mathbb{E} \text{ is a power of } 2 & -4.7.9 \\
\iff & \dim_{\mathbb{Q}} \mathbb{F} \text{ is a power of } 2 & \\
\iff & \phi(n) \text{ is a power of } 2. &
\end{array}$$

Let $n = 2^k p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m}$, where $k, m \in \mathbb{N}$, $p_1, p_2 \ldots, p_m$ are pairwise distinct primes and $n_1, \ldots, n_m \in \mathbb{Z}^+$.

If $k = 0$, then $\phi(n) = \prod_{i=1}^{n} p_i^{n_i - 1}(p_i - 1)$ and if $k > 0$, $\phi(n) = 2^{k-1} \prod_{i=1}^{n} p_i^{n_i - 1}(p_i - 1)$ if follows that $\phi(n)$ is a power of 2 if and only if $n_i = 1$ and $p_i - 1$ is a power of 2 for all $1 \leq i \leq m$. □

4.7.35 (Fermat primes)**.** [**fermat**] For which $n \in \mathbb{N}$ is $2^n + 1$ a prime?

$2^0 + 1 = 2$ yes
$2^1 + 1 = 2 + 1 = 3$ yes
$2^2 + 1 = 4 + 1 = 5$ yes
$2^3 + 1 = 8 = 1 = 9$ no
$2^4 + 1 = 16 + 1 = 17$ yes
$2^5 + 1 = 32 + 1 = 33$ no
$2^6 + 1 = 64 + 1 = 65$ no
$2^7 + 1 = 128 + 1 = 129$ no
$2^8 + 1 = 256 + 1 = 257$ yes.

It seems that $2^n + 1$ is a prime if and only if n is a power of 2. But only the forward direction turns out to be true. If $2^n + 1$ is a prime, then n is a power of 2. Indeed suppose n is not a power two. Then $n = rs$, $r, s \in \mathbb{Z}^+$, $r < n$ and s odd. Since $\frac{a^n - b^n}{a - b} = \sum_{i=0}^{n-1} a^i b^{n-i}$, $a - b$ divides $a^n - b^n$ for any integers a, b. Since $2^n + 1 = 2^{rs} + 1 = (2^r)^s - (-1)^s$ we conclude that $2^r - (-1)$ divides $2^n - 1$. Since $1 < 2^r + 1 < 2^n + 1$ we conclude that $2^n + 1$ is not a prime, Thus if $2^n + 1$ is a prime, then n is a power of 2.

$2^{16}+1 = 65537$ is a prime.
$2^{32}+1 = 4294967297 = 641 \cdot 6700417$
$2^{64}+1 = 18446744073709551617 = 27417 \cdot 67280421310721$

No Fermat Primes other than the first five is known. For the first five explicit construction of corresponding m-gon are known. The last one, $m = 2^{16}+1$, took 10 years to construct (Hermes, around 1900)

Here is an fairly easy proof that 641 divides $2^{32}+1$:
$641 = 625 + 16 = 5^4 + 2^4$. Hence

$$611 \mid (5^4 + 2^4)2^{28} = 5^4 2^{28} + 2^{32}.$$

$641 = 640+1 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1$ and so 641 divides $(5\cdot 2^7+1)(5\cdot 2^7-1) = 5^2 \cdot 2^{14} - 1$. Hence

$$641 \mid (5^2 \cdot 2^{14} - 1)(5^2 \cdot 2^{14} + 1) = 5^4 2^{28} - 1.$$

Thus

$$641 \mid (5^4 2^{28} + 2^{32}) - (5^4 2^{28} - 1) = 2^{32} + 1$$

4.8 Wedderburn's Theorem

Lemma 4.8.1. [**nt for wedderburn**] *Let $q, n, m \in \mathbb{Z}^+$ with $q \geq 2$. Suppose that $q^m - 1$ divides $q^n - 1$ in $\mathbb{Z}$. Then $m \mid n$ and if $m < n$ then $\Phi_n(q) \mid \frac{q^n-1}{q^t-1}$.*

Proof. Let $n = km + r$ with $k, r \in \mathbb{N}$ and $0 \leq r < m$. Then $q^m - 1$ divides $q^{km} - 1$ and so also

$$(q^n - 1) - (q^{km} - 1) = q^{km+r} - q^{km} = q^{km}(q^r - 1)$$

Since $\gcd(q^m - 1, q^{km}) = 1$ we conclude that $q^m - 1$ divides $q^r - 1$. Since $q^r - 1 < q^m - 1$ this implies $q^r - 1 = 0$ and so $r = 0$ and $m \mid n$.

Suppose now that $m < n$. Put $f := \prod_{1 \leq d < n. d|n, d\nmid m} \Phi_d$. Then $f \in \mathbb{Z}[x]$ and

$$x^n - 1 = \prod_{1 \leq d \leq n, d|n} \Phi_d = \Phi_n \prod_{1 \leq d \leq m, d|m} \prod_{1 \leq d < n, d|n, d\nmid n} = \Phi_n \cdot (x^m - 1) \cdot f$$

Thus $\frac{x^n-1}{x^m-1} = f \cdot \Phi_n$ and so

$$\frac{q^n - 1}{q^m - 1} = f(q)\Phi_n(q)$$

□

Theorem 4.8.2 (Wedderburn)**.** [**wedderburn**] *Every finite division ring is a field*

Proof. Let $\mathbb{D}$ be a finite division ring and put $\mathbb{K} = \mathrm{Z}(\mathbb{D}) = \{a \in \mathbb{D} \mid ad = de \text{ for all } d \in \mathbb{D}\}$. Then $\mathbb{K}$ is a subfield of $\mathbb{D}$ containing $0_{\mathrm{D}}, 1_{\mathbb{D}}$. Note that $\mathbb{K}^\sharp = \mathrm{Z}(\mathrm{D}^\sharp)$. Put $q := |\mathbb{K}|$. Then $q \leq 2$. Let $\mathcal{R}$ be a set of representatives for the conjugacy classes of $D^\sharp$ and put $\mathcal{T} := \mathcal{R} \setminus \mathrm{Z}(\mathbb{D}^\sharp)$. Then by the class equation 2.7.24

$$(*) \qquad |\mathbb{D}^\sharp| = |\mathbb{K}^\sharp| + \sum_{t \in \mathcal{T}} |\mathbb{D}^\sharp / \mathrm{C}_{\mathbb{D}^\sharp}(t)|.$$

For $r \in \mathcal{R}$ let $\mathrm{C}_{\mathbb{D}}(r) := \{a \in \mathbb{D} \mid ar = ra\}$. So $\mathrm{C}_{\mathbb{D}}(t)^\sharp = \mathrm{C}_{\mathbb{D}^\sharp}(t)$. Note that $\mathbb{D}$ is a $\mathbb{K}$ space via left multiplication. Since $\mathbb{D}$ is finite, $\mathbb{D}$ is a finite dimensional $\mathbb{K}$-space. We claim that $\mathrm{C}_{\mathbb{D}}(r)$ is a $\mathbb{K}$-subspace of $\mathbb{D}$. . Indeed if $a, b \in \mathrm{C}_{\mathbb{D}}(r)$ and $k \in \mathbb{K}$, then

$$(a+b)r = ar + br = ra + rb = r(a+b)$$

and

$$(ka)r = k(ar) = k(ra) = (ra)k = r(ak) = r(ka).$$

Put $n_r = \dim_{\mathbb{D}} \mathrm{C}_{\mathbb{D}}(r)$. Then $\mathrm{C}_{\mathbb{D}}(r) \cong \mathbb{F}^{n_r}$ as a $\mathbb{K}$-space and so

$$|\mathrm{C}_{\mathbb{D}}(r)| = q^{n_r}.$$

Put $n = n_{1_{\mathbb{D}}}$. Then $|\mathbb{D}| = |\mathrm{C}_{\mathbb{D}}(1_{\mathbb{D}}) = q^n$. (*) now gives

$$(**) \qquad q^n - 1 = (q-1) + \sum_{t \in \mathcal{T}} \frac{q^n - 1}{q^{n_t} - 1}.$$

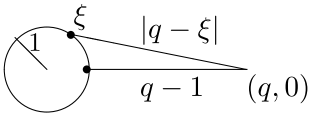
Let $t \in \mathcal{T}$. Then $t \notin \mathrm{Z}(D)$ and so $\mathrm{C}_{\mathbb{D}}(t) \neq \mathbb{D}$ and $n_t < n$. 4.8.1 shows that $\Phi_n(q)$ divides $\frac{q^n-1}{q^{n_t}-1}$. Also $\Phi_n \mid x^n - 1$ and so $\Phi_n(q) \mid q^n - 1$. Hence and implies that $\Phi_n(q) \mid q - 1$ in $\mathbb{Z}$. Thus

$$(***) \qquad |\Phi_n(q)| \leq q - 1.$$

Put $U = U_n^*(\mathbb{C})$. Then $\Phi_n = \prod_{\xi \in U}(x - \xi)$ and so

$$|\Phi_n(q)| = \left| \prod_{\xi \in U} (q - \xi) \right| = \prod_{\xi \in U} |q - \xi|$$

Let $\xi \in U$. From the picture



we conclude that $|\Phi_n(q)| \geq |\xi - q| > q - 1$ unless $\xi = 1$. Thus (***) gives $\xi = 1$ and $n = 1$. Hence $\dim_{\mathbb{F}} \mathbb{D} = 1$ and $\mathbb{F} = \mathbb{D}$. So $\mathbb{D}$ is a field. □

Appendix A

A.1 The Binomial Theorem

Definition A.1.1. [**def:binomial**] *Let $n, k \in \mathbb{N}$ with $k \leq n$.*

(a) [**a**] $0! = 1$ *and inductively* $(n+1)! := (n+1)n!$.

(b) [**b**] $\binom{n}{k} := \frac{n!}{k!(n-k)!}$.

Lemma A.1.2. [**binomial**] *Let $m, k \in \mathbb{N}$ with $k \leq n$.*

(a) [**a**] $\binom{n}{k} = \binom{n}{n-k}$, $\binom{n}{0} = 1 = \binom{n}{n}$ *and* $\binom{n}{1} = n = \binom{n}{n-1}$.

(b) [**b**] *Suppose $n, k \geq 1$. Then*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Proof.

[**a**] Readily verified.

[**b**]

$$\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k(n-1-k)} + \frac{(n-1)!}{(k-1)!(n-k)!} &&= \frac{(n-1)!}{(k-1)!(n-1-k)!}\left(\frac{1}{k} + \frac{1}{n-k}\right) \\
&= \frac{(n-1)!}{(k-1)!(n-1-k)!}\frac{(n-k)+k}{k(n-k)} &&= \frac{(n-1)!}{(k-1)!(n-1-k)!}\frac{n}{k(n-k)} \\
&= \frac{n!}{k!(n-k)!} &&= \binom{n}{k}
\end{aligned}$$

□

Lemma A.1.3. [**binomial theorem**] *Let R be a ring with identity and $a, b \in R$ with $ab = ba$. Let $n \in \mathbb{N}$. Then*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

Proof. If $n = 0$ the both sides are equal to 1_R. So suppose $n > 1$ and that the lemma holds for $n - 1$.

Then

$$\begin{aligned}
(a+b)^n &= (a+b)(a+b)^{n-1} \\
&= (a+b)\left(\textstyle\sum_{i=0}^{n-1} \binom{n-1}{i} a^i b^{n-1-i}\right) \\
&= \left(\textstyle\sum_{i=0}^{n-1} \binom{n-1}{i} a^{i+1} b^{n-1-i}\right) + \left(\textstyle\sum_{i=0}^{n-1} \binom{n-1}{i} a^i b^{n-i}\right) \\
&= \left(\textstyle\sum_{i=1}^{n} \binom{n-1}{i-1} a^i b^{n-i}\right) + \left(\textstyle\sum_{i=0}^{n-1} \binom{n-1}{i} a^i b^{n-i}\right) \\
&= \binom{n-1}{n-1} a^n b^0 + \left(\textstyle\sum_{i=1}^{n-1} \left(\binom{n-1}{i-1} + \binom{n-1}{i}\right) a^i b^{n-i}\right) + \binom{n-1}{0} a^0 b^n \\
&= \binom{n}{n} a^n b^0 + \left(\textstyle\sum_{i=1}^{n-1} \binom{n}{i} a^i b^{n-1}\right) + \binom{n}{0} a^0 b^n \\
&= \textstyle\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}
\end{aligned}$$

□

Bibliography

[Gro] Larry C. Grove, *Algebra* Pure and Applied Mathematics 110, Academic Press, (1983) New Work.

[Herstein] I.N. Herstein, *TOPICS IN ALGEBRA*, 2nd edition, John Wiley & Sons (1975)

[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.

[Lay] David. C. Lay *Linear Algebra and its Applications* Third Edition (Update) Pearson Education, Addison Wesley (2006)

Index