A.3 Special Topics

A.3.1 The Euclidean algorithm

Let F be a field. In Theorem A.2.16 we gave a nonconstructive proof for the existence of the greatest common divisor of two polynomials $a(x)$ and $b(x)$ of $F[x]$. The Euclidean algorithm is an algorithm that constructs $\gcd(a(x), b(x))$ explicitly. The basic method is simple. If $q(x)$ is any polynomial, then

$$\gcd(a(x), b(x)) = \gcd(a(x) - q(x)b(x), b(x)).$$

In particular, $a(x)$ can be replaced in the calculation by its remainder $r(x)$ upon division by $b(x)$. Assuming that $a(x)$ has degree at least as big as that of $b(x)$, the remainder $r(x)$ will have smaller degree than $a(x)$; so the gcd of the original pair of polynomials will be equal to the gcd of a new pair with smaller total degree. We can continue in this fashion decreasing the degree of the remainder at each stage until the process stops with remainder 0, and at this point the gcd becomes clear.

In fact the approach we take is a little different. From our proof of Theorem A.2.16 we know that $\gcd(a(x), b(x))$ is the monic polynomial of minimal degree within the set

$$G = \{\, s(x)a(x) + t(x)b(x) \mid s(x), t(x) \in F[x] \,\}$$

Thus we examine all equations of the form

$$p(x) = s(x)a(x) + t(x)b(x)\,,$$

looking for one in which nonzero $p(x)$ has minimal degree. The unique monic scalar multiple of this $p(x)$ is then equal to $\gcd(a(x), b(x))$.

If we have two suitable equations:

$$m(x) = e(x)a(x) + f(x)b(x)\,; \tag{A.1}$$

$$n(x) = g(x)a(x) + h(x)b(x)\,; \tag{A.2}$$

then we can find a third with lefthand side of smaller degree. Assume that the degree of $m(x)$ is at least as big as that of $n(x)$. By the Division Algorithm A.2.5 there are $q(x)$ and $r(x)$ with $m(x) = q(x)n(x)+r(x)$and $\deg(r(x)) < \deg(n(x))$. Subtracting $q(x)$ times equation (2) from equation (1) we have the desired

$$r(x) = m(x) - q(x)n(x) = \tag{A.3}$$
$$\Big(e(x) - q(x)g(x)\Big)a(x) + \Big(f(x) - q(x)h(x)\Big)b(x).$$

Next we may divide $r(x)$ into $n(x)$ and, using equations (2) and (3), further reduce the degree of the lefthand side. Continuing as before we must ultimately arrive at an equation with 0 on the left. The lefthand side of the previous equation will then have the desired minimal degree. A benefit of this method of

calculation is that the appropriate polynomials $s(x)$ and $t(x)$ are produced at the same time as the gcd.

To succeed with this approach we must have two equations to begin with. These are provided by:

$$a(x) = 1 \cdot a(x) + 0 \cdot b(x); \tag{A.4}$$
$$b(x) = 0 \cdot a(x) + 1 \cdot b(x). \tag{A.5}$$

(A.3.1) THEOREM. *(THE EUCLIDEAN ALGORITHM.)*
Assume that $\deg(a(x)) \geq \deg(b(x))$ *with* $a(x) \neq 0$. *At Step i we construct the equation*

$$\mathbf{E_i} : r_i(x) = s_i(x)a(x) + t_i(x)b(x).$$

Equation $\mathbf{E_i}$ *is constructed from* $\mathbf{E_{i-1}}$ *and* $\mathbf{E_{i-2}}$, *the appropriate initialization being provided by (4) and (5):*

$$r_{-1}(x) = a(x); \quad s_{-1}(x) = 1; \quad t_{-1}(x) = 0;$$
$$r_0(x) = b(x); \quad s_0(x) = 0; \quad t_0(x) = 1.$$

Step i. Starting with $r_{i-2}(x)$ *and* $r_{i-1}(x)$ $(\neq 0)$ *use the Division Algorithm A.2.5 to define* $q_i(x)$ *and* $r_i(x)$*:*

$$r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x) \text{ with } \deg(r_i(x)) < \deg(r_{i-1}(x)).$$

Next define $s_i(x)$ *and* $t_i(x)$ *by:*

$$s_i(x) = s_{i-2}(x) - q_i(x)s_{i-1}(x);$$
$$t_i(x) = t_{i-2}(x) - q_i(x)t_{i-1}(x).$$

We then have the equation

$$\mathbf{E_i} : r_i(x) = s_i(x)a(x) + t_i(x)b(x).$$

Begin with $i = 0$. *If we have* $r_i(x) \neq 0$, *then proceed to Step i+1. Eventually there will be an i with* $r_i(x) = 0$. *At that point halt and declare* $\gcd(a(x), b(x))$ *to be the unique monic scalar multiple of the nonzero polynomial* $r_{i-1}(x)$.

PROOF. For each i, $r_i(x) = r_{i-2}(x) - q_i(x)r_{i-1}(x)$; so $\mathbf{E_i}$ holds. This also shows that

$$\gcd(r_{i-1}(x), r_i(x)) = \gcd(r_{i-2}(x), r_{i-1}(x))$$
$$= \cdots = \gcd(r_{-1}(x), r_0(x)) = \gcd(a(x), b(x)).$$

As long as $i \geq 0$ and $r_i(x) \neq 0$, $\deg(r_{i+1}(x)) < \deg(r_i(x))$. Thus in at most $\deg(b(x))$ steps $r_i(x) = 0$ is reached. Then $\gcd(r_{i-1}(x), 0) = \gcd(a(x), b(x))$ is the unique monic multiple of $r_{i-1}(x)$, completing verification of the algorithm. □

(A.3.2) PROBLEM.
(a) *Prove that* $q_i(x)$ *of Theorem A.3.1 has positive degree, for all* $i \geq 2$.
(b) *Prove that* $\deg(s_i(x))$ *and* $\deg(t_i(x))$ *are increasing functions of* $i \geq 1$.

We can think of the Euclidean algorithm as finding a new equation $\mathbf{E_i}$ from the previous two via

$$\mathbf{E_i} = -q_i(x)\mathbf{E_{i-1}} + \mathbf{E_{i-2}}\,.$$

This provides the entry to another presentation of the Euclidean algorithm that for certain purposes is quite helpful.

Consider the matrix with entries from $F[x]$

$$R_0 = \begin{bmatrix} a(x) & 1 & 0 \\ b(x) & 0 & 1 \end{bmatrix}\,.$$

We wish, by elementary row operations over $F[x]$, to reduce this matrix to echelon form

$$R = \begin{bmatrix} p(x) & * & * \\ 0 & * & * \end{bmatrix}\,,$$

where in fact $p(x) = \gcd(a(x), b(x))$. For each $i > 1$, set

$$Q_i = \begin{bmatrix} 0 & 1 \\ 1 & -q_i(x) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -q_i(x) \\ 0 & 1 \end{bmatrix}\,,$$

a product of the matrices for two elementary row operations. Then after defining

$$R_i = \begin{bmatrix} r_{i-1}(x) & s_{i-1}(x) & t_{i-1}(x) \\ r_i(x) & s_i(x) & t_i(x) \end{bmatrix}\,,$$

we find that $R_i = Q_i R_{i-1}$, for all $i \geq 1$. Therefore left multiplication by Q_i can be thought of as accomplishing *Step i* of the Euclidean algorithm. Because $(1, -a(x), -b(x))^\top$ is a null vector of R_0, it is also a null vector of each R_i. That is, for each i we have the equation

$$\mathbf{E_i} : r_i(x) = s_i(x)a(x) + t_i(x)b(x).$$

When first $r_i(x) = 0$, then $r_{i-1}(x)$ is a scalar multiple of $\gcd(a(x), b(x))$; so the desired matrix R can be realized as a scalar multiple of R_i.

For each $i \geq 1$, set $S_i = \prod_{j=1}^{i} Q_j$, so that $S_i R_0 = R_i$. Each Q_j has determinant equal to -1 (see Problem A.1.15), so S_i has determinant $(-1)^i$. If, for each i, we define $R_i(r,t)$ (respectively, $R_i(s,t)$) to be the 2×2 submatrix of R_i composed of the r- and t-columns (resp., s- and t-columns), then we have

$$S_i \begin{bmatrix} a(x) & 0 \\ b(x) & 1 \end{bmatrix} = S_i R_0(r,t) = R_i(r,t) = \begin{bmatrix} r_{i-1}(x) & t_{i-1}(x) \\ r_i(x) & t_i(x) \end{bmatrix}\,.$$

Similarly

$$S_i \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = S_i R_0(s,t) = R_i(s,t) = \begin{bmatrix} s_{i-1}(x) & t_{i-1}(x) \\ s_i(x) & t_i(x) \end{bmatrix}.$$

Calculating determinants, we have a proof of

(A.3.3) LEMMA. (1) $r_{i-1}(x)t_i(x) - r_i(x)t_{i-1}(x) = (-1)^i a(x)$, for $i \geq 0$.
(2) $s_{i-1}(x)t_i(x) - s_i(x)t_{i-1}(x) = (-1)^i$, for $i \geq 0$. □

(A.3.4) COROLLARY. $\gcd(s_i(x), t_i(x)) = 1$, *for all* $i \geq -1$.

PROOF. This follows from Lemma A.3.3(2) and Theorem A.2.16. □

(A.3.5) PROBLEM. *Prove that* $\deg(r_{i-1}(x)) + \deg(t_i(x)) = \deg(a(x))$, *for all* $i \geq 0$. *(*HINT: *use Problem A.3.2(b) and Lemma A.3.3(1).)*

(A.3.6) PROBLEM.
(a) *Prove that* $r_{i-1}(x)s_i(x) - r_i(x)s_{i-1}(x) = (-1)^{i+1}b(x)$, *for all* $i \geq 0$.
(b) *Prove that* $\deg(r_{i-1}(x)) + \deg(s_i(x)) =$ *deg*$(b(x))$, *for all* $i \geq 1$.

A Euclidean Algorithm example

We calculate $\gcd(x^4, 4x^3+3x^2+5x) = x$ over $\mathbb{F}_7$ using the Euclidean algorithm. At Step i we define $q_i(x)$, $r_i(x)$, $s_i(x)$, and $t_i(x)$ using

$$\begin{aligned} r_{i-2}(x) &= q_i(x)r_{i-1}(x) + r_i(x) \\ s_i(x) &= s_{i-2}(x) - q_i(x)s_{i-1}(x) \\ t_i(x) &= t_{i-2}(x) - q_i(x)t_{i-1}(x)\ . \end{aligned}$$

Step i	$q_i(x)$	$r_i(x)$	$s_i(x)$	$t_i(x)$
-1	–	x^4	1	0
0	–	$4x^3+3x^2+5x$	0	1
1	$2x+2$	$5x^2+4x$	1	$5x+5$
2	$5x+5$	**6x**	$2x+2$	$3x^2+6x+4$
3	$2x+3$	0	$3x^2+4x+2$	x^3

Step 1.

$$\begin{array}{rrrrrrrrl} & & & & & & 2x & +2 & = q_1(x) \\ r_0(x) = & 4x^3 & +3x^2 & +5x & \big| & x^4 & & & = r_{-1}(x) \\ & & & & & x^4 & +6x^3 & +3x^2 & \\ \hline & & & & & & x^3 & +4x^2 & \\ & & & & & & x^3 & +6x^2 & +3x \\ \hline & & & & & & & 5x^2 & +4x \quad = r_1(x) \end{array}$$

$$\begin{aligned} r_{-1}(x) &= q_1(x)r_0(x) + r_1(x) \\ x^4 &= (2x+2)(4x^3+3x^2+5x) + (5x^2+4x) \\ q_1(x) &= 2x+2 \\ r_1(x) &= 5x^2+4x \end{aligned}$$

$$\begin{aligned} s_1(x) &= s_{-1}(x) - q_1(x)s_0(x) \\ s_1(x) &= 1 - (2x+2)0 = 1 \end{aligned}$$

$$\begin{aligned} t_1(x) &= t_{-1}(x) - q_1(x)t_0(x) \\ t_1(x) &= 0 - (2x+2)1 = 5x+5 \end{aligned}$$

Step 2.

$$\begin{aligned} r_0(x) &= q_2(x)r_1(x) + r_2(x) \\ 4x^3 + 3x^2 + 5x &= (5x+5)(5x^2+4x) + 6x \\ q_2(x) &= 5x+5 \\ r_2(x) &= 6x \end{aligned}$$

$$\begin{aligned} s_2(x) &= s_0(x) - q_2(x)s_1(x) \\ s_2(x) &= 0 - (5x+5)1 = 2x+2 \end{aligned}$$

$$\begin{aligned} t_2(x) &= t_0(x) - q_2(x)t_1(x) \\ t_2(x) &= 1 - (5x+5)(5x+5) = 3x^2+6x+4 \end{aligned}$$

Step 3.

$$\begin{aligned} r_1(x) &= q_3(x)r_2(x) + r_3(x) \\ 5x^2 + 4x &= (2x+3)(6x) + 0 \\ q_3(x) &= 2x+3 \\ r_3(x) &= 0 \end{aligned}$$

$$\begin{aligned} s_3(x) &= s_1(x) - q_3(x)s_2(x) \\ s_3(x) &= 1 - (2x+3)(2x+2) = 3x^2+4x+2 \end{aligned}$$

$$\begin{aligned} t_3(x) &= t_1(x) - q_3(x)t_2(x) \\ t_3(x) &= (5x+5) - (2x+3)(3x^2+6x+4) \\ &= (5x+5) - (6x^3+5x+5) = -6x^3 = x^3 \end{aligned}$$

As $r_3(x) = 0$, $\gcd(x^4, 4x^3+3x^2+5x)$ is the unique monic scalar multiple of $r_2(x) = 6x$. Thus $\mathbf{x = gcd(x^4, 4x^3 + 3x^2 + 5x)}$, as claimed.

We should also have $r_2(x) = s_2(x)x^4 + t_2(x)(4x^3+3x^2+5x)$ and therefore $x = 6r_2(x) = 6s_2(x)x^4 + 6t_2(x)(4x^3+3x^2+5x)$. We check:

$$\begin{aligned} 6r_2(x) &= 6s_2(x)x^4 + 6t_2(x)(4x^3+3x^2+5x) \\ &= 6(2x+2)x^4 + 6(3x^2+6x+4)(4x^3+3x^2+5x) \\ &= (5x+5)x^4 + (4x^2+x+3)(4x^3+3x^2+5x) \\ &= (5x^5+5x^4) + (2x^5+5x^4+6x^3) + \\ &\qquad +(4x^4+3x^3+5x^2) + (5x^3+2x^2+x) \\ &= x \text{ !!} \end{aligned}$$

A.3.2 Finite Fields

Consider a finite field F of characteristic p. (Remember from Lemma A.1.3 that this says 1 lies in a subfield of F that is a copy of $\mathbb{F}_p$.) Let α be any element of F. Any subfield (indeed any subring) of F that contains both the subfield $\mathbb{F}_p$ and α must contain the set E of all polynomials in α with coefficients in $\mathbb{F}_p$:

$$E = \{\, a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_k\alpha^k \mid a_i \in \mathbb{F}_p, k > 0\}.$$

Notice however that in this instance α is not an indeterminate; there are going to be various different polynomials $f(x)$ in $\mathbb{F}_p[x]$ that represent the same element $f(\alpha)$ of F. Indeed as F is finite while $\mathbb{F}_p[x]$ is infinite, this must be the case. As in the proof of Lemma A.1.3 this forces the set

$$I = \{\, \text{all polynomials } f(x) \in \mathbb{F}_p[x] \text{ with } f(\alpha) = 0 \,\}$$

to contain polynomials other than the constant polynomial 0. As in Theorem A.2.18, the greatest common divisor of the set I, $m(x) = \gcd(I)$, is called the *minimal polynomial* of α over $\mathbb{F}_p$ and is usually denoted $m_\alpha(x)$ (but also sometimes $m_{\alpha,\mathbb{F}_p}(x)$). The set I then consists of all members of $F[x]$ that are multiples of $m_\alpha(x)$. That is, the polynomial $m_\alpha(x)$ is uniquely determined in $\mathbb{F}_p[x]$ as a monic polynomial with α as a root that divides all polynomials with α as a root. We observe that a minimal polynomial must always be irreducible. Indeed if $m(x) = f(x)g(x)$, then $0 = m(\alpha) = f(\alpha)g(\alpha)$ whence $f(\alpha) = 0$ or $g(\alpha) = 0$. Therefore at least one of $f(x)$ and $g(x)$ is in I, but the greatest common divisor $m(x)$ of I has minimal degree among the nonzero elements of I.

minimal polynomial

Let us now examine the set E. E is closed under addition and multiplication and contains 0 and 1. Thus E is at least a subring of F. Furthermore no two nonzero members of E have product 0, as this is true in F itself. Thus E is moreover a sub-integral domain of F. Now Problem A.1.2 shows that E is in fact a subfield of F, indeed the smallest subfield of F that contains α. (All subfields contain 1 and so all of $\mathbb{F}_p$.) What is the arithmetic of the subfield E?

Let us assume that the minimal polynomial $m(x)$ has degree d (greater than 0). Then by the division algorithm every polynomial $f(x)$ of $\mathbb{F}_p[x]$ has a unique remainder $r(x)$ of degree less than d upon division by $m(x)$, and $f(\alpha) = r(\alpha)$ as $m(\alpha) = 0$. Thus in fact

$$E = \{\, r(\alpha) \,|\, r(x) \in \mathbb{F}_p[x] \text{ of degree } < d \,\}.$$

Furthermore two distinct polynomials $r_1(x), r_2(x) \in \mathbb{F}_p[x]_d$ can not have $r_1(\alpha) = r_2(\alpha)$, because their difference would then be a nonzero polynomial of degree less than d having α as a root. Such a polynomial would belong to I, whereas $m(x)$ has minimal degree among all nonzero members of I. In particular E has exactly p^d elements. Note also that for polynomials $a(x), b(x) \in \mathbb{F}_p[x]$ we have in E that $a(\alpha)b(\alpha) = r(\alpha)$, where $r(x)$ is the remainder of $a(x)b(x)$ upon division by $m(x)$. Thus the arithmetic of E is exactly that of $\mathbb{F}_p[x] \pmod{m(x)}$. Indeed we have:

(A.3.7) LEMMA. *Let F be a finite field of characteristic p, and let α be an arbitrary element of F. Then the smallest subfield E of F that contains α is a copy of the field $\mathbb{F}_p[x] \pmod{m_\alpha(x)}$ where $m_\alpha(x)$ is the minimal polynomial of α over $\mathbb{F}_p$.* □

We next examine a result of great theoretical and practical importance.

(A.3.8) THEOREM. *Let F be a finite field with $|F| = q$. Then there is an element α in F with the property that*

$$F - \{0\} = \{\, \alpha, \alpha^2, \ldots, \alpha^{q-2}, \alpha^{q-1} = \alpha^0 = 1\}.$$

PROOF. We first observe that for any nonzero α of F, the set

$$X = \{\, \alpha, \alpha^2, \ldots, \alpha^i, \ldots \mid i \in \mathbb{Z}^+\}$$

is finite and contained within $F - \{0\}$. As before this implies that, for each nonzero α of F, there is a positive integer n (depending upon α) with $\alpha^n = 1$. The smallest such positive n is called the *order* of α. Among all the nonzero elements of F choose α one of maximal order n, say. Note that the statement that α has order n is equivalent to the statement that the set X contains exactly n elements of F. Additionally for each $\beta = \alpha^i$ of X we have $\beta^n = (\alpha^i)^n = (\alpha^n)^i = 1^i = 1$. The crucial point in the proof is that X, for our choice of α, is precisely the set of all roots in F of the polynomial $x^n - 1$. In particular any element of F with order dividing n must belong to X. An element $\alpha \in F$ is called a *primitive n^{th} root of unity* if it has order n.

order

primitive n^{th} root of unity

Assume now that it is possible to find a nonzero element γ of F that does not belong to X. By the remark at the end of the previous paragraph the order m of g is not a divisor of n. Thus there is a prime s and a prime power s^i that divides m but does not divide n. Let $m = s^i u$ and $n = s^j v$, where i is larger than j and neither u nor v are multiples of s. A somewhat lengthy calculation suffices to check (do it!) that the element $\delta = \alpha^{s^j} \cdot \gamma^u$ has order $s^i v$. As this is larger than n we have contradicted our original choice of α. Therefore no such element γ can be found; and X is all of F, proving the theorem. □

Of course for an α as in Theorem A.3.8, F itself is the smallest subfield of F containing α. Thus from Lemma A.3.7 and Theorem A.3.8 we have:

(A.3.9) THEOREM. *Every finite field F can be written as $\mathbb{F}_p[x] \pmod{m(x)}$ for some prime p and some irreducible polynomial $m(x)$ in $\mathbb{F}_p[x]$.* □

Note that Theorem A.3.9 can be thought of as a converse to Theorem A.2.14 for finite fields.

An α as in Theorem A.3.8 is a primitive $(|F| - 1)^{th}$ root of unity in F and is called a *primitive element* of F. Its minimal polynomial is called a *primitive polynomial*. Thus Theorem A.3.9 remains true with the word 'primitive' in place of 'irreducible'.

primitive element

primitive polynomial

One consequence of Theorem A.3.9 is that a finite field must have the number of its elements equal to a power of a prime (although we already knew this from Problem A.1.6). By Lemma A.1.3 there are fields of prime order for every prime, but what about every prime power? For the time being we are content to state without proof:

(A.3.10) THEOREM. *For each prime p and each positive integer d, there exist fields containing exactly p^d elements.* □

We note that by Theorem A.3.9 this is equivalent to proving that for each p and d there is an irreducible polynomial $m(x)$ in $\mathbb{F}_p[x]$ of degree d.

How do we actually find and calculate in finite fields? Theorem A.3.9 gives the answer. If we want a field F with p^d elements (usually written as $F = GF(p^d)$ or $F = \mathbb{F}_{p^d}$), then we first find an irreducible polynomial $m(x)$ of degree d in $\mathbb{F}_p[x]$ and then realize F as $\mathbb{F}_p[x] \pmod{m(x)}$.

We can check for irreducibility of a given polynomial in a way similar to the Sieve of Eratosthenes — if a polynomial of degree d is reducible, then it must be a multiple of an irreducible polynomial of degree at most $d/2$. For example $x^3 + x + 1 \in \mathbb{F}_2[x]$ is irreducible as it has no nonscalar factor of degree at most $3/2$, that is, it has no linear factors (as it has no roots in $\mathbb{F}_2$). Therefore even though Theorem A.3.10 is quite difficult to prove, it may not too hard to find an irreducible polynomial of a specific desired degree d in $\mathbb{F}_p[x]$. To do so, use the sieve to find all reducible polynomials of degree d, then all the remaining polynomials are irreducible. (There are only finitely many polynomials of a fixed degree in $\mathbb{F}_p[x]$.)

(A.3.11) PROBLEM. (*a*) *Find all irreducible polynomials of degree* 4 *or less in* $\mathbb{F}_2[x]$.
(*b*) *Find all monic irreducible polynomials of degree* 3 *or less in* $\mathbb{F}_3[x]$.
(*c*) *Find all monic irreducible polynomials of degree* 2 *or less in* $\mathbb{F}_4[x]$.
(*d*) *Find all monic irreducible polynomials of degree* 2 *or less in* $\mathbb{F}_5[x]$.

For notational elegance, we usually do not write F as $\mathbb{F}_p[x] \pmod{m(x)}$, but instead as the collection of polynomials of degree less than d in ρ, a root of the degree d irreducible $m(x)$. So, for example, rather than write the complex numbers as $\mathbb{R}[x] \pmod{x^2+1}$ we write them as the set of all $a + bi,\ a, b \in \mathbb{R}$, where i is a root of the irreducible polynomial $x^2 + 1$ of degree 2.

At the end of this section we give an example of a field with 32 elements, $\mathbb{F}_{32}$, written as polynomials of degree less than 5 in a root α of the primitive polynomial $x^5 + x^2 + 1 \in \mathbb{F}_2[x]$. Notice that as α is primitive, we may also write the nonzero elements of $\mathbb{F}_{32}$ as powers of α. This is helpful, because addition in $\mathbb{F}_{32}$ is easily done in terms of the polynomials of degree less than 5 in α, while multiplication is more easily done in terms of the powers of α.

(A.3.12) PROBLEM. (a) *Prove that the polynomial $x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible but not primitive.*

(b) *Let β be a root of the primitive polynomial $x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. Write out a table of the elements of a field with* 16 *elements, $\mathbb{F}_{16}$, both as powers of β and as polynomials of degree less than* 4 *in β.*

The following simple result about finite fields is of great importance.

(A.3.13) LEMMA. *Let K be a field of characteristic p and J a subfield of K.*
(1) *If q is any power of p, then for any $a, b \in K$ we have $(a+b)^q = a^q + b^q$.*
(2) *If $|J| = q$ then $a^q = a$, for all $a \in J$, and J is the complete set of solutions to the equation $x^q = x$ in K.*

PROOF. (1) As $(c^p)^p = c^{p^2}, (c^{p^2})^p = c^{p^3}, \ldots$, we need only prove (1) for $q = p$. In that case it follows easily as each binomial coefficient $\binom{p}{i}$ is 0 modulo p, for $0 < i < p$.
(2) By Theorem A.3.8 $a^q = a$ for all $a \in J$. By Proposition A.2.10 $x^q - x$ has at most q roots in K, and these are exactly the members of J. □

Let D be a subfield of the finite field F, and assume that $D = \mathbb{F}_q$. As F can be viewed as a vector space over D, we must have $F = \mathbb{F}_{q^m}$, for some m. Define the *trace* from F to D of the element $\alpha \in F$ by trace

$$Tr_D(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} .$$

If D is the prime subfield $\mathbb{F}_p$, we often drop the subscript and write Tr for $Tr_{\mathbb{F}_p}$.

(A.3.14) PROPOSITION. (1) *The trace is a map from F onto D.*
(2) *The trace is a D-linear; that is, for all $r_1, r_2 \in D$ and $\alpha_1, \alpha_2 \in F$, we have*

$$Tr_D(r_1\alpha_1 + r_2\alpha_2) = r_1 Tr_D(\alpha_1) + r_2 Tr_D(\alpha_2) .$$

(3) *For a fixed $\beta \in F$, if $Tr_D(\alpha\beta) = 0$ for all α in a D-basis of F, then $\beta = 0$.*

PROOF. It is elementary to prove that the trace is a linear map into D as in (2) using Lemma A.3.13. It is not so clear that the map is actually onto D. The trace is given by a polynomial of degree q^{m-1}, so by Proposition A.2.10 there are at most q^{m-1} elements of F with trace 0. Since the trace is linear, the subset K of elements of F with trace 0 is a D-subspace of F, and the value of the trace map is constant on cosets $\alpha + K$ of K. Again by linearity, different cosets of K give different values. As $|F| = q^m$, there must be the largest possible number $q = |D|$ of values and cosets, and each coset must have the largest possible size, q^{m-1}. This gives (1).
By linearity, if $Tr_D(\alpha\beta) = 0$, for all α in a D-basis for F, then in fact $Tr_D(\alpha\beta) = 0$, for all $\alpha \in F$. But for $\beta \neq 0$, by (1) there are many choices of α with $Tr_D(\alpha\beta) \neq 0$, proving (3). □

(A.3.15) PROBLEM. *Let $T\colon F \to D$ be a D-linear map, that is,*

$$T(r_1\alpha_1 + r_2\alpha_2) = r_1 T(\alpha_1) + r_2 T(\alpha_2) ;$$

and define the map $B\colon F \times F \to D$ by $B(\alpha, \beta) = T(\alpha\beta)$.
(a) *Prove that B is a symmetric D-bilinear map; that is,*

$$B(\alpha, \beta) = B(\beta, \alpha) \text{ and}$$

$$B(r_1\alpha_1 + r_2\alpha_2, \beta) = r_1 B(\alpha_1, \beta) + r_2 B(\alpha_2, \beta), \text{ for all } r_1, r_2 \in D\,.$$

(*b*) *Prove that, conversely, every symmetric D-bilinear map B arises in this fashion from a D-linear map T. (*HINT: *Prove that the map T given by $T(\alpha) = B(\alpha, 1)$ is D-linear.)*

(*c*) *Prove, for a fixed nonzero $\beta \in F$, that $B(\alpha, \beta) = 0$ for all α in a D-basis of F if and only if T is the 0 map, that is, the map that takes each element of F to 0.*

trace dual basis

Let $\alpha_1, \ldots, \alpha_m$ be a basis for F over D. The second basis $\beta_1, \ldots, \beta_m$ is *trace dual basis* to the first if $Tr_D(\alpha_i\beta_j)$ $(= B(\alpha_i, \beta_j))$ is 1 when $i = j$ and 0 when $i \neq j$. In the next result we see that a trace dual basis always exists.

(A.3.16) PROPOSITION. *Let D be a subfield of the finite field F, and let $\alpha_1, \ldots, \alpha_m$ be a basis for F over D.*

We let A be the $m \times m$ matrix whose $\{i, j\}$-entry is $Tr_D(\alpha_i\alpha_j)$. For the $m \times s$ matrix B let the $\{j, k\}$-entry be $b_{j,k} \in F$. Finally let $\beta_k = \sum_{j=1}^{m} b_{j,k}\alpha_j$.

(1) *The $\{i, k\}$-entry of the matrix product AB is $Tr_D(\alpha_i\beta_k)$.*

(2) *The matrix A is invertible.*

(3) *For $B = A^{-1}$, the basis $\beta_1, \ldots, \beta_m$ is trace dual to $\alpha_1, \ldots, \alpha_m$.*

PROOF. Part (1) follows by an elementary matrix calculation.

If A is not invertible, then we can find a nonzero column vector B (with $s = 1$) such that $AB = 0$. This would correspond to a nonzero $\beta \in F$ with $Tr_D(\alpha_i\beta) = 0$, for all i. By Proposition A.3.14(3) this can not happen. This gives (2), and (3) is immediate from (1) and (2). □

(A.3.17) PROBLEM. *Reprove Proposition A.3.16 starting with an arbitrary nonzero D-linear map T.*

(A.3.18) PROBLEM. *Let the field $\mathbb{F}_8$ be written as polynomials of degree less than 3 over $\mathbb{F}_2$ in the primitive element α, a root of $x^3 + x + 1$, so that $\alpha^3 = \alpha + 1$. The trace $Tr = Tr_{\mathbb{F}_2}$ from $\mathbb{F}_8$ to $\mathbb{F}_2$ is then given by*

$$Tr(\beta) = \beta + \beta^2 + \beta^4$$

for all $\beta \in \mathbb{F}_8$. Set $e_1 = \alpha^3$, $e_2 = \alpha^5$, $e_3 = \alpha^6$, so that e_1, e_2, e_3 form a basis for $\mathbb{F}_8$ over $\mathbb{F}_2$.

(*a*) *Prove that the basis e_1, e_2, e_3 is trace self-dual: $Tr(e_ie_j)$ is 1 if $i = j$ and is 0 if $i \neq j$.*

(*b*) *For each $r \in \mathbb{F}_8$, let $\hat{r}$ be defined by $\hat{r} = (a, b, c)$, where $r = ae_1 + be_2 + ce_3$, for $a, b, c \in \mathbb{F}_2$. Prove that, for all $r, s \in \mathbb{F}_8$,*

$$\begin{aligned} Tr(rs) &= \hat{r} \cdot \hat{s} \text{ (dot product)} \\ &= af + bg + ch \end{aligned}$$

if $\hat{r} = (a, b, c)$ and $\hat{s} = (f, g, h)$.

(*c*) *Let $\mathbf{x}, \mathbf{y}$ be vectors in $\mathbb{F}_8^n$. Define the vectors $\hat{\mathbf{x}}, \hat{\mathbf{y}}$ by*

$$\hat{\mathbf{x}} = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n) \text{ for } \mathbf{x} = (x_1, x_2, \ldots, x_n)\ ,$$

$$\hat{\mathbf{y}} = (\hat{y}_1, \hat{y}_2, \ldots, \hat{y}_n) \text{ for } \mathbf{y} = (y_1, y_2, \ldots, y_n)\ .$$

Show that if $\mathbf{x} \cdot \mathbf{y} = 0$ in $\mathbb{F}_8$, then $\hat{\mathbf{x}} \cdot \hat{\mathbf{y}} = 0$ in $\mathbb{F}_2$.

Table. $\mathbb{F}_{32}$ where α is a root of the polynomial $x^5 + x^2 + 1$

Power	Polynomial of degree less than 5 in α	5−tuple
0	0	00000
1	1	00001
α^1	α^1	00010
α^2	α^2	00100
α^3	α^3	01000
α^4	α^4	10000
α^5	$\alpha^2 + 1$	00101
α^6	$\alpha^3 + \alpha^1$	01010
α^7	$\alpha^4 + \alpha^2$	10100
α^8	$\alpha^3 + \alpha^2 + 1$	01101
α^9	$\alpha^4 + \alpha^3 + \alpha^1$	11010
α^{10}	$\alpha^4 + 1$	10001
α^{11}	$\alpha^2 + \alpha^1 + 1$	00111
α^{12}	$\alpha^3 + \alpha^2 + \alpha^1$	01110
α^{13}	$\alpha^4 + \alpha^3 + \alpha^2$	11100
α^{14}	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	11101
α^{15}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha^1 + 1$	11111
α^{16}	$\alpha^4 + \alpha^3 + \alpha^1 + 1$	11011
α^{17}	$\alpha^4 + \alpha^1 + 1$	10011
α^{18}	$\alpha^1 + 1$	00011
α^{19}	$\alpha^2 + \alpha^1$	00110
α^{20}	$\alpha^3 + \alpha^2$	01100
α^{21}	$\alpha^4 + \alpha^3$	11000
α^{22}	$\alpha^4 + \alpha^2 + 1$	10101
α^{23}	$\alpha^3 + \alpha^2 + \alpha^1 + 1$	01111
α^{24}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha^1$	11110
α^{25}	$\alpha^4 + \alpha^3 + 1$	11001
α^{26}	$\alpha^4 + \alpha^2 + \alpha^1 + 1$	10111
α^{27}	$\alpha^3 + \alpha^1 + 1$	01011
α^{28}	$\alpha^4 + \alpha^2 + \alpha^1$	10110
α^{29}	$\alpha^3 + 1$	01001
α^{30}	$\alpha^4 + \alpha^1$	10010
α^{31}	1	00001

A.3.3 Minimal Polynomials

Let D be any field and F an extension field of D (that is, D is a subfield of F). If α is any element of F, then as in Section A.3.2 we consider the collection of polynomials that have α as a root:

$$I = \{\, p(x) \in D[x] \,|\, p(\alpha) = 0 \}\,.$$

It is possible for I to contain only the zero polynomial, an example being given by $D = \mathbb{Q}$, $F = \mathbb{R}$, $\alpha = \pi$. We are interested here in the case where F is finite, and there the argument of Lemma A.1.3 and Section A.3.2 shows that I must contain nonzero polynomials.

minimal polynomial

Assuming that I contains nonzero polynomials, we denote by $m_{\alpha,D}(x)$ the *minimal polynomial* of α over D, that is, the greatest common divisor of I. When D is the prime subfield (here, $\mathbb{F}_p$ for some prime p) we have abbreviated this to $m_\alpha(x)$. A minimal polynomial must always be irreducible.

For a finite collection S of nonzero polynomials, the least common multiple, $\mathrm{lcm}(S)$, was introduced in Problem A.2.19. When all the members of S are monic irreducible, the lcm is easy to calculate — it is just the product of all distinct members of S (see Problem A.2.25).

(A.3.19) LEMMA. *Let $\alpha, \beta, \ldots, \omega$ be members of the extension field F of the field D. Then the set*

$$J = \{\, p(x) \in D[x] \mid p(\alpha) = p(\beta) = \cdots = p(\omega) = 0 \,\}$$

consists precisely of all multiples of

$$g(x) = \mathrm{lcm}(m_{\alpha,D}(x), m_{\beta,D}(x), \ldots, m_{\omega,D}(x)).$$

PROOF. By the definition of a minimal polynomial, for each element γ of $\alpha, \beta, \ldots, \omega$, the set J consists of multiples of $m_{\gamma,D}(x)$. Therefore by the definition of least common multiples (see Problem A.2.19) all members of J are multiples of $g(x)$. On the other hand, any multiple of $g(x)$ has each of $\alpha, \beta, \ldots, \omega$ as a root and so is in J. □

The remark before Lemma A.3.19 shows that, in the computation of $g(x)$ the only difficult part is the calculation of the minimal polynomials over D of members of F. In Theorem A.3.20 and Problem A.3.21 we describe an easy way to do this for finite D. At the end of the section an example of such a calculation using Theorem A.3.20 is presented.

(A.3.20) THEOREM. *Let F be a finite field of characteristic p, and let α be a member of F. Then for*

$$A = \{\alpha^{p^i} \mid i = 0, 1, 2, \ldots \}$$

we have

$$m_\alpha(x) = \prod_{a \in A} (x - a)\ .$$

PROOF. Let $m(x) = m_\alpha(x) = \sum_i m_i x^i$ with each m_i in $\mathbb{F}_p$. As $m(\alpha) = 0$, also $(m(\alpha))^p = 0$. That is,

$$\begin{aligned} 0 &= (\sum m_i\alpha^i)^p = \sum (m_i\alpha^i)^p && \text{by } A.3.13(1) \\ &= \sum m_i^p \alpha^{ip} = \sum m_i(\alpha^p)^i && \text{by } A.3.13(2) \\ &= m(\alpha^p). \end{aligned}$$

Thus from $m(\alpha) = 0$ we may conclude that $m(\alpha^p) = 0$ and then that $m((\alpha^p)^p) = m(\alpha^{p^2}) = 0$; indeed $m(a) = 0$, for all $a \in A$. By Lemma A.2.8 $x - a$ divides $m(x)$ for each $a \in A$, and so by repeated application of Lemma A.2.9 we know that $\prod_{a\in A}(x - a)$ is in any event a divisor of $m(x)$ in $F[x]$. To complete a proof that $m(x) = \prod_{a\in A}(x - a)$ it is enough to show that $\prod_{a\in A}(x - a)$ in fact has all its coefficients in $\mathbb{F}_p$, for then $m(x)$ and $\prod_{a\in A}(x - a)$ will be two monic polynomials of $\mathbb{F}_p[x]$ that divide each other and so must be equal.

Let $A = \{a_1, a_2, \ldots, a_d\}$. Then in $\prod_{a\in A}(x - a)$ the coefficient of x^k is

$$\sum_{\{i_1,i_2,\ldots,i_{d-k}\}} a_{i_1} a_{i_2} \cdots a_{i_{d-k}} ,$$

where the summation runs over all $d-k$ subsets of $\{1, 2, \ldots, d\}$. By design, for each a_i in A, a_i^p is also a member of A. Therefore for each term $a_{i_1} a_{i_2} \cdots a_{i_{d-k}}$ of the above summation, the power $(a_{i_1} a_{i_2} \cdots a_{i_{d-k}})^p = a_{i_1}^p a_{i_2}^p \cdots a_{i_{d-k}}^p$ is also one of the terms of the summation. Hence using Lemma A.3.13(1) again we have

$$(\sum a_{i_1} a_{i_2} \cdots a_{i_{d-k}})^p = \sum a_{i_1}^p a_{i_2}^p \cdots a_{i_{d-k}}^p = \sum a_{i_1} a_{i_2} \cdots a_{i_{d-k}} .$$

That is, the coefficient of x^k in $\prod_{a\in A}(x - a)$ is equal to its own p^{th} power. By Lemma A.3.13(2) this coefficient is a member of the prime subfield $\mathbb{F}_p$, as required. □

Essentially the same proof with q in place of p gives the more general result (which we leave as an exercise) with $D = \mathbb{F}_q$ in place of $\mathbb{F}_p$:

(A.3.21) PROBLEM. *Let F be a finite field of characteristic p, D a subfield of F containing exactly q elements, and α be a member of F. Then for*

$$A = \{\alpha^{q^i} \mid i = 0, 1, 2, \ldots\}$$

we have

$$m_{\alpha,D}(x) = \prod_{a\in A}(x - a).$$

REMARK. At first sight, the final equations in the statement of Theorem A.3.20 and Problem A.3.21 seem to go against our claim that minimal polynomials must be irreducible. Here $m_{\alpha,D}(x)$ is a minimal polynomial, but $\prod_{a\in A}(x-a)$

appears to be a nontrivial factorization. The point is that $m_{\alpha,D}(x)$ is an irreducible polynomial in the polynomial ring $D[x]$; it has no factorizations into polynomials of $D[x]$ of smaller degree. The factorization $\prod_{a\in A}(x-a)$ involves factors $x-a$ that are polynomials of $F[x]$ but not of $D[x]$ (as long as $a \notin D$). For example, as a polynomial of $\mathbb{R}[x]$, x^2+1 is irreducible; but as a polynomial of $\mathbb{C}[x]$ it factors as $x^2+1=(x+i)(x-i)$. Indeed $m_{i,\mathbb{R}}(x)=x^2+1$.

Below we give an example which details the calculation using Theorem A.3.20 of the minimal polynomial of α^5 over $\mathbb{F}_2$, $m_{\alpha^5,\mathbb{F}_2}(x)$, where α is a root of the primitive polynomial $x^5+x^2+1 \in \mathbb{F}_2[x]$. (See the table at the end of Section A.3.2.)

(A.3.22) PROBLEM. *Let β be a root of the polynomial $x^4+x^3+1 \in \mathbb{F}_2[x]$. Calculate the minimal polynomial of β^3.*

Calculation of a minimal polynomial

Let α be a primitive element in $\mathbb{F}_{32}$ with minimal polynomial $m_\alpha(x)=m_{\alpha,\mathbb{F}_2}(x)=x^5+x^2+1$. We wish to calculate the minimal polynomial of α^5.

$$
\begin{aligned}
& m_{\alpha^5,\mathbb{F}_2}(x) \\
&\quad = \quad (x-\alpha^5)(x-\alpha^{10})(x-\alpha^{20})(x-\alpha^9)(x-\alpha^{18}) \\
&\quad = \quad x^5-(\alpha^5+\alpha^{10}+\alpha^{20}+\alpha^9+\alpha^{18})x^4 \\
&\qquad\quad +(\alpha^{15}+\alpha^{25}+\alpha^{14}+\alpha^{23}+\alpha^{30}+\alpha^{19}+\alpha^{28}+\alpha^{29}+\alpha^{38}+\alpha^{27})x^3 \\
&\qquad\quad -(\alpha^{47}+\alpha^{37}+\alpha^{48}+\alpha^{39}+\alpha^{32}+\alpha^{43}+\alpha^{34}+\alpha^{33}+\alpha^{24}+\alpha^{35})x^2 \\
&\qquad\quad +(\alpha^{57}+\alpha^{52}+\alpha^{42}+\alpha^{53}+\alpha^{44})x-\alpha^{62} \\
&\quad = \quad x^5+1x^4+0x^3+1x^2+1x+1 \\
&\quad = \quad x^5+x^4+x^2+x+1\ .
\end{aligned}
$$

Where, for instance, the coefficient of x is given by:

$$
\begin{aligned}
& \alpha^{57}+\alpha^{52}+\alpha^{42}+\alpha^{53}+\alpha^{44} \\
&\quad = \quad \alpha^{26}+\alpha^{21}+\alpha^{11}+\alpha^{22}+\alpha^{13} \\
&\quad = \quad (\alpha^4+\alpha^2+\alpha+1)+(\alpha^4+\alpha^3)+(\alpha^2+\alpha+1) \\
&\qquad\quad +(\alpha^4+\alpha^2+1)+(\alpha^4+\alpha^3+\alpha^2) \\
&\quad = \quad 1\ .
\end{aligned}
$$