

4 Polynomials

The set of functions $f : \mathbb{R} \rightarrow \mathbb{R}$ is a ring in a very straightforward manner: the sum of two functions f and g is $(f + g)(x) = f(x) + g(x)$ and the product $(fg)(x) = f(x)g(x)$. The subset $\{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in \mathbb{R}\}$ of polynomials is a subring of this ring. It is easy to show that the above addition and multiplication lead to the addition

$$\begin{aligned} & (a_0 + a_1x + a_2x^2 + \cdots) + (b_0 + b_1x + b_2x^2 + \cdots) \\ &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots \end{aligned}$$

and the multiplication

$$\begin{aligned} & (a_0 + a_1x + a_2x^2 + \cdots)(b_0 + b_1x + b_2x^2 + \cdots) \\ &= (a_0b_0) + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots \end{aligned}$$

of polynomials. The marvelous thing is that this addition and multiplication is algebraic in nature and makes sense even if we replace the coefficients with elements in an arbitrary (commutative) ring.

In many ways polynomials form the heart of algebra. In this chapter we begin by introducing polynomials formally. Straight after the formal introduction we will give a surprising application of the addition and multiplication of polynomials. We will show how one can easily compute the remainder of a binomial coefficient divided by a prime number p by computing with polynomials with coefficients in \mathbb{F}_p .

The division algorithm for polynomials is crucial. We give it here in a slightly modified form (see Proposition 4.2.4) to make clear why the general division algorithm in several variables (see Proposition 5.3.1) is really a natural extension. After the important Theorem 4.3.5 we move on to the classical subjects of cyclotomic polynomials and finite fields. You will miss a golden opportunity

if you do not immerse yourself in these topics. It is your ticket to a real understanding of this chapter.

As promised in Section 1.11 we give a proof of Gauss' famous theorem on quadratic reciprocity. The proof uses Freshman's Dream (Theorem 3.3.9) and computations with Gauss sums in a suitable quotient ring of a polynomial ring. You will have the necessary background to learn a proof of a really deep theorem in number theory just by knowing basic properties of polynomials.

Freshman's Dream is also a key player in the odd fact that there are fast algorithms for factoring polynomials with coefficients in \mathbb{F}_p into irreducible polynomials. We go through this by describing the basic steps of Berlekamp's algorithm. Notice the stark contrast with the integers \mathbb{Z} , where no one (so far) has come up with a fast algorithm for factoring. Most of the mathematics in this chapter can be traced back to the seminal work [11] of Gauss.

4.1 Polynomial rings

We will introduce the polynomial ring formally. It will be important for us to view polynomials as purely algebraic objects and not as a subring of a ring of functions (see Exercise 4.1).

Let R be a ring (commutative as usual) and $R[\mathbb{N}]$ the set of functions $f: \mathbb{N} \rightarrow R$ such that $f(n) = 0$ for $n \gg 0$ (here one should think of the polynomial $f(0) + f(1)X + f(2)X^2 + \dots$). Given $f, g \in R[\mathbb{N}]$ we define their sum as $(f + g)(n) = f(n) + g(n)$. Inspired by the way "real-world polynomials" multiply, we define

$$(fg)(n) = \sum_{i+j=n} f(i)g(j),$$

where $i, j \in \mathbb{N}$. For example $(fg)(3) = f(3)g(0) + f(2)g(1) + f(1)g(2) + f(0)g(3)$. We let $X^i \in R[\mathbb{N}]$ denote the function

$$X^i(n) = \begin{cases} 1 & \text{if } n = i, \\ 0 & \text{if } n \neq i. \end{cases}$$

Notice that $X^i X^j = X^{i+j}$, where $i, j \in \mathbb{N}$. We view an element $a \in R$ as the function

$$a(n) = \begin{cases} a & \text{if } n = 0, \\ 0 & \text{if } n > 0 \end{cases}$$

in $R[\mathbb{N}]$. So, an element $f \in R[\mathbb{N}]$ can be written as

$$f = a_0 + a_1X + \cdots + a_nX^n,$$

where $a_i = f(i)$ and $f(i) = 0$ if $i > n$. Notice that $1 = X^0$ is (the) neutral element for the multiplication. The neutral element for $+$ is $0 \in R$. Clearly $fg = gf$ and $f(g+h) = fg + fh$ for $f, g, h \in R[\mathbb{N}]$. With these tools it becomes easy (see Exercise 4.2) to verify the associative rule for the multiplication, i.e. $f(gh) = (fg)h$ for every $f, g, h \in R[\mathbb{N}]$, since we may assume that $h = cX^m$, where $c \in R$ and $m \in \mathbb{N}$.

Definition 4.1.1 We define the polynomial ring $R[X]$ in one variable over the ring R as $R[\mathbb{N}]$. Here X denotes the function $X^1 \in R[\mathbb{N}]$. A *term* is a polynomial of the form aX^m , where $a \in R \setminus \{0\}$. A polynomial $f \in R[X]$ can be written

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n,$$

where $a_0, \dots, a_n \in R$ are called the *coefficients* of f . If $a_n \neq 0$ we put $\deg(f) = n$ and call a_n the *leading coefficient* of f . In this case $\deg(f)$ is called the *degree* of f and $a_{\deg(f)}X^{\deg(f)}$ its *leading term*. A non-zero polynomial is called *monic* if its leading coefficient is 1.

Remark 4.1.2 The degree of a polynomial is a function $\deg : R[X] \setminus \{0\} \rightarrow \mathbb{N}$. It is an extremely useful invariant of a polynomial. The degree of the zero polynomial is not defined.

Now you have seen the formal definition of $R[X]$. When computing with polynomials it pays to treat them as the usual polynomial expressions that we know.

Remark 4.1.3 Two polynomials $f = a_mX^m + \cdots + a_1X + a_0$ and $g = b_nX^n + \cdots + b_1X + b_0$ in $R[X]$ are the same if and only if $a_0 = b_0$, $a_1 = b_1$, \dots . This is clear when we view the polynomials as functions $\mathbb{N} \rightarrow R$. Two functions $\mathbb{N} \rightarrow R$ are the same if and only if they assume the same value for every $n \in \mathbb{N}$.

We have proved that $R[X]$ really is a ring when R is a ring. This means that all the concepts from Chapter 3 apply. For example, it makes sense to ask whether $R[X]$ is a domain, a Euclidean domain or a unique factorization domain. It also makes sense to ask whether a polynomial in $R[X]$ is a unit or a zero divisor.

4.1.1 Binomial coefficients modulo a prime number

Let us pause for a while after having introduced polynomials formally. We will give an example showing that computations with polynomials can be helpful in reasoning about numbers and congruences. We wish to prove that

$$7 \mid \binom{55}{22}.$$

Judging from the size of the binomial coefficient on the right, this may not be an easy task, unless of course we dig a bit deeper into the structure of the polynomial ring. If n is a natural number > 1 then every $x \in \mathbb{N}$ has a unique n -adic expansion (see Exercise 1.5)

$$x = a_0 + a_1n + a_2n^2 + \cdots + a_rn^r,$$

where $r \in \mathbb{N}$, $a_i \in \mathbb{N}$ and $0 \leq a_i < n$ for $i = 0, \dots, r$. Recall Freshman's Dream (Theorem 3.3.9) from Chapter 3: if R is a commutative ring of prime characteristic p then

$$(a + b)^{p^r} = a^{p^r} + b^{p^r}$$

for $a, b \in R$ and $r \in \mathbb{N}$. This shows that if m is a natural number with the p -adic expansion

$$m = a_0 + a_1p + \cdots + a_rp^r$$

then

$$(1 + X)^m = (1 + X)^{a_0}(1 + X^p)^{a_1} \cdots (1 + X^{p^r})^{a_r}$$

in the polynomial ring $\mathbb{F}_p[X]$ (which is a commutative ring of characteristic p). Now let

$$n = b_0 + b_1p + \cdots + b_sp^s$$

be another natural number and its p -adic expansion. Compare the coefficients of the left hand side of the previous equation,

$$(1 + X)^m = \sum_{n=0}^m \binom{m}{n} X^n,$$

with the coefficients of its right hand side,

$$\begin{aligned} (1+X)^{a_0}(1+X^p)^{a_1}\cdots(1+X^{p^r})^{a_r} \\ = \left(\sum_{b_0=0}^{a_0}\binom{a_0}{b_0}X^{b_0}\right)\left(\sum_{b_1=0}^{a_1}\binom{a_1}{b_1}X^{pb_1}\right)\cdots\left(\sum_{b_r=0}^{a_r}\binom{a_r}{b_r}X^{p^rb_r}\right). \end{aligned}$$

A term in the product above is given uniquely as the product of a term from the first factor, a term from the second factor and so on. This follows from the uniqueness of the p -adic expansion. Two polynomials are the same if and only if their coefficients are the same (Remark 4.1.3). This leads to the surprising identity

$$\binom{m}{n} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots \pmod{p},$$

where

$$\binom{r}{s} = \frac{r(r-1)\cdots(r-s+1)}{s(s-1)\cdots 2\cdot 1}.$$

Thus $p \mid \binom{m}{n}$ if and only if $a_i < b_i$ for some i . Expanding 7-adically 55 and 22 we get

$$\begin{aligned} 55 &= 6 + 1 \cdot 7^2, \\ 22 &= 1 + 3 \cdot 7^1. \end{aligned}$$

Thus

$$\binom{55}{22} \equiv \binom{6}{1}\binom{0}{3}\binom{1}{0} = 0 \pmod{7},$$

so 7 divides $\binom{55}{22}$.

4.2 Division of polynomials

We move on to describe the important division algorithm for polynomials. First, we give a few properties of the degree function.

Example 4.2.1 If $R = \mathbb{Z}/4\mathbb{Z}$ and $f = g = 2X + 1$ then $fg = 1$, so that $\deg(fg) = 0$ but $\deg(f) = \deg(g) = 1$. Remember that when we write 2 in the ring $\mathbb{Z}/4\mathbb{Z}$ it really means $[2] = 2 + 4\mathbb{Z}$ (see Remark 3.3.4).

The above example shows that the formula $\deg(fg) = \deg(f) + \deg(g)$ for $f, g \in R[X] \setminus \{0\}$ breaks down in general. It can be repaired by imposing some mild restrictions.

Proposition 4.2.2 *Let $f, g \in R[X] \setminus \{0\}$. If the leading coefficient of f or g is not a zero divisor then*

$$\deg(fg) = \deg(f) + \deg(g).$$

Proof. We may write $f = a_m X^m + \cdots$ and $g = b_n X^n + \cdots$, where a_m, b_n are the leading coefficients (thus $m = \deg(f)$ and $n = \deg(g)$). Then

$$fg = a_m b_n X^{m+n} + \cdots.$$

Since one of a_m and b_n is not a zero divisor, we must have $a_m b_n \neq 0$. Therefore $\deg(fg) = m + n = \deg(f) + \deg(g)$. \square

We have seen in Example 4.2.1 that there can be units in $R[X]$ of degree > 0 . This is rather pathological. In most cases units have degree zero. A monic polynomial of degree > 0 can never be a unit (why?).

Proposition 4.2.3 *Let R be a domain. Then $R[X]^* = R^*$.*

Proof. Assume that $f \in R[X]^*$. Then there exists $g \in R[X]$ such that $fg = 1$. Thus $\deg(fg) = \deg(f) + \deg(g) = \deg(1) = 0$ by Proposition 4.2.2. This shows that $\deg(f) = \deg(g) = 0$ and $f, g \in R^* \subseteq R$. Thus $R[X]^* \subseteq R^*$. Clearly $R^* \subseteq R[X]^*$. \square

Now we come to the division algorithm in $R[X]$. It can be viewed as an analogue of division with remainder for the integers (Theorem 1.2.1). We are rephrasing it a little so that it generalizes naturally to the division algorithm for polynomials in several variables later. Notice that $:=$ means assignment to a variable (we use $:=$ to distinguish it from $=$, which has a well defined mathematical meaning).

Proposition 4.2.4 *Let d be a non-zero polynomial in $R[X]$. Assume that the leading coefficient of d is not a zero divisor in R . Given $f \in R[X]$, there exist polynomials $q, r \in R[X]$ such that*

$$f = qd + r$$

and either $r = 0$ or none of the terms in r is divisible by the leading term of d .

Proof. Let aX^m denote the leading term of d , where a is not a zero divisor in R . To begin with we have the identity $f = qd + (r + s)$, where $q = 0$, $r = 0$ and $s = f$. If $s = 0$ we are done. If not, let bX^n denote the leading term of s . If aX^m divides bX^n then $n \geq m$, $b = ca$, for a unique $c \in R$, and $bX^n = cX^{n-m}aX^m$. We put

$$\begin{aligned} q &:= q + cX^{n-m}, \\ s &:= s - cX^{n-m}d. \end{aligned}$$

After these assignments we see that the identity $f = qd + (r + s)$ still holds. If aX^m does not divide bX^n we put

$$\begin{aligned} r &:= r + bX^n, \\ s &:= s - bX^n. \end{aligned}$$

Again after these assignments the identity $f = qd + (r + s)$ holds. After both assignments r will only contain terms not divisible by the leading term of d . Now proceed with the same steps using the new s . If $s = 0$ the procedure will stop. If not we know that the degree of s has strictly decreased since it does so in both steps. After finitely many steps (the degree of f is finite) we will reach the case $s = 0$. \square

If the leading coefficient of d in Proposition 4.2.4 is invertible then there is a more appealing way of formulating the division of polynomials. This is the content of the following corollary.

Corollary 4.2.5 *Let d be a non-zero polynomial in $R[X]$. Assume that the leading coefficient of d is invertible in R . Given $f \in R[X]$, there exist unique polynomials $q, r \in R[X]$ such that*

$$f = qd + r$$

and either $r = 0$ or $\deg(r) < \deg(d)$.

Proof. An invertible element divides every other element in R . Therefore the leading term of d divides a term of degree n if and only if $\deg(d) \leq n$. In this situation Proposition 4.2.4 may be reformulated as $f = qd + r$, where $r = 0$ or $\deg(r) < \deg(d)$ if $r \neq 0$.

Assume that $f = q_1d + r_1 = q_2d + r_2$, where $q_1, r_1, q_2, r_2 \in R[X]$ and r_1, r_2 satisfy the conditions in the corollary. Then $(q_1 - q_2)d = r_2 - r_1$. If $r_2 - r_1 \neq 0$ then $\deg(q_1 - q_2) + \deg(d) = \deg(r_2 - r_1)$. Since $\deg(r_2 - r_1) \leq \max(\deg(r_1), \deg(r_2))$ (see Exercise 4.3), we get $\deg(d) \leq \deg(r_1)$ or $\deg(d) \leq$

$\deg(r_2)$. This is a contradiction. It implies that $r_1 = r_2$ and thereby that $q_1 = q_2$, proving the uniqueness of q and r . \square

The division algorithm for polynomials is illustrated in the following example.

Example 4.2.6 If $f = X^4 + X - 1$ and $d = X - 1$ are polynomials in $\mathbb{Z}[X]$, we may write the algorithm in the proof of Proposition 4.2.4 schematically as

$$\begin{array}{rcl}
 X^4 + X - 1 & : & X - 1 = X^3 + X^2 + X + 2 \\
 \underline{X^4 - X^3} & & \\
 X^3 + X - 1 & & \\
 \underline{X^3 - X^2} & & \\
 X^2 + X - 1 & & \\
 \underline{X^2 - X} & & \\
 2X - 1 & & \\
 \underline{2X - 2} & & \\
 1 & &
 \end{array}$$

This shows that $X^4 + X - 1 = (X^3 + X^2 + X + 2)(X - 1) + 1$.

Definition 4.2.7 The polynomial r in Corollary 4.2.5 is called the *remainder* of f divided by d .

4.3 Roots of polynomials

The map $j : R \rightarrow R[X]$ given by

$$j(r) = r + 0X + 0X^2 + \cdots$$

is an injective ring homomorphism. We identify the image $j(R)$ with R and view R as a subring of $R[X]$ in this way.

Proposition 4.3.1 Let $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ and $\alpha \in R$. The map $\varphi_\alpha : R[X] \rightarrow R$ given by

$$\varphi_\alpha(f) = f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$$

is a ring homomorphism.

Proof. This follows from the rules for adding and multiplying in $R[X]$. \square

This leads us to the crucial concept of a root of a polynomial. Let $f \in R[X]$ be a polynomial. The element $\alpha \in R$ is called a *root* of f if $f(\alpha) = \varphi_\alpha(f) = 0$. We let $V(f) = \{\alpha \in R \mid f(\alpha) = 0\}$ denote the set of roots of $f \in R[X]$. The following corollary is a stepping stone toward introducing the concept of the multiplicity of roots in polynomials.

Corollary 4.3.2 *Let $f \in R[X]$. Then $\alpha \in R$ is a root of f if and only if $X - \alpha$ divides f .*

Proof. Assume α is a root of f . By Corollary 4.2.5 we may write

$$f = q(X - \alpha) + r,$$

where r is a constant ($r \in R$). Substituting α for X on both sides (see Proposition 4.3.1) we get $0 = f(\alpha) = r$, which proves $r = 0$. If $X - \alpha$ divides f then $r = 0$ and α is a root of f . \square

If a monic polynomial q divides a non-zero polynomial f then $f = qr$ for a unique r (q is not a zero divisor in $R[X]$) and $\deg(f) = \deg(q) + \deg(r)$ by Proposition 4.2.2. Thus $\deg(q) \leq \deg(f)$. The *multiplicity* of α as a root in a non-zero polynomial f is the largest power $n \in \mathbb{N}$ such that

$$(X - \alpha)^n \mid f.$$

The multiplicity of α in f is denoted $v_\alpha(f)$. Notice that $v_\alpha(f) \leq \deg(f)$ and $f = (X - \alpha)^{v_\alpha(f)}h$, where $h(\alpha) \neq 0$. A *multiple root* in f is a root $\alpha \in R$ with $v_\alpha(f) > 1$.

The following example shows that one needs to exercise some caution with regard to roots. There may be too many of them in pathological cases (see also Exercise 4.6).

Example 4.3.3 Let $R = \mathbb{Z}/6\mathbb{Z}$ and $f = X^2 + 3X + 2 \in R[X]$. Then f can have at most six roots (after all there are only six elements in R). Let us tabulate $f(\alpha)$ for $\alpha \in R$:

α	0	1	2	3	4	5
$f(\alpha)$	2	0	0	2	0	0

We see that $V(f) = \{1, 2, 4, 5\}$. In this case f has four roots but the degree of f is 2. It is not true that $f = (X - 1)(X - 2)(X - 4)(X - 5)$.

The usual type of polynomial $f \in \mathbb{R}[X] \setminus \{0\}$ cannot have more than $\deg(f)$ roots. This is wrong in the general case (Example 4.3.3). However, if R is a domain we can get the “right” bound on the number of roots for a non-zero polynomial in $R[X]$. The following simple lemma captures the essence.

Lemma 4.3.4 *Let R be a domain and $f, g \in R[X]$. Then $V(fg) = V(f) \cup V(g)$.*

Proof. The inclusion $V(fg) \supseteq V(f) \cup V(g)$ is true without any assumptions on R . We will prove that $V(fg) \subseteq V(f) \cup V(g)$. If $\alpha \in V(fg)$ then $(fg)(\alpha) = f(\alpha)g(\alpha) = 0$. Since R is a domain we get $f(\alpha) = 0$ or $g(\alpha) = 0$. Thus $\alpha \in V(f)$ or $\alpha \in V(g)$ and $\alpha \in V(f) \cup V(g)$. \square

Theorem 4.3.5 *Let R be a domain and $f \in R[X] \setminus \{0\}$. If $V(f) = \{\alpha_1, \dots, \alpha_r\}$ then*

$$f = q(X - \alpha_1)^{v_{\alpha_1}(f)} \cdots (X - \alpha_r)^{v_{\alpha_r}(f)},$$

where $q \in R[X]$ and $V(q) = \emptyset$. The number of roots of f , counted with multiplicity, is bounded by the degree of f .

Proof. We prove this using induction on $\deg(f)$. We will show the induction step and leave the cases $\deg(f) = 0$ and $V(f) = \emptyset$ to the reader. If $\alpha \in V(f)$ then $f = (X - \alpha)^{v_{\alpha}(f)}g$, where $\deg(g) < \deg(f)$ and $g(\alpha) \neq 0$. Thus $V(f) = \{\alpha\} \cup V(g)$ by Lemma 4.3.4 and $\alpha \notin V(g)$. By induction

$$g = q(X - \beta_1)^{v_{\beta_1}(g)} \cdots (X - \beta_s)^{v_{\beta_s}(g)},$$

where $V(g) = \{\beta_1, \dots, \beta_s\}$ and $V(q) = \emptyset$. This gives the desired formula

$$f = q(X - \alpha)^{v_{\alpha}(f)}(X - \beta_1)^{v_{\beta_1}(f)} \cdots (X - \beta_s)^{v_{\beta_s}(f)},$$

where $V(f) = \{\alpha\} \cup V(g) = \{\alpha, \beta_1, \dots, \beta_s\}$ and $V(q) = \emptyset$. Now it follows by Proposition 4.2.2 that

$$v_{\alpha}(f) + v_{\beta_1}(f) + \cdots + v_{\beta_s}(f) \leq \deg(f),$$

proving that the number of roots of f counted with multiplicity is bounded by the degree of f . \square

As a first example of the usefulness of Theorem 4.3.5 we give a (natural) proof of Wilson’s theorem (see Exercise 1.29(ii)), which says that $(p - 1)! \equiv -1 \pmod{p}$ if p is a prime number.

Example 4.3.6 Consider the polynomial $X^p - X \in \mathbb{F}_p[X]$. Then

$$V(X^p - X) = \{0, 1, \dots, p-1\}$$

by Fermat's little theorem, Corollary 1.9.2. It follows by Theorem 4.3.5 that

$$X^p - X = qX(X-1)(X-2)\cdots(X-(p-1)),$$

where q is a polynomial of degree zero (which has to be 1 by comparing the leading coefficients on both sides). Comparing coefficients of degree one on the left and right hand sides, we get $1 \cdot 2 \cdots (p-1) = (p-1)! = -1$ in \mathbb{F}_p . This shows that $(p-1)! \equiv -1 \pmod{p}$.

We now describe a useful algebraic gadget inspired by differentiation in analysis. We cannot employ the usual definition of the derivative from analysis, so we have to be a little more formal.

4.3.1 Differentiation of polynomials

Let R be a ring and $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$. Then

$$D(f) = a_n n X^{n-1} + a_{n-1}(n-1)X^{n-2} + \cdots + a_1$$

is called the *derivative* of f . When a polynomial is viewed formally as a map $f: \mathbb{N} \rightarrow R$ (see Section 4.1), this can be rephrased as $D(f)(n-1) = nf(n)$ for $n \geq 1$. The following lemma shows that the derivative behaves just as in ordinary differentiation.

Lemma 4.3.7 Let $f, g \in R[X]$ and $\lambda \in R$. Then

- (i) $D(f+g) = D(f) + D(g)$,
- (ii) $D(\lambda f) = \lambda D(f)$,
- (iii) $D(fg) = fD(g) + D(f)g$.

Proof. We will prove (iii) and leave (i) and (ii) to the reader. Viewing polynomials formally as maps $\mathbb{N} \rightarrow R$, (iii) follows from the identity

$$\begin{aligned} (fD(g) + D(f)g)(n-1) &= \sum_{i+j=n-1} f(i)D(g)(j) + \sum_{i+j=n-1} D(f)(i)g(j) \\ &= \sum_{i+j=n-1} f(i)(j+1)g(j+1) \\ &\quad + \sum_{i+j=n-1} (i+1)f(i+1)g(j) \end{aligned}$$

$$\begin{aligned}
&= \sum_{i+j=n} f(i)jg(j) + \sum_{i+j=n} if(i)g(j) \\
&= n \sum_{i+j=n} f(i)g(j) \\
&= n(fg)(n) = D(fg)(n-1),
\end{aligned}$$

where $n \geq 1$. □

The most useful property of the derivative is the Leibniz rule (Lemma 4.3.7(iii)). We will use the derivative to reason about roots of polynomials, as shown in the lemma below.

Lemma 4.3.8 *Suppose that $f, g \in R[X]$.*

- (i) *If $f^2 \mid g$ then $f \mid D(g)$.*
- (ii) *An element $\alpha \in R$ is a multiple root of f if and only if α is a root of f and $D(f)$.*

Proof. Assume that $g = qf^2$. Then $D(g) = D(q)f^2 + 2qD(f)f = (D(q)f + 2qD(f))f$ by Lemma 4.3.7(iii). This proves (i). If α is a multiple root of f then $(X - \alpha)^2$ divides f . Therefore $X - \alpha$ divides $D(f)$ by (i) and α is a root of $D(f)$. Now assume that α is a root of f and $D(f)$. Then $f = (X - \alpha)^m h$, where $m = v_\alpha(f) \geq 1$ and $h(\alpha) \neq 0$. If $m = 1$ we get $D(f) = h + (X - \alpha)D(h)$. This leads to $D(f)(\alpha) = h(\alpha) \neq 0$, contradicting that α is a root of $D(f)$. Therefore $m \geq 2$ and α is a multiple root of f . This proves (ii). □

Remark 4.3.9 If the polynomial ring $R[X]$ is of prime characteristic $p > 0$ one encounters many non-constant polynomials with zero derivatives. Take $X^p \in \mathbb{F}_p[X]$ as an example. Here

$$D(X^p) = pX^{p-1} = 0.$$

In fact $D(X^n) = 0$ if and only if p divides n when $X^n \in \mathbb{F}_p[X]$. This looks strange but can be very useful.

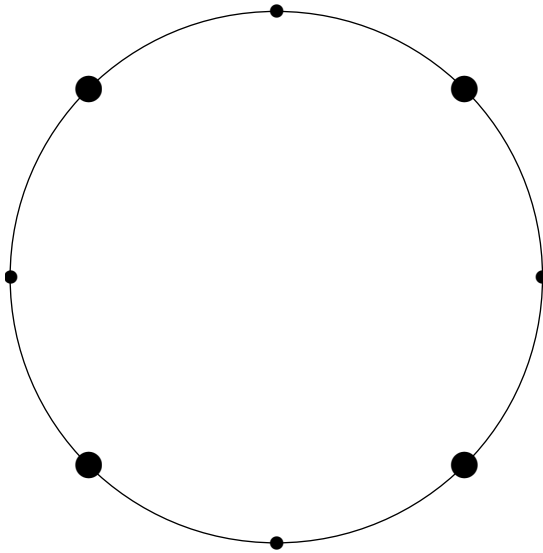
4.4 Cyclotomic polynomials

A complex number ξ is called an n th root of unity for a positive integer n if $\xi^n = 1$. Writing ξ in polar coordinates as $re^{i\theta} = r(\cos \theta + i \sin \theta)$, it follows that $r = 1$ and $\theta = k2\pi/n$ for $k = 0, \dots, n-1$ if ξ is an n th root of unity. Of course, n may not be the smallest positive integer with the property $\xi^n = 1$

(if $\xi = i$ then, $\xi^8 = 1$ but already $\xi^4 = 1$). A complex number ζ is called a primitive n th root of unity if $\zeta^n = 1$ and

$$\zeta, \zeta^2, \dots, \zeta^{n-1} \neq 1,$$

where $n \geq 1$. The eighth roots of unity are plotted below as dots on the unit circle in the complex plane. The bigger dots represent the primitive eighth roots of unity.



Lemma 4.4.1 *A complex number ζ is a primitive n th root of unity if and only if*

$$\zeta = e^{k2\pi i/n},$$

where $1 \leq k \leq n$ and $\gcd(k, n) = 1$. If ζ is a primitive n th root of unity and $\zeta^m = 1$ then $n \mid m$.

Proof. The n th roots of unity are $e^{k2\pi i/n}$, where $k = 1, \dots, n$. Let $\xi = e^{k2\pi i/n}$ be an n th root of unity. If $\xi^m = 1$ then $mk2\pi/n$ is an integer multiple of 2π and therefore $n \mid mk$. Assume that $\gcd(k, n) = 1$. Then $n \mid km$ implies that $n \mid m$ by Corollary 1.5.10. Thus $\xi, \xi^2, \dots, \xi^{n-1} \neq 1$. Therefore ξ is a primitive n th root of unity. However, if $\gcd(k, n) = g > 1$ then $\xi^{n/g} = 1$ and ξ cannot be a primitive n th root of unity. If ζ is a primitive n th root of unity and $\zeta^m = 1$ then we may write $m = qn + r$, where $0 \leq r < n$. This shows that $\zeta^m = \zeta^r$ and therefore that $r = 0$. \square

The set of all n th roots of unity is a subgroup of \mathbb{C}^* . This subgroup is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$. Using this and Lemma 4.4.1 you get a different angle (see Exercise 4.14) on Proposition 2.7.4 that is more in the spirit of Gauss.

Now we construct a polynomial in $\mathbb{C}[X]$ whose roots are all the primitive n th roots of unity. Although the reason will not yet be clear, this will lead to some amazing algebra later.

Definition 4.4.2 Let $n \in \mathbb{N}$ with $n \geq 1$. The n th cyclotomic polynomial is defined as the polynomial

$$\Phi_n(X) = \prod_{1 \leq k \leq n, \gcd(k,n)=1} (X - e^{2\pi i k/n})$$

in $\mathbb{C}[X]$.

Notice that $\deg \Phi_n = \varphi(n)$. The first four cyclotomic polynomials are

$$\Phi_1(X) = X - 1,$$

$$\Phi_2(X) = X + 1,$$

$$\Phi_3(X) = X^2 + X + 1,$$

$$\Phi_4(X) = X^2 + 1.$$

Cyclotomic polynomials are quite complicated. In one version of a manual for the computer algebra system Maple ([21], p. 242, **numtheory[cyclotomic](n, var)**), it is stated that their coefficients are always ± 1 . It appears to be so, when looking at the first 104 cyclotomic polynomials. But

$$\begin{aligned} \Phi_{105}(X) = & 1 + X + X^2 - X^5 - X^6 - 2X^7 - X^8 - X^9 + X^{12} \\ & + X^{13} + X^{14} + X^{15} + X^{16} + X^{17} - X^{20} - X^{22} - X^{24} - X^{26} \\ & - X^{28} + X^{31} + X^{32} + X^{33} + X^{34} + X^{35} + X^{36} - X^{39} - X^{40} \\ & - 2X^{41} - X^{42} - X^{43} + X^{46} + X^{47} + X^{48} \end{aligned}$$

where the coefficients of X^7 and X^{41} are both -2 . I. Schur (1875–1941) proved that the coefficients of Φ_n are unbounded when n goes to infinity. In fact the coefficients of Φ_n have attracted the attention of researchers all through the twentieth century. The coefficients of Φ_n are always ± 1 if n is a product of two distinct prime numbers (notice that $105 = 3 \cdot 5 \cdot 7$). Cyclotomic polynomials have integer coefficients even though they are defined using roots of unity in the complex plane. This follows from a crucial identity, which turns out to make sense for polynomials over any ring, not just those with complex coefficients.

Proposition 4.4.3 *Let $n \geq 1$. Then*

- (i) $X^n - 1 = \prod_{d|n} \Phi_d(X)$;
- (ii) *the cyclotomic polynomials have integer coefficients,*

$$\Phi_n(X) \in \mathbb{Z}[X].$$

Proof. The roots of the polynomial on the right hand side of the identity in (i) are the primitive d th roots of unity, where $d | n$. They are also roots of the polynomial on the left hand side. However, if $\xi = e^{k2\pi i/n}$, where $1 \leq k \leq n$ is a root of the polynomial on the left hand side, then ξ is a primitive d th root of unity for some $d \leq n$. But $\xi^n = 1$ implies that $d | n$ by Lemma 4.4.1, so that ξ is also a root of the polynomial on the right hand side. Thus the polynomials on the left and right hand sides have the same roots. Since they are both monic and neither has multiple roots, they must be identical by Theorem 4.3.5. To prove that $\Phi_n \in \mathbb{Z}[X]$, we use induction. Clearly $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Let $n > 1$ and $f = \prod_{d < n, d|n} \Phi_d$. Then

$$X^n - 1 = \Phi_n f.$$

By induction, f is a monic polynomial in $\mathbb{Z}[X]$. Division of polynomials (Corollary 4.2.4) gives $X^n - 1 = \varphi f + r$, where $r = 0$ or $r \neq 0$, $\deg(r) < \deg(f)$ and $\varphi \in \mathbb{Z}[X]$. The uniqueness of q and r in Corollary 4.2.5 applied inside $\mathbb{C}[X]$ to f and $X^n - 1$ shows that $\Phi_n = \varphi$ and $r = 0$. Thus $\Phi_n = \varphi \in \mathbb{Z}[X]$. \square

Now let R be a ring. The unique ring homomorphism $\kappa : \mathbb{Z} \rightarrow R$ (see Lemma 3.3.3) gives a ring homomorphism $\kappa' : \mathbb{Z}[X] \rightarrow R[X]$ (see Exercise 4.15). In this way we may view the cyclotomic polynomial $\Phi_n \in \mathbb{Z}[X]$ as the polynomial $\kappa'(\Phi_n) \in R[X]$. This leads to the important identity

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{4.1}$$

in $R[X]$ by applying the ring homomorphism κ' to the corresponding identity in $\mathbb{Z}[X]$ (which comes from Proposition 4.4.3).

4.5 Primitive roots

The definition of a primitive root makes sense not only in the complex numbers but also in an arbitrary ring. Notice again that we take a classical idea (from

complex numbers) and bring it to use (in fact a great deal of use) in abstract algebra.

Definition 4.5.1 Let R be a ring and n a positive natural number. An element $\alpha \in R$ is called a *primitive n th root of unity* in R if $\alpha^n = 1$ and

$$\alpha, \alpha^2, \dots, \alpha^{n-1} \neq 1.$$

This leads to the following important lemma.

Lemma 4.5.2 Let α be an element in a domain R . If $\Phi_n(\alpha) = 0$ and α is not a multiple root of $X^n - 1 \in R[X]$ then α is a primitive n th root of unity in R .

Proof. The identity (4.1) in $R[X]$ gives $f\Phi_n = X^n - 1$ for $f \in R[X]$. Therefore $\alpha^n - 1 = f(\alpha)\Phi_n(\alpha) = 0$ and $\alpha^n = 1$. If α is a primitive d th root of unity for $1 \leq d < n$ then $d \mid n$, as in the proof of Lemma 4.4.1. In this case $X^d - 1 = \prod_{e \mid d} \Phi_e(X)$, again by (4.1). Since R is a domain we must have $\Phi_e(\alpha) = 0$ for some $e \mid d$. Therefore α is a root in Φ_n and Φ_e , where $e \mid n$ and $e < n$. This proves by (4.1) that α is a multiple root of $X^n - 1$, contradicting our assumption. \square

Having introduced primitive roots in rings and proved Lemma 4.5.2 we can obtain a simple proof of the following beautiful result due to Gauss.

Theorem 4.5.3 (Gauss) Let F be a field and $G \subseteq F^*$ a finite subgroup of the group of the units in F . Then G is cyclic.

Proof. Let $N = |G|$ and consider the polynomial

$$X^N - 1 = \prod_{d \mid N} \Phi_d \in F[X].$$

The roots of the polynomial on the left hand side are precisely the elements of G , since $\alpha^N = 1$ for every $\alpha \in G$ by Proposition 2.6.3(ii). There can be no more than N roots by Theorem 4.3.5 and none of these is a multiple root. This shows that Φ_N must have $\deg \Phi_N = \varphi(N)$ roots. These are primitive N th roots of unity in F by Lemma 4.5.2 and thereby generators of G . \square

Theorem 4.5.3 shows in particular that \mathbb{F}_p^* is a cyclic group, where p is a prime number. An integer a such that $[a]$ generates \mathbb{F}_p^* is called a *primitive root*

modulo p . Thus a primitive root a satisfies

$$\mathbb{F}_p^* = \{[1], [a], [a^2], \dots, [a^{p-2}]\}.$$

If $p = 13$ and $a = 2$ we have

$$\mathbb{F}_{13}^* = \{[1], [2], [4], [8], [3], [6], [12], [11], [9], [5], [10], [7]\}.$$

So 2 is a primitive root modulo 13. Finding primitive roots modulo a given prime p is very difficult. There seems to be no other way than trying out elements in \mathbb{F}_p^* and seeing whether they generate \mathbb{F}_p^* . In this sense the proof of Theorem 4.5.3 is abstract and nice. It gives the comfort of knowing of the existence of a generator by appealing to properties of cyclotomic polynomials. But it leaves no clue as how to find the former. The difficulty of this problem is probably related to the difficulty of computing φ for large integers. Suppose that we pick a random element $a \in \mathbb{F}_p^*$. By Theorem 4.5.3, the probability that a will be a primitive root is

$$\frac{\varphi(p-1)}{p-1},$$

since there are $\varphi(p-1)$ generators in a cyclic group of order $p-1$ by Proposition 2.7.4(iii). This number depends heavily on the prime p . Using the Dirichlet theorem on primes in arithmetic progressions one may show that there are primes for which this probability is arbitrarily small ([17], Proposition II.1.3).

4.5.1 Decimal expansions and primitive roots

Here is a famous open problem called the Artin conjecture (after E. Artin (1898–1962)). Given an integer $a > 1$ that is not a square, is a a primitive root for infinitely many prime numbers p ? For $a = 10$ this was proved by Gauss. It amounts to showing that there are infinitely many primes p such that the period of the decimal expansion of $1/p$ has length $p-1$. Let us give two examples of this. If $p = 7$ then

$$1/p = 0.142857142857 \dots$$

Here the period length is 6. If $p = 17$ then

$$1/p = 0.05882352941176470588 \dots$$

Here the period length is 16. In general the period length of the fraction $1/p$ is of order $[10]$ in \mathbb{F}_p^* (see Exercise 4.23). So you can use floating point arithmetic to determine the order of $[10]$ in \mathbb{F}_p^* (pocket calculators have limited display size, but a small PC easily handles “infinite” precision floating point numbers).

4.5.2 Primitive roots and public key cryptography

Let us briefly illustrate how the cyclic group $G = \mathbb{F}_p^*$ can be used to construct a public key cryptosystem called the ElGamal cryptosystem. We know from Chapter 1 how to find a large prime number p . Assume now that the involved parties have agreed on sharing a common generator g for G .

The secret deciphering key for A is a number $0 < a < p - 1$. The public key for A is then g^a . To send a message $P \in G$ to A we first generate a random integer k and then send

$$(g^k, Pg^{ak})$$

to A . Now A receives a pair (x, y) where $x, y \in G$. Since A knows a , A can retrieve the original message P by computing $x^{-a}y$. All these operations can be done quite effectively using the repeated squaring algorithm and the extended Euclidean algorithm from Chapter 1.

The security of the cryptosystem relies on the observation that it is difficult to compute a given g^a in G . This problem is known as the discrete logarithm problem in the group G , since a can be viewed as the “discrete” logarithm $\log_g(g^a)$ in the finite group G .

The above cryptosystem makes sense for any cyclic group G . One of the most promising avenues for modern cryptosystems is taking G as a (large) cyclic subgroup of an elliptic curve over a finite field.

4.5.3 Yet another application of cyclotomic polynomials

Using Gaussian integers we proved in Theorem 3.5.20 that there are infinitely many prime numbers $\equiv 1 \pmod{4}$. Using cyclotomic polynomials we can generalize this result.

Theorem 4.5.4 *There are infinitely many prime numbers $\equiv 1 \pmod{n}$ for a natural number $n \geq 2$.*

Proof. It suffices to prove that there exists a prime number $\equiv 1 \pmod{n}$ for every $n \geq 2$ (why?). Let n be given. We must find a prime number $p \equiv 1 \pmod{n}$. Since $n \geq 2$ we get $|\Phi_n(n)| > 1$ from Definition 4.4.2. So we may find a prime number p dividing $\Phi_n(n)$. Now Φ_n has a constant term $= \pm 1$ since $|\Phi_n(0)| = 1$ and $\Phi_n(0) \in \mathbb{Z}$. This implies that $p \nmid n$. Therefore $[n]$ is not a multiple root of $X^n - 1 \in \mathbb{F}_p[X]$ by Lemma 4.3.8. Since $\Phi_n([n]) = 0$ in \mathbb{F}_p , this implies by Lemma 4.5.2 that $\text{ord}([n]) = n$ in \mathbb{F}_p^* , and therefore that n divides $|\mathbb{F}_p^*| = p - 1$ by Proposition 2.6.3(i). This proves that $p \equiv 1 \pmod{n}$. \square

4.6 Ideals in polynomial rings

When is a polynomial ring a Euclidean domain, a principal ideal domain, a unique factorization domain? What are the units? The irreducible elements (polynomials)? How do these concepts relate to roots of polynomials?

In the case of an arbitrary ring these questions cannot be answered easily. There is one crucial result, once again due to Gauss: if R is a unique factorization domain then $R[X]$ is a unique factorization domain. We will not prove this. Our point of departure will be the case where R is a field, which will be denoted F .

Proposition 4.6.1 *The polynomial ring $F[X]$ is a Euclidean domain, a principal ideal domain and a unique factorization domain.*

Proof. We will prove that the degree function $\deg : F[X] \setminus \{0\} \rightarrow \mathbb{N}$ is a Euclidean function on $F[X]$ (see subsection 3.5.4). Let $d \in F[X] \setminus \{0\}$. Then there exists $q, r \in F[X]$ such that

$$f = qd + r,$$

where either $r = 0$ or $\deg(r) < \deg(d)$. This is the content of Corollary 4.2.5, and it follows that \deg is a Euclidean function on $F[X]$. Thus $F[X]$ is a Euclidean domain. This implies by Proposition 3.5.9 that $F[X]$ is a principal ideal domain. We obtain that $F[X]$ is a unique factorization domain by Theorem 3.5.7. \square

Having proved that the degree function on $F[X]$ is a Euclidean function $F[X] \setminus \{0\} \rightarrow \mathbb{N}$, we may now use the Euclidean algorithm (as in subsection 3.5.4). This is illustrated in the following example.

Example 4.6.2 Let us use the Euclidean algorithm to find a greatest common divisor of $X^5 + X + 1$ and $X^4 + X^3 + X + 1$ in $\mathbb{F}_2[X]$. Using the division algorithm for polynomials we get

$$X^5 + X + 1 = (X + 1)(X^4 + X^3 + X + 1) + X^3 + X^2 + X$$

and

$$\begin{aligned} X^4 + X^3 + X + 1 &= X(X^3 + X^2 + X) + X^2 + X + 1 \\ X^3 + X^2 + X &= X(X^2 + X + 1). \end{aligned}$$

This shows that $X^2 + X + 1$ is a greatest common divisor of $X^5 + X + 1$ and $X^4 + X^3 + X + 1$ in $\mathbb{F}_2[X]$.

Now we move on to state some useful facts about the unique factorization domain $F[X]$. Notice that the concepts of units, irreducible elements etc. from Chapter 3 make perfectly sense for $F[X]$. Irreducible elements in $F[X]$ are called irreducible polynomials. Before embarking upon the next result, let us notice how the degree function comes into play. If $f \in F[X]$ and $f = f_1 f_2$ then

$$\deg(f) = \deg(f_1) + \deg(f_2).$$

If $f = f_1 f_2$ is an honest factorization of f , i.e. if neither f_1 nor f_2 is a constant then $0 < \deg(f_1), \deg(f_2) < \deg(f)$. Polynomials that are units are non-zero constants (degree zero). So if f is not irreducible there is a factorization $f = f_1 f_2$ such that

$$0 < \deg(f_1), \deg(f_2) < \deg(f).$$

This gives us a nice way of deducing that some polynomials are irreducible even if they do not have any roots.

Proposition 4.6.3 *Let $f \in F[X]$. Then we have the following.*

- (i) *The ideal $\langle f \rangle$ is a maximal ideal if and only if f is irreducible. In this case the quotient ring*

$$F[X]/\langle f \rangle$$

is a field.

- (ii) *If $f \neq 0$ then f is a unit if and only if $\deg(f) = 0$.*
 (iii) *If $\deg(f) = 1$ then f is irreducible.*
 (iv) *If f is irreducible and $\deg(f) > 1$ then f does not have any roots.*
 (v) *If $\deg(f) = 2$ or $\deg(f) = 3$ then f is irreducible if and only if it has no roots.*

Proof. (i) This is a consequence of Proposition 3.5.6 and the fact that $F[X]$ is a principal ideal domain. If $\langle f \rangle$ is a maximal ideal then $F[X]/\langle f \rangle$ is a field by Proposition 3.2.7.

(ii) Non-zero constants (polynomials of degree 0) are units, since F is a field. This follows from Proposition 4.2.3.

(iii) If f is not an irreducible polynomial then there is a factorization $f = f_1 f_2$ where $0 < \deg(f_1), \deg(f_2) < \deg(f)$. In particular, if $\deg(f) = 1$ then f has to be irreducible.

(iv) If $\alpha \in k$ is a root of f then $f(\alpha) = 0$ and $f = (X - \alpha)h$ for some $h \in k[X]$, by Corollary 4.3.2. This gives $\deg(f) = 1 + \deg(h)$. Since $\deg(f) > 1$, f cannot be irreducible if it has a root.

(v) If $\deg(f) = 2$ or 3 and f is reducible then there is a factorization $f = f_1 f_2$, where either $\deg(f_1) = 1$ or $\deg(f_2) = 1$, since $\deg(f_1) + \deg(f_2) = \deg(f) = 2$ or 3 . This shows that f is reducible if and only if a polynomial of degree 1 divides f . This is equivalent to f having a root. \square

Example 4.6.4 Consider the polynomial

$$f = X^3 + X + 1 \in \mathbb{F}_5[X].$$

The following table shows that f does not have any roots:

x	0	1	2	3	4
$f(x)$	1	3	1	1	4

So we may conclude from Proposition 4.6.3(v) that f is an irreducible polynomial in $\mathbb{F}_5[X]$. What about the polynomial $g = X^4 + X^2 + 1 \in \mathbb{F}_2[X]$? Clearly g does not have any roots. Can we conclude from Proposition 4.6.3 that g is irreducible?

Remark 4.6.5 Cyclotomic polynomials are irreducible as polynomials in $\mathbb{Q}[X]$. This is classical result due to Gauss. The proof consists of a number of clever steps (see Exercise 4.45 (HOF)). What about cyclotomic polynomials when viewed as polynomials in $\mathbb{F}_p[X]$? The cyclotomic polynomial $\Phi_8 = X^4 + 1$ is an example of a polynomial that is reducible in $\mathbb{F}_p[X]$ for all prime numbers p (see Exercise 4.13). In fact one can prove that Φ_n is irreducible in $\mathbb{F}_p[X]$ if and only if $[p]$ generates the group $(\mathbb{Z}/n\mathbb{Z})^*$ (see Exercise 4.43).

A central example is the polynomial $X^2 + 1 \in \mathbb{R}[X]$. This polynomial does not have any roots in \mathbb{R} (since no real number squared equals -1). So by Proposition 4.6.3(v) it follows that $X^2 + 1$ is an irreducible polynomial in $\mathbb{R}[X]$. Also, it follows from Proposition 4.6.3(i) that

$$\mathbb{R}[X]/\langle X^2 + 1 \rangle$$

is a field. In fact it is a very well known field. The next section will reveal the details.

4.6.1 Polynomial rings modulo ideals

The following situation is extremely common: there is a field F and a polynomial $f \in F[X]$ with no roots in F along with an extension field $E \supset F$ such that there exists $\alpha \in E$ with $f(\alpha) = 0$ (think of $F = \mathbb{R}$, $f = X^2 + 1$ and $E = \mathbb{C}$). For later use it is important to notice that $f(\alpha)$ makes sense even though $\alpha \in E$ and $f \in F[X]$. The simple reason is that $F[X] \subseteq E[X]$ as a subring. The purpose of this subsection is to describe an algebraic tool for obtaining an extension field E and a root $\alpha \in E$ given F and $f \in F[X]$. The idea is very clear but hidden in a few technicalities. Let us begin with a detailed example.

Example 4.6.6 We know that

$$F = \mathbb{R}[X]/\langle X^2 + 1 \rangle$$

is a field, since $X^2 + 1$ is an irreducible polynomial in $\mathbb{R}[X]$. How do we describe this field? At this point it is just an abstract quotient ring consisting of cosets of the ideal $\langle X^2 + 1 \rangle$. If we make a few identifications then things become much clearer. By definition

$$F = \{[f] \mid f \in \mathbb{R}[X]\},$$

where $[f]$ is the coset $f + \langle X^2 + 1 \rangle$. Dividing f by $X^2 + 1$ we get

$$f = q(X^2 + 1) + aX + b,$$

where $a, b \in \mathbb{R}$. This is a consequence of Proposition 4.2.4 and a substantial simplification of $[f]$, since

$$[f] = [q(X^2 + 1) + aX + b] = [aX + b]$$

because $q(X^2 + 1) \in \langle X^2 + 1 \rangle$. So we may write

$$F = \{[aX + b] \mid a, b \in \mathbb{R}\}.$$

An added bonus is that the elements in F are uniquely given as $[aX + b]$, where $a, b \in \mathbb{R}$. Suppose that $[aX + b] = [cX + d]$, where $c, d \in \mathbb{R}$. Then $(aX + b) - (cX + d) = (a - c)X + (b - d) \in \langle X^2 + 1 \rangle$. Thus

$$(a - c)X + (b - d) = q(X^2 + 1)$$

for some $q \in \mathbb{R}[X]$. Here Proposition 4.2.2 gives that $a = c$ and $b = d$.

The next step is to realize that \mathbb{R} is a subring of F . This is easy: instead of writing $[r]$ we simply write r when $r \in \mathbb{R}$ is a constant polynomial. This is

allowed, since $[r_1] = [r_2]$ if and only $r_1 = r_2$, when $r_1, r_2 \in \mathbb{R}$. So

$$F = \{a + b[X] \mid a, b \in \mathbb{R}\}.$$

We now have a satisfactory description of the elements in F . Addition and multiplication in F are given using addition and multiplication in a quotient ring: thus $[g_1] + [g_2] = [g_1 + g_2]$ and $[g_1][g_2] = [g_1g_2]$. In our notation addition is given by

$$(a + b[X]) + (c + d[X]) = (a + c) + (b + d)[X].$$

To do multiplication we obtain initially

$$(a + b[X])(c + d[X]) = ac + (ad + bc)[X] + bd[X^2].$$

But $[X^2]$ does not fit our description of elements in F as given by $x + y[X]$ with $x, y \in \mathbb{R}$. Fortunately this is easy to repair since $[X^2] = [-1] = -1 \in F$. With this in mind we get

$$(a + b[X])(c + d[X]) = (ac - bd) + (ad + bc)[X].$$

Through this algebraic process we have shown that F is the field \mathbb{C} of complex numbers. The role of $i = \sqrt{-1}$ is played by $[X] \in F$ as $[X]^2 = [X^2] = -1$.

We now return to the general case of coefficients in a ring R . We know that R is a natural subring (consisting of the constant polynomials) of $R[X]$. Let I be an ideal in $R[X]$ with $R \cap I = \langle 0 \rangle$ (0 is the only constant polynomial in I). If $r_1, r_2 \in R$ and $[r_1] = [r_2]$ in $R[X]/I$ then $r_1 - r_2 \in R \cap I$. Therefore $r_1 = r_2$. So if $R \cap I = \langle 0 \rangle$ then we may use the notation r to denote the element $[r]$ in $R[X]/I$ (where $r \in R$). The details of Example 4.6.6 cover all the steps in the proof of the following proposition.

Proposition 4.6.7 *Let R be a ring and*

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$$

a monic polynomial of positive degree n . Then $R \cap \langle f \rangle = \langle 0 \rangle$. The elements $[g] = g + \langle f \rangle$ in the quotient ring $R[X]/\langle f \rangle$ can be expressed uniquely as polynomials of degree $< n$

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

where $b_0, \dots, b_{n-1} \in R$ and $\alpha = [X]$. In $R[X]/\langle f \rangle$ we have the identity

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0.$$

Proof. Suppose that $r \in R \cap \langle f \rangle$. Then there exists $q \in R[X]$ such that $r = qf$. If $q \neq 0$ then $\deg(q) + \deg(f) = \deg(q) + n > 0$ by Proposition 4.2.2. This contradicts that r is a constant. So $q = 0$ and $R \cap \langle f \rangle = \langle 0 \rangle$.

Suppose that $[g] \in R[X]/\langle f \rangle$. Write $g = qf + r$, where $r = 0$ or $r \neq 0$ and $\deg(r) < n = \deg(f)$ after dividing by f . So $[g] = [qf + r] = [qf] + [r] = [r]$. Suppose that $r_1, r_2 \in R[X] \setminus \{0\}$, that $\deg(r_1), \deg(r_2) < n$ and that $[r_1] = [r_2]$. Then there exists $q \in R[X]$ such that $r_1 - r_2 = qf$. By the same reasoning (using Proposition 4.2.2) as above we see that $r_1 = r_2$. So every non-zero element in the quotient ring can be described uniquely as $[g]$, where $\deg(g) < n$ and $g \in R[X] \setminus \{0\}$. Writing this out we obtain

$$[g] = [b_0 + b_1X + \cdots + b_{n-1}X^{n-1}] = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

where $\alpha = [X]$ and $b_0, \dots, b_{n-1} \in R$. Since

$$\begin{aligned} [f] &= [X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0] \\ &= [X^n] + a_{n-1}[X^{n-1}] + \cdots + a_1[X] + a_0 \\ &= \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0, \end{aligned}$$

we get the desired identity for α^n in $R[X]/\langle f \rangle$. \square

Notice that R is a natural subring of $R[X]/\langle f \rangle$ above. The natural ring homomorphism $\varphi : R \rightarrow R[X]/\langle f \rangle$ given by $\varphi(r) = [r]$ is injective.

Remark 4.6.8 If F is a field and $f \in F[X]$ an irreducible polynomial then $\langle f \rangle$ is a maximal ideal and $F[X]/\langle f \rangle$ becomes a field extension E of F . Now $\alpha = [X] \in E$, and this actually is a root of $f \in F[X] \subseteq E[X]$ since $f(\alpha) = 0$ by the identity for α^n in Proposition 4.6.7. This is the algebraic way of using an irreducible polynomial to construct a bigger field where it has a root.

Let us illustrate how the identity for α^n in Proposition 4.6.7 completely determines multiplication in the quotient ring.

Example 4.6.9 Let $f = X^2 + X + 1 \in \mathbb{F}_2[X]$. Then f is an irreducible polynomial since it has no roots (Proposition 4.6.3). This means that $\langle f \rangle$ is a maximal ideal and that the quotient ring $F = \mathbb{F}_2[X]/\langle f \rangle$ is a field. Now, by Proposition 4.6.7, $F = \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{F}_2\}$, where $\alpha = [X]$ and the rule $\alpha^2 = -1 - \alpha$ determines the multiplication. Multiplying $a + b\alpha$ by $c + d\alpha$ we get

$$\begin{aligned} ac + (ad + bc)\alpha + bd\alpha^2 &= ac + (ad + bc)\alpha + bd(-1 - \alpha) \\ &= (ac - bd) + (ad + bc - bd)\alpha. \end{aligned}$$

Notice that F is an extension field of \mathbb{F}_2 with four elements.

Having proved Proposition 4.6.7 we have the tools for proving one of the true highlights of number theory.

4.7 Theorema Aureum: the law of quadratic reciprocity

We now show how a specific quotient of a polynomial ring gives a beautiful proof of the law of quadratic reciprocity (see Section 1.11). Gauss called the law of quadratic reciprocity Theorema Aureum, the golden theorem. He gave six proofs (see [14], Chapter 5) of this theorem during his lifetime. In 1921 there were 56 known proofs of quadratic reciprocity. Today there could be well over a hundred. Let us recall the statement of quadratic reciprocity. We are given two odd prime numbers p and q . Then the Legendre symbols (Definition 1.11.1) of p and q are related through the breathtaking identity

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

We will work in the ring

$$R = \mathbb{F}_p[X]/(1 + X + \cdots + X^{q-1}).$$

Recall from Proposition 4.6.7 that an element in R can be written uniquely in terms of $\zeta = [X]$ as

$$a_0 + a_1\zeta + \cdots + a_{q-2}\zeta^{q-2},$$

where $a_0, \dots, a_{q-2} \in \mathbb{F}_p$.

Lemma 4.7.1 *The element ζ is a primitive q th root of unity in R . Let $\xi = \zeta^l$ where $q \nmid l$. Then*

$$1 + \xi + \cdots + \xi^{q-1} = 0$$

in R .

Proof. It follows from Proposition 4.6.7 that $\zeta, \dots, \zeta^{q-2} \neq 1$ and

$$\zeta^{q-1} = -1 - \zeta - \cdots - \zeta^{q-2} \neq 1.$$

A small computation now shows that $\zeta^q = \zeta\zeta^{q-1} = 1$. This proves that ζ is a primitive q th root of unity. If $q \nmid l$ then $\gcd(q, l) = 1$. Therefore $\{1, \zeta, \dots, \zeta^{q-1}\} = \{1, \xi, \dots, \xi^{q-1}\}$. It follows that

$$1 + \xi + \cdots + \xi^{q-1} = 1 + \zeta + \cdots + \zeta^{q-1} = 0. \quad \square$$

Now consider the so-called Gauss sum

$$G = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \zeta^j$$

in R . The individual terms satisfy

$$\left(\frac{j}{q}\right) \zeta^j = \left(\frac{j+qm}{q}\right) \zeta^{j+qm}$$

for every $m \in \mathbb{Z}$. This is used heavily in the proof of the following important lemma.

Lemma 4.7.2 *The Gauss sum $G \in R$ satisfies the following.*

- (i) $G^2 = (-1)^{(q-1)/2} q$.
- (ii) G is an invertible element in the ring R if $p \neq q$.

Proof. The invertibility of G follows from (i) as $q \in \mathbb{F}_p \subset R$ is invertible in R since it is invertible in \mathbb{F}_p if $p \neq q$. The proof of (i) is fairly straightforward, but it contains some clever rewritings:

$$\begin{aligned} G^2 &= \left(\sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \zeta^j \right) \left(\sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \zeta^j \right) \\ &= \left(\sum_{i=1}^{q-1} \left(\frac{i}{q}\right) \zeta^i \right) \left(\sum_{j=1}^{q-1} \left(\frac{-j}{q}\right) \zeta^{-j} \right), \end{aligned}$$

since

$$\left(\frac{-j}{q}\right) \zeta^{-j} = \left(\frac{q-j}{q}\right) \zeta^{q-j}.$$

We continue by rewriting the last sum in the expression for G^2 :

$$\begin{aligned} \sum_{i,j=1}^{q-1} \left(\frac{i}{q}\right) \left(\frac{-j}{q}\right) \zeta^{i-j} &= \left(\frac{-1}{q}\right) \sum_{i,j=1}^{q-1} \left(\frac{ij}{q}\right) \zeta^{i-j} \\ &= (-1)^{(q-1)/2} \sum_{i,j=1}^{q-1} \left(\frac{i^2 j}{q}\right) \zeta^{i(1-j)}. \end{aligned}$$

Here we have used the formula

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$$

from Proposition 1.11.6. We have also replaced j with ij in the terms of the sum. We may do this because if j runs through $1, \dots, q-1$ then the remainders of ij modulo q run through $1, \dots, q-1$ (though not in the same order). Since

$$\left(\frac{i^2}{q}\right) = 1,$$

we end up with the expression

$$(-1)^{(q-1)/2} \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \sum_{i=1}^{q-1} \zeta^{i(1-j)},$$

which is equal to

$$(-1)^{(q-1)/2} \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \sum_{i=0}^{q-1} \zeta^{i(1-j)}$$

since

$$\sum_{j=1}^{q-1} \left(\frac{j}{q}\right) = 0$$

by Proposition 1.11.3. By Lemma 4.7.1 it follows that

$$\sum_{i=0}^{q-1} \zeta^{i(1-j)}$$

is non-zero precisely if $j = 1$. In this case it is equal to q , proving the formula for G^2 . \square

Raising G to the p th power in R we get the formula

$$\begin{aligned} G^p &= (G^2)^{(p-1)/2} G = (-1)^{(p-1)(q-1)/4} q^{(p-1)/2} G \\ &= (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right) G \end{aligned} \quad (4.2)$$

by Lemma 4.7.2 and Theorem 1.11.4. Computing the left hand side from the definition and using Freshman's Dream (Theorem 3.3.9) in the ring R we get

$$\begin{aligned} G^p &= \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \zeta^{pj} = \sum_{j=0}^{q-1} \left(\frac{p}{q}\right) \left(\frac{pj}{q}\right) \zeta^{pj} \\ &= \left(\frac{p}{q}\right) G. \end{aligned}$$

Comparing this expression with (4.2) and using that G is invertible in R (Lemma 4.7.2), we obtain the law of quadratic reciprocity,

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).$$

4.8 Finite fields

Finite fields are among the most beautiful objects in algebra. We already know the finite fields \mathbb{F}_p , where p is a prime number. But Example 4.6.9 indicated that this is not the whole story (there we constructed a field with $4 = 2^2$ elements). In this section we prove that there exists a unique (up to ring isomorphism) finite field with p^n elements, where p is a prime number and n a natural number. We start out with a lemma showing that a finite field looks exactly like the extension field we encountered in Example 4.6.9.

Lemma 4.8.1 *Let F be a finite field. Then $|F| = p^n$, where p is a prime number, $n \geq 1$ and there exists an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n such that*

$$F \cong \mathbb{F}_p[X]/\langle f \rangle.$$

Proof. Consider the unique ring homomorphism $\kappa : \mathbb{Z} \rightarrow F$. Since F is finite, κ is not injective. This implies that the characteristic of F is a prime number p , by Proposition 3.3.7. We may view \mathbb{F}_p as a subring of F by Lemma 3.3.5. As F is finite we obtain from Theorem 4.5.3 that F^* is a cyclic group. Let $\gamma \in F^*$ be a generator for F^* . Thus every element in F is either 0 or a power γ^n of γ . Since $\varphi_\gamma(X^n) = \gamma^n$, the ring homomorphism $\varphi_\gamma : \mathbb{F}_p[X] \rightarrow F$ is surjective. More than this is true, though. In fact by restricting φ_γ to $\mathbb{F}_p[X] \subseteq F[X]$ we get a surjective ($X^n \in \mathbb{F}_p[X]$) ring homomorphism

$$\varphi : \mathbb{F}_p[X] \rightarrow F.$$

The kernel $\text{Ker } \varphi$ of φ is a principal ideal $\langle f \rangle \subseteq \mathbb{F}_p[X]$ by Proposition 4.6.1. By Proposition 3.3.2 we get

$$\mathbb{F}_p[X]/\langle f \rangle \cong F,$$

so that $\langle f \rangle$ is a maximal ideal by Proposition 3.2.7. This implies that f is an irreducible polynomial by Proposition 4.6.3(i). By Proposition 4.6.7, $|F| = p^n$, where $n = \deg(f)$. This proves the lemma. \square

The main result is the existence and uniqueness up to isomorphism of the finite fields alluded to in Lemma 4.8.1. Below we state the theorem. The main ingredients in the proof will occupy subsections 4.8.1 and 4.8.2.

Theorem 4.8.2 *There exists a unique finite field with p^n elements, where p is a prime number and $n \geq 1$. More precisely, we have the following.*

- (i) *There exists an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n .*
- (ii) *Suppose that F and F' are finite fields with p^n elements. Then there exists a ring isomorphism $F \xrightarrow{\sim} F'$.*

Proof. Suppose that f is an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n . Then $\langle f \rangle$ is a maximal ideal by Proposition 4.6.3(i). Therefore $\mathbb{F}_p[X]/\langle f \rangle$ is a field. It has p^n elements by Proposition 4.6.7. The proof of (i) is a surprising application of cyclotomic polynomials and will be described in subsection 4.8.1. The proof of (ii) is described in subsection 4.8.2. \square

Before entering the finer details of the proof of Theorem 4.8.2 we need a crucial lemma involving only natural numbers.

Lemma 4.8.3 *Let τ , d and n be natural numbers, where $\tau > 1$. Then $\tau^d - 1$ divides $\tau^n - 1$ if and only if d divides n .*

Proof. We may assume that $d \geq 1$. By Theorem 1.2.1 we write $n = qd + r$, where $0 \leq r < d$. Then

$$\begin{aligned} \frac{\tau^n - 1}{\tau^d - 1} &= \frac{(\tau^d)^q \tau^r - 1}{\tau^d - 1} \\ &= \tau^r \frac{(\tau^d)^q - 1}{\tau^d - 1} + \frac{\tau^r - 1}{\tau^d - 1} \\ &= \tau^r (1 + \tau^d + \cdots + (\tau^d)^{q-1}) + \frac{\tau^r - 1}{\tau^d - 1}. \end{aligned}$$

As $0 \leq \tau^r - 1 < \tau^d - 1$ this proves the claim. \square

Remark 4.8.4 Theorem 4.8.2 says that there exists a unique field F with p^n elements up to isomorphism. We denote F by \mathbb{F}_{p^n} . Informally one may say that there is only one way to multiply in a finite field with p^n elements.

4.8.1 Existence of finite fields

We know that there are infinitely many irreducible polynomials in $\mathbb{F}_p[X]$ (see Exercise 4.7), but this does not guarantee that we may find one of each degree. This is where cyclotomic polynomials enter. If we view them as polynomials in $\mathbb{F}_p[X]$ they have very interesting properties.

Theorem 4.8.5 *There exists an irreducible polynomial in $\mathbb{F}_p[X]$ of degree $n \geq 1$. More precisely, if f is an irreducible polynomial dividing Φ_{p^n-1} in $\mathbb{F}_p[X]$ then $\deg(f) = n$.*

Proof. Let $d = \deg(f)$. Then $L = \mathbb{F}_p[X]/\langle f \rangle$ is a field with p^d elements and $\alpha = [X]$ is a root of $f \in \mathbb{F}_p[X] \subseteq L[X]$ by Remark 4.6.8. Since $gf = \Phi_{p^n-1}$ for $g \in \mathbb{F}_p[X]$ we get $\Phi_{p^n-1}(\alpha) = g(\alpha)f(\alpha) = 0$. The derivative of $X^{p^n-1} - 1$ is

$$D(X^{p^n-1} - 1) = (p^n - 1)X^{p^n-2} = -X^{p^n-2}.$$

This shows by Lemma 4.3.8 that α is not a multiple root of $X^{p^n-1} - 1$ and therefore that α is a primitive $(p^n - 1)$ th root of unity in L by Lemma 4.5.2. Now, $\alpha^{p^d-1} = 1$ shows that $p^n - 1 \mid p^d - 1$ by Proposition 2.6.3.

Let $R = \{\xi \in L \mid \xi^{p^n} = \xi\}$. This is a subring of L by Theorem 3.3.9. Since $\alpha^{p^n-1} = 1$ we must have $\alpha \in R$. But since $L = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \mid a_i \in \mathbb{F}_p\}$ by Proposition 4.6.7 it follows that $R = L$ (R contains $1, \alpha, \alpha^2, \dots$ and is a subring). By Theorem 4.5.3 there exists a primitive $(p^d - 1)$ th root of unity ζ in L . Since $\zeta \in R$ we obtain $\zeta^{p^n-1} = 1$. Proposition 2.6.3(iii) gives $p^d - 1 \mid p^n - 1$. Therefore $p^d - 1 = p^n - 1$. This shows that $d = n$. \square

Remark 4.8.6 Theorem 4.8.5 says that if

$$\Phi_{p^n-1} = f_1 \cdots f_r$$

is an irreducible factorization of Φ_{p^n-1} in $\mathbb{F}_p[X]$ then $\deg(f_i) = n$. In particular, $n \mid \varphi(p^n - 1)$.

4.8.2 Uniqueness of finite fields

Suppose that F and F' are finite fields with p^n elements. Then $F \cong \mathbb{F}_p[X]/\langle f \rangle$ for a suitable irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n , by Lemma 4.8.1.

Furthermore $f(\alpha) = 0$, where $\alpha = [X] \in F$ by Remark 4.6.8. Notice that $I = \{g \in \mathbb{F}_p[X] \mid g(\alpha) = 0\} \subsetneq \mathbb{F}_p[X]$ is an ideal in $\mathbb{F}_p[X]$. Now $f \in I$ and therefore $\langle f \rangle \subseteq I$. But since $\langle f \rangle$ is a maximal ideal we must have $I = \langle f \rangle$. Because F^* is a finite group with $p^n - 1$ elements, we obtain $\xi^{p^n-1} = 1$ for every $\xi \in F^*$ by Proposition 2.6.3(ii). This implies that $X^{p^n} - X \in I$ and therefore that $f \mid X^{p^n} - X$ in $\mathbb{F}_p[X]$. In $F'[X]$ we have the factorization

$$X^{p^n} - X = \prod_{\alpha \in F'} (X - \alpha),$$

since every $\beta \in F'$ satisfies $\beta^{p^n} = \beta$ by Proposition 2.6.3(ii). Therefore $f \in \mathbb{F}_p[X] \subseteq F'[X]$ must have a root α' in F' since it divides $X^{p^n} - X$. Now look at

$$\varphi_{\alpha'} : \mathbb{F}_p[X] \rightarrow F'.$$

Obviously $\langle f \rangle \subseteq \text{Ker } \varphi_{\alpha'}$, but since $\text{Ker } (\varphi_{\alpha'})$ is a proper ideal and $\langle f \rangle$ is a maximal ideal, we must have $\langle f \rangle = \text{Ker } (\varphi_{\alpha'})$. Therefore we get an injective ring homomorphism

$$\mathbb{F}_p[X]/\langle f \rangle \rightarrow F'.$$

But since F' has p^n elements, this must be a bijection and thereby an isomorphism (of rings). We have proved that two finite fields F and F' with the same number of elements are isomorphic.

4.8.3 A beautiful identity

We already know that

$$X^{p^n} - X = X(X^{p^n-1} - 1) = X \prod_{d \mid p^n-1} \Phi_d$$

in $\mathbb{F}_p[X]$. By Theorem 4.8.5, $X^{p^n} - X$ is divisible by an irreducible polynomial of degree n . This is not the entire story. We will compute the complete irreducible factorization of $X^{p^n} - X$ in $\mathbb{F}_p[X]$. Let us compute this factorization in some special cases.

Example 4.8.7 In $\mathbb{F}_2[X]$ we have

$$X^{2^2} - X = X^4 - X = X(X+1)(X^2+X+1).$$

In $\mathbb{F}_3[X]$ we have

$$X^{3^2} - X = X^9 - X = X(X+1)(X+2)(X^2+1)(X^2+X+2)(X^2+2X+2).$$

The general result is the following surprising theorem.

Theorem 4.8.8 *The polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$ is the product*

$$X^{p^n} - X = f_1 \cdots f_r$$

of the monic irreducible polynomials f_1, \dots, f_r in $\mathbb{F}_p[X]$ of degree d , where $1 \leq d \leq n$ and $d \mid n$.

Proof. Let $f \in \mathbb{F}_p[X]$ be a monic irreducible polynomial of degree d . Then $L = \mathbb{F}_p[X]/\langle f \rangle$ is a field (by Proposition 4.6.3(i)) with p^d elements (by Proposition 4.6.7). Let $\alpha = [X]$ in L . Then $\alpha^{p^d} = \alpha$ by Proposition 2.6.3(ii). If $d \mid n$ then $\alpha^{p^n} = \alpha$. This is seen by raising both sides of $\alpha^{p^d} = \alpha$ to the p^d th power $q-1$ times, where $n = qd$. The identity $\alpha^{p^n} = \alpha$ in L means that $X^{p^n} - X \in \langle f \rangle$ or that $f \mid X^{p^n} - X$.

Now assume that f divides $X^{p^n} - X$. We wish to prove that $d \mid n$. Consider the subset

$$R = \{\zeta \in L \mid \zeta^{p^n} = \zeta\}.$$

Then R is a subring of L by Theorem 3.3.9. It contains α , as f divides $X^{p^n} - X$. But since $L = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \mid a_i \in \mathbb{F}_p\}$, by Proposition 4.6.7, it follows that $R = L$ (R contains $1, \alpha, \alpha^2, \dots$ and is a subring). Let γ be a generator for the cyclic group L^* . The order of γ in the group L^* is $p^d - 1$, and $\gamma^{p^n-1} = 1$ since $\gamma \in R$. This implies by Proposition 2.6.3(iii) that $p^d - 1 \mid p^n - 1$. Finally, we obtain $d \mid n$ by Lemma 4.8.3.

Let f_1, \dots, f_r denote the monic irreducible polynomials of degree $d \mid n$. We have proved that

$$X^{p^n} - X = f_1^{n_1} \cdots f_r^{n_r},$$

where $n_1, \dots, n_r \geq 1$. One thing is still missing in the proof of our identity. We need to make sure that the multiplicities n_1, \dots, n_r are all 1. This can be done by proving that $X^{p^n} - X$ is not divisible by the square of an irreducible polynomial. This follows from Lemma 4.3.8(i), since $D(X^{p^n} - X) = p^n X^{p^n-1} - 1 = -1$. \square

We have the following consequence of Theorem 4.8.8.

Corollary 4.8.9 *Let N_d denote the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[X]$. Then*

$$p^n = \sum_{d|n} dN_d.$$

Proof. This follows by applying the degree function \deg to both sides of the formula in Theorem 4.8.8. \square

There are p irreducible monic polynomials of degree 1 in $\mathbb{F}_p[X]$. These can be listed as

$$X, \quad X - 1, \quad X - 2, \quad \dots, \quad X - (p - 1),$$

showing that $N_1 = p$. If q is a prime number then Corollary 4.8.9 implies that

$$p^q = qN_q + N_1 = qN_q + p;$$

thus

$$N_q = \frac{p^q - p}{q}.$$

It follows from Theorem 4.8.8 that in general

$$N_n = \frac{p^n - \sum_{d < n, d|n} dN_d}{n}.$$

An explicit formula for N_n is given by

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d,$$

where μ is the Möbius function (given by $\mu(1) = 1$, $\mu(n) = 0$, if n is divisible by a square > 1 , and $\mu(p_1 \cdots p_l) = (-1)^l$, where p_1, \dots, p_l are distinct primes). Another important consequence of Theorem 4.8.8 is a clever factoring algorithm for polynomials.

Suppose that $g \in \mathbb{F}_p[X]$ is a monic polynomial, $\deg(g) = d$ and

$$g = g_1 \cdots g_d,$$

where g_i denotes the product of the (monic) irreducible polynomials of degree i dividing g . Then it follows from Theorem 4.8.8 that

$$\gcd(g, X^{p^i} - X)$$

is the product of g_j for $j \mid i$. A straightforward algorithm for finding g_1, \dots, g_d is to insert $i = 1, 2, \dots$ in $\gcd(g, X^{p^i} - X)$ and use the Euclidean algorithm to compute the greatest common divisor; it is not clear when this algorithm was first discovered. The remaining problem is how to factor out the irreducible polynomials of the same degree i from g_i . A nice solution to this problem was found by Cantor and Zassenhaus in 1979 (see [16], subsection 4.6.2, or [6], subsection 8.4.4). You should prove Lemma 4.8.10 and gain some computational experience by doing Exercise 4.41.

We will move on to describe a general factoring algorithm for polynomials over \mathbb{F}_p and an easy criterion detecting when a given polynomial is irreducible, using only linear algebra. For an introduction to linear algebra over arbitrary fields please consult Appendix B.

4.9 Berlekamp's algorithm

Let f be a polynomial in $\mathbb{F}_p[X]$. We have a few ways, but they are very limited, of deciding whether f is irreducible. If $\deg(f) = 2, 3$ then Proposition 4.6.3 shows that f is irreducible if and only if f does not have a root. In degree 4 and above there seems to be no way other than brute force for deciding whether f is irreducible. Therefore it is quite surprising to find that there is an easy way of deciding this merely by looking at the matrices of two linear maps.

Since the quotient ring $R = \mathbb{F}_p[X]/\langle f \rangle$ has characteristic p , the Frobenius map $F(v) = v^p$ is a ring homomorphism

$$F : R \rightarrow R.$$

This is just Theorem 3.3.9. But here R is not only a ring, it is also a vector space over \mathbb{F}_p . Since $\lambda^p = \lambda$ for $\lambda \in \mathbb{F}_p$, $F : R \rightarrow R$ is in fact a linear map of \mathbb{F}_p vector spaces. A simple example will illustrate how linear algebra comes into play.

Example 4.9.1 Let $f = X^5 + X + 1 \in \mathbb{F}_2[X]$. Then $R = \mathbb{F}_2[X]/\langle f \rangle$ is a vector space over \mathbb{F}_2 with basis $1, \alpha, \alpha^2, \alpha^3, \alpha^4$, where $\alpha = [X]$. The element $\alpha^5 \in R$ is expressed in this basis as $\alpha + 1$ by Proposition 4.6.7. The Frobenius map $F(v) = v^2$ is an \mathbb{F}_2 -linear map $R \rightarrow R$. We can compute its 5×5 matrix with respect to the basis $1, \alpha, \alpha^2, \alpha^3, \alpha^4$. Since $F(1) = 1$, $F(\alpha) = \alpha^2$, $F(\alpha^2) = \alpha^4$, $F(\alpha^3) = \alpha^6 = \alpha\alpha^5 = \alpha(\alpha + 1) = \alpha^2 + \alpha$ and $F(\alpha^4) = \alpha^8 = \alpha^3\alpha^5 = \alpha^3(\alpha + 1) = \alpha^4 + \alpha^3$, the matrix of F is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

If $\text{Ker}(F) \neq 0$ we can find a non-constant polynomial $g \in F_p[X]$ such that $\deg(g) < \deg(f)$ and $[g]^p = [0]$. This means that $f \mid g^p$. If π is an irreducible polynomial dividing f then π divides g . Thus we obtain that $\gcd(f, g)$ is a non-trivial divisor in f ($0 < \deg(\gcd(f, g)) < \deg(f)$).

If $g \in \mathbb{F}_p[X]$ is a polynomial such that $0 < \deg(g) < \deg(f)$ and $[g] \in \text{Ker}(F - I)$, where I is the identity map, then $[g]^p = [g]$ in R . We have the crucial factorization

$$g^p - g = g(g - 1) \cdots (g - p + 1),$$

since

$$X^p - X = X(X - 1) \cdots (X - p + 1)$$

in $\mathbb{F}_p[X]$. Let π be an irreducible polynomial dividing f . Since $f \mid g^p - g$ we obtain that π divides one of $g, g - 1, \dots, g - p + 1$. Thus one of $\gcd(f, g), \gcd(f, g - 1), \dots, \gcd(f, g - p + 1)$ is a non-trivial factor of f , since $\deg(g) < \deg(f)$.

Example 4.9.2 The matrix for $F - I$, where F is given in Example 4.9.1, is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

We see that

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

This implies that the polynomial $g = 1 + X + X^3 + X^4$ satisfies $f \mid g^p - g$. By the Euclidean algorithm one obtains (see Example 4.6.2)

$$\gcd(X^5 + X + 1, X^4 + X^3 + X + 1) = X^2 + X + 1.$$

This is a non-trivial factor in $X^5 + X + 1$.

The big surprise is that one needs only to look at the \mathbb{F}_p linear maps F and $F - I$ in order to decide whether f is irreducible. The proof of the following theorem is due to B. Iversen.

Theorem 4.9.3 *Let $f \in \mathbb{F}_p[X]$ be a non-constant polynomial and let F denote the Frobenius map*

$$F : R \rightarrow R,$$

where $R = \mathbb{F}_p[X]/\langle f \rangle$. Then f is irreducible if and only if $\text{Ker}(F) = 0$ and $\text{Ker}(F - I) = \mathbb{F}_p$, where I is the identity map $R \rightarrow R$.

Proof. We have seen that $\text{Ker}(F) = 0$ and $\text{Ker}(F - I) = \mathbb{F}_p$ if f is irreducible (if not, we saw how to find a non-trivial factor in f). Assume now that $\text{Ker}(F) = 0$ and $\text{Ker}(F - I) = \mathbb{F}_p$ and let a be a non-zero element of R . We wish to prove that $1 \in \text{Im}(\varphi)$, where φ is the linear map $\varphi(x) = ax$. This will imply that a is invertible and therefore that R is a field (so that f has to be irreducible). Suppose that $x \in \text{Ker}(\varphi) \cap \text{Im}(\varphi)$. Then $x = ay$ for a suitable $y \in R$ and $ax = 0$. This implies that $F(x) = a^p y^p = a^{p-2} y^{p-1} ax = 0$. Therefore $x \in \text{Ker}(F)$, so that $x = 0$ and $\text{Ker}(\varphi) \cap \text{Im}(\varphi) = 0$. If v_1, \dots, v_r is a basis of $\text{Ker}(\varphi)$ and w_1, \dots, w_s is a basis of $\text{Im}(\varphi)$ then $v_1, \dots, v_r, w_1, \dots, w_s$ is a basis of the subspace $\text{Ker}(\varphi) + \text{Im}(\varphi)$ of R . This implies that $\dim_{\mathbb{F}_p} \text{Ker}(\varphi) + \text{Im}(\varphi) = \dim_{\mathbb{F}_p} \text{Ker}(\varphi) + \dim_{\mathbb{F}_p} \text{Im}(\varphi) = \dim_{\mathbb{F}_p} R$, so that

$$R = \text{Ker}(\varphi) + \text{Im}(\varphi).$$

Notice that if $x \in \text{Ker}(\varphi)$ then $F(x) \in \text{Ker}(\varphi)$ (the same holds for $\text{Im}(\varphi)$). Now write $1 = \alpha + \beta$, where $\alpha \in \text{Ker}(\varphi)$ and $\beta \in \text{Im}(\varphi)$. Then $F(1) = 1 = F(\alpha) + F(\beta)$. This means that $F(\alpha) = \alpha$ and $F(\beta) = \beta$. Since $\text{Ker}(F - I) = \mathbb{F}_p$ we must have $\alpha \in \mathbb{F}_p$. Therefore $\alpha = 0$ and $\beta = 1 \in \text{Im}(\varphi)$. \square

By Theorem 4.9.3 we know that a polynomial is irreducible if and only if the two conditions $\text{Ker}(F) = 0$ and $\text{Ker}(F - I) = \mathbb{F}_p$ are satisfied. If one of these conditions fails then we have seen how to extract a non-trivial factor in f . This procedure is called Berlekamp's algorithm ([3]). For small prime numbers p it is very efficient for finding non-trivial factors.

Remark 4.9.4 If f is divisible by the square π^2 of an irreducible polynomial $\pi \in \mathbb{F}_p[X]$ then one can find a non-trivial factor of f by computing $\gcd(f, D(f))$. This is a consequence of Lemma 4.3.8.

4.10 Exercises

1. Let R be a commutative ring and let $F = F(R, R)$ be the set of functions $f : R \rightarrow R$. Functions in F can be added and multiplied by borrowing the operations from R :

$$(f + g)(x) = f(x) + g(x)$$

$$(fg)(x) = f(x)g(x).$$

- (i) Prove that F is a commutative ring.
- (ii) Let I denote the identity function $I(r) = r$ in F . Prove that the map $\varphi : R[X] \rightarrow F$ given by

$$\varphi(a_n X^n + \cdots + a_1 X + a_0) = a_n I^n + \cdots + a_1 I + a_0$$

is a ring homomorphism.

- (iii) Give an example showing that φ in general is not injective (hint: try $R = \mathbb{F}_2$). Find $\text{Ker}(\varphi)$ when $R = \mathbb{F}_p$.

The fact that φ is not injective means that one cannot in general view polynomials in $R[X]$ as R -valued functions on R .

2. Let $f, g, h \in R[X] = R[\mathbb{N}]$.
 - (i) Prove that $fg = gf$.
 - (ii) Prove that $f(g + h) = fg + fh$.
 - (iii) Prove that $f(gh) = (fg)h$ by reducing to the case $h = cX^m$, where $c \in R$ and $m \in \mathbb{N}$.

3. Let $f, g \in R[X] \setminus \{0\}$ with $f + g \neq 0$. Prove that

$$\deg(f + g) \leq \max(\deg(f), \deg(g)).$$

4. Prove that a monic polynomial $q \in R[X]$ is not a zero divisor. Prove also that $qf = qg$ implies $f = g$, where $f, g \in R[X]$.
5. Prove that $R[X]$ is a domain if R is a domain.
6. Let R be the ring of functions $f : \mathbb{N} \rightarrow \mathbb{Z}/2\mathbb{Z}$. Recall that $(f + g)(n) = f(n) + g(n)$ and $(fg)(n) = f(n)g(n)$, where $f, g \in R$. Prove that the polynomial $X^2 - X \in R[X]$ has infinitely many roots.
7. Show that there are infinitely many irreducible polynomials in $\mathbb{F}_p[X]$, where p is a prime number (hint: look at the proof of Theorem 1.8.2).
8. Let R be a unique factorization domain and K the field of fractions $Q(R)$ of R . Suppose that $\alpha = a/s \in K$ and that a and s have no associated prime divisors. Prove that $s \mid a_n$ and $a \mid a_0$ if α is a root in the polynomial

$$a_n X^n + \cdots + a_1 X + a_0 \in K[X],$$

where $a_n, \dots, a_1, a_0 \in R$. Use this to prove that a real number $\zeta \in \mathbb{R} \setminus \mathbb{Z}$, which is a root in a monic polynomial with integer coefficients, cannot be rational.

9. We let $D : R[X] \rightarrow R[X]$ denote the derivative introduced in subsection 4.3.1.
- (i) Prove that $D(f + g) = D(f) + D(g)$, where $f, g \in R[X]$.
- (ii) Prove that $D(\lambda f) = \lambda D(f)$, where $\lambda \in R$ and $f \in R[X]$.
10. Show that $\Phi_p(X) = X^{p-1} + \cdots + X + 1$, where p is a prime number.
11. Show that $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$, where p is a prime number.
12. Prove that $\Phi_{2n}(X) = \Phi_n(-X)$, if n is odd and > 1 .
13. Let $f = \Phi_8(X) = X^4 + 1$.
- (i) Prove that f is reducible in $\mathbb{F}_p[X]$ for $p \equiv 1 \pmod{4}$.
- (ii) Suppose that $p \equiv 3 \pmod{8}$. Prove that we may find $a \in \mathbb{F}_p$ with $a^2 = -2$. Prove for this a that $f = (X^2 + aX - 1)(X^2 - aX - 1)$ in $\mathbb{F}_p[X]$.
- (iii) Suppose that $p \equiv 7 \pmod{8}$. Prove that we may find $a \in \mathbb{F}_p$ with $a^2 = 2$. Prove for this a that $f = (X^2 + aX + 1)(X^2 - aX + 1)$ in $\mathbb{F}_p[X]$.
- (iv) Conclude that f is reducible in $\mathbb{F}_p[X]$ for every prime number p .
14. Let $n \in \mathbb{N}$ with $n > 1$.
- (i) Prove that the set of n th roots of unity is a subgroup of (\mathbb{C}^*, \cdot) isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

- (ii) Use Lemma 4.4.1 to prove that $\mathbb{Z}/n\mathbb{Z}$ contains $\varphi(n)$ elements of order n .
15. Let $\varphi : R \rightarrow S$ be a ring homomorphism. Prove that $\varphi' : R[X] \rightarrow S[X]$ given by
- $$\varphi'(a_0 + a_1X + \cdots + a_nX^n) = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$$
- is a ring homomorphism.
16. Let R be a domain. Prove that a finite subgroup of R^* is cyclic.
17. Find a generator of the cyclic group \mathbb{F}_{17}^* .
18. Let G be a finite subgroup of \mathbb{C}^* . Prove, without using Theorem 4.5.3, that G is cyclic.
19. Prove that \mathbb{R}^* is not a cyclic group.
20. Prove that a natural number p is a prime number if and only if

$$a^{p-1} \equiv 1 \pmod{p},$$

$$a^{(p-1)/q} \not\equiv 1 \pmod{p} \text{ for every prime } q \mid p-1$$

for some integer a .

21. Let p be a prime number $\neq 2$, $a \in \mathbb{N}$ a primitive root modulo p and $G = (\mathbb{Z}/p^2\mathbb{Z})^*$.
- (i) Prove that $\text{ord}_G([a]) = p-1$ or $p(p-1)$.
 - (ii) Suppose that $a^{p-1} \equiv 1 \pmod{p^2}$. Prove that $r^{p-1} = 1 + tp$, where $r = a + p$ and $p \nmid t$.
 - (iii) Prove that $\text{ord}_G([a + p]) = p(p-1)$ if $\text{ord}_G([a]) = p-1$.
 - (iv) Conclude that $(\mathbb{Z}/p^2\mathbb{Z})^*$ is a cyclic group.
 - (v) Suppose that $a^{p-1} = 1 + tp$, where $p \nmid t$. Prove that

$$a^{p^{m-1}(p-1)} = 1 + t_m p^m$$

where $m > 1$ and $p \nmid t_m$.

- (vi) Prove that $(\mathbb{Z}/p^m\mathbb{Z})^*$ is a cyclic group if $m \geq 1$.
22. Let a be a primitive root modulo the prime number $p > 2$. Show that

$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

23. Let p be a prime number.
- (i) Suppose that s is a non-zero natural number such that $p \mid 10^s - 1$. Prove that the period length of $1/p$ is $\leq s$ (hint: write $1/p = x/10^s + 1/10^s \cdot 1/p$ for a natural number $0 \leq x < 10^s$).
 - (ii) Prove that the period length of $1/p$ is $\leq p-1$.
 - (iii) Prove that the period length of $1/p$ is the order of $[10]$ in \mathbb{F}_p^* .

24. Let p be an odd prime number and let $\alpha = [X] \in R = \mathbb{F}_p[X]/\langle X^4 + 1 \rangle$.
- (i) Prove that α is a primitive eighth root of unity in R .
 - (ii) Let $y = \alpha + \alpha^{-1}$. Prove that $y^2 = 2$ and that $y^p = \alpha^p + \alpha^{-p}$.
 - (iii) Prove that $y^p = y$ if $p \equiv 1, 7 \pmod{8}$ and that $y^p = -y$ if $p \equiv 3, 5 \pmod{8}$.
 - (iv) Use the facts on $y \in R$ developed earlier in this exercise to prove that $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1, 7 \pmod{8}$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3, 5 \pmod{8}$.
25. Compute a greatest common divisor d of $f = X^7 + X^6 + X^2 + X + 1$ and $g = X^7 + X^5 + X^4 + X^2 + 1$ in $\mathbb{F}_2[X]$ along with $\lambda, \mu \in \mathbb{F}_2[X]$ such that $\lambda f + \mu g = d$.
26. Let $R = \mathbb{F}_3[X]$.
- (i) Show that $X^2 + 1$, $X^2 + X + 2$ and $X^2 + 2X + 2$ are the only monic irreducible polynomials of degree 2 in R .
 - (ii) Show that if a polynomial $f \in R$ of degree 4 or 5 with no roots is reducible then there is a monic irreducible polynomial of degree 2 dividing f .
 - (iii) Show that $X^5 - X + 1$ is an irreducible polynomial in R and that $L = R/\langle X^5 - X + 1 \rangle$ is a field with 243 elements. Let $\alpha = [X]$. Find an element $\gamma \in L$ such that $\alpha\gamma = 1$ in L .
27. Show that if a polynomial $f \in \mathbb{C}[X]$ is irreducible then $\deg(f) = 1$.
28. Let $R = \mathbb{F}_2[X]$.
- (i) Show that $X^5 + X + 1$ is not an irreducible polynomial in R .
 - (ii) Show that $X^4 + X + 1$ is an irreducible polynomial in R .
 - (iii) Show that $L = R/\langle X^4 + X + 1 \rangle$ is a field with 16 elements.
 - (iv) Show that L^* is a cyclic group and that $L^* = \langle \alpha \rangle$, where $\alpha = [X]$.
29. Let $L = \mathbb{F}_2[X]/\langle X^3 + X + 1 \rangle$.
- (i) Show that $|L| = 8$.
 - (ii) Write down the seven elements in L^* . Show by explicit computation that their product is -1 .
 - (iii) Let K be a finite field with N elements. Show that the polynomial

$$X^{N-1} - 1 \in K[X]$$

is a product of $N - 1$ polynomials of degree 1 with non-zero constant coefficient.

- (iv) Let π be the product of the elements in K^* . Show that $\pi = -1$.
30. Let $R = \mathbb{F}_2[X]/\langle X^3 + 1 \rangle$ and $\alpha = [X] \in R$.
- (i) Show that $(X^2 + X + 1)(X + 1)$ is an irreducible factorization of $X^3 + 1$ in $\mathbb{F}_2[X]$.
 - (ii) Show that $|R| = 8$ and $(\alpha^2 + \alpha + 1)(\alpha + 1) = 0$.

- (iii) Show that $\alpha^2 + \alpha + 1$, $\alpha + 1$, $\alpha^2 + \alpha$, $\alpha^2 + 1$ cannot be units in R .
 (iv) Show that R^* is cyclic of order 3.
31. Let $R = \mathbb{F}_2[X]$.
 (i) Show that $X^2 + X + 1$ is the only irreducible polynomial of degree 2 in R .
 (ii) Show that $X^3 + X + 1$ and $X^3 + X^2 + 1$ are the only irreducible polynomials of degree 3 in R .
 (iii) Find two distinct irreducible polynomials f and g of degree 6 in R .
 (iv) Use the notation from (iii). Prove that the rings $R/\langle f \rangle$ and $R/\langle g \rangle$ are isomorphic.
32. Let $R = \mathbb{F}_2[X]$.
 (i) Show that $X - 1 \mid X^7 - 1$ and compute the polynomial $f = (X^7 - 1)/(X - 1)$. Prove that $R/\langle f \rangle$ is a ring with 64 elements.
 (ii) List the irreducible polynomials in R of degree 3 and write f as a product of irreducible polynomials.
 (iii) Prove that $R/\langle f \rangle$ is not a field.
33. Construct a field with eight elements.
34. Give an example of an infinite field of characteristic $p > 0$.
35. List the monic irreducible polynomials of degree 3 in $\mathbb{F}_3[X]$.
36. List the monic irreducible polynomials of degree 4 in $\mathbb{F}_2[X]$.
37. Suppose that the ring R contains the field F as a subring. Prove that R is a vector space over F using the multiplication in R (see Appendix B).
38. Let K be a finite field with p^n elements and $L \subseteq K$ a subfield with p^m elements
 (i) Prove that $m \mid n$ (see Exercise 4.37).
 (ii) Suppose that $r \mid s$, where $r, s \in \mathbb{N}$. Prove that

$$X^{p^r} - X \mid X^{p^s} - X$$

in $\mathbb{Z}[X]$.

- (iii) Prove that K contains a subfield with p^m elements if $m \mid n$ by showing explicitly that

$$\{x \in K \mid x^{p^m} = x\}$$

is a subfield of K with p^m elements.

39. Show that there are 440 monic irreducible polynomials of degree 3 in $\mathbb{F}_{11}[X]$.
40. Show that there are 804076 monic irreducible polynomials of degree 6 in $\mathbb{F}_{13}[X]$.

41. Prove Lemma 4.8.10 and apply it to factor $X^5 + X^4 + X^3 + 2X + 2 \in \mathbb{F}_3[X]$.
42. Use Berlekamp's algorithm to find a prime factorization of $f = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Compare with Exercise 4.32.
43. Consider the n th cyclotomic polynomial Φ_n in $\mathbb{F}_p[X]$, where $p \nmid n$. Let π be an irreducible polynomial of degree d in $\mathbb{F}_p[X]$ that divides Φ_n . Put $m = \text{ord}([p])$ in the group $(\mathbb{Z}/n\mathbb{Z})^*$ and let

$$\alpha = [X] \in L = \mathbb{F}_p[X]/\langle \pi \rangle.$$

- (i) Prove that L is a field with p^d elements and that α is a primitive n th root of unity in L . Show that this implies that $p^d \equiv 1 \pmod{n}$.
 - (ii) Prove that $L' = \{\xi \in L \mid \xi^{p^m} = \xi\}$ is a subfield of L . Prove that $\alpha \in L'$ and that $L' = L$. Conclude that $p^d \leq p^m$.
 - (iii) Prove that Φ_n is a product of distinct irreducible polynomials of degree m in $\mathbb{F}_p[X]$.
 - (iv) Prove that Φ_n is irreducible in $\mathbb{F}_p[X]$ if and only if $[p]$ generates $(\mathbb{Z}/n\mathbb{Z})^*$.
44. Let $f, g \in \mathbb{Q}[X] \setminus \{0\}$. Prove that if f is an irreducible polynomial and $f(z) = g(z) = 0$ for some complex number $z \in \mathbb{C}$ then $f \mid g$ in $\mathbb{Q}[X]$.
45. **(HOF)** This exercise is a guided tour of the proof that cyclotomic polynomials are irreducible as polynomials in $\mathbb{Q}[X]$. Needless to say, this result goes back to Gauss. Let $n \geq 1$ and f an irreducible monic polynomial dividing Φ_n in $\mathbb{Q}[X]$.
- (i) Consider f as a polynomial in $\mathbb{C}[X]$. Prove that $f(\zeta) = 0$ for some primitive n th root of unity ζ .
 - (ii) Prove that the fact that every primitive n th root of unity is a root in f if $f(\zeta) = 0$ implies that $f(\zeta^p) = 0$, where ζ is a primitive n th root of unity and p is a prime number not dividing n .
 - (iii) Let f and g be monic polynomials in $\mathbb{Q}[X]$. Prove that $f, g \in \mathbb{Z}[X]$ if $fg \in \mathbb{Z}[X]$.
 - (iv) Prove that $f \mid X^n - 1$ in $\mathbb{Q}[X]$ and write

$$X^n - 1 = f(X)g(X).$$

Prove that $f, g \in \mathbb{Z}[X]$.

- (v) Let ζ be a primitive n th root of unity such that $f(\zeta) = 0$. Suppose that p is a prime number not dividing n and $f(\zeta^p) \neq 0$. Prove that ζ is a root in $g(X^p)$ and that $f(X) \mid g(X^p)$ (see Exercise 4.44). Write $g(X^p) = f(X)h(X)$ for $h(X) \in \mathbb{Q}[X]$. Consider the

corresponding polynomials $\bar{f}, \bar{g}, \bar{h} \in \mathbb{F}_p[X]$. Prove that $\bar{g}(X^p) = \bar{g}(X)^p$ and that an irreducible polynomial $\pi \in \mathbb{F}_p[X]$ dividing \bar{f} must divide \bar{g} .

- (vi) Why is it impossible for $\bar{f}, \bar{g} \in \mathbb{F}_p[X]$ to have a common prime divisor when $p \nmid n$?
- (vii) Prove that $f(\zeta) = 0$ implies that $f(\zeta^p) = 0$, where ζ is a primitive n th root of unity and $p \nmid n$. Show that this implies that f equals Φ_n and therefore that Φ_n is irreducible.