A.2 Polynomial Algebra over Fields

A.2.1 Polynomial rings over fields

We have introduced fields in order to give arithmetic structure to our alphabet F. Our next wish is then to give arithmetic structure to words formed from our alphabet. Additive structure has been provided by considering words as members of the vector space F^n of n-tuples from F for appropriate n. Scalar multiplication in F^n does not however provide a comprehensive multiplication for words and vectors. In order to construct a workable definition of multiplication for words, we introduce polynomials over F.

indeterminate

Let F be a field, and let x be a symbol not one of those of F, an *indeterminate*. To any n-tuple

$$(a_0, a_1, a_2, \ldots, a_{n-1})$$

polynomial

of members of F we associate the *polynomial* in x :

$$a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_{n-1}x^{n-1}.$$

In keeping with common notation we usually write a_0 for a_0x^0 and a_1x for a_1x^1. Also we write $0 \cdot x^i = 0$ and $1 \cdot x^i = x^i$. We sometimes use summation notation for polynomials:

$$\sum_{i=0}^{d} a_i x^i = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_dx^d.$$

$F[x]$

We next define $F[x]$ as the set of all polynomials in x over F:

$$F[x] = \{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in F,\ a_i = 0 \text{ for all but a finite number of } i\}.$$

Polynomials are added in the usual manner:

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i.$$

This addition is compatible with vector addition of n-tuples in the sense that if the vector $\mathbf{a}$ of F^n is associated with the polynomial $a(x)$ and the vector $\mathbf{b}$ is associated with the polynomial $b(x)$, then the vector $\mathbf{a} + \mathbf{b}$ is associated with the polynomial $a(x) + b(x)$.

Polynomial multiplication is also familiar:

$$\sum_{i=0}^{\infty} a_i x^i \cdot \sum_{j=0}^{\infty} b_j x^j = \sum_{k=0}^{\infty} c_k x^k,$$

where the coefficient c_k is given by convolution: $c_k = \sum_{i+j=k} a_i b_j$. This multiplication is the inevitable consequence of the distributive law provided we require

that $ax^i \cdot bx^j = (ab)x^{i+j}$ always. (As usual we shall omit the $\cdot$ in multiplication when convenient.)

The set $F[x]$ equipped with the operations $+$ and $\cdot$ is the *polynomial ring* in x over the field F. F is the field of *coefficients* of $F[x]$.

polynomial ring

coefficients

Polynomial rings over fields have many of the properties enjoyed by fields. $F[x]$ is closed and distributive nearly by definition. Commutativity and additive associativity for $F[x]$ are easy consequences of the same properties for F, and multiplicative associativity is only slightly harder to check. The constant polynomials $0x^0 = 0$ and $1x^0 = 1$ serve respectively as additive and multiplicative identities. The polynomial $ax^0 = a$, for $a \in F$, is usually referred to as a *constant polynomial* or a *scalar polynomial*. Indeed if we define scalar multiplication by $\alpha \in F$ as multiplication by the scalar polynomial $\alpha(= \alpha x^0)$, then $F[x]$ with polynomial addition and this scalar multiplication is a vector space over F, a basis for which is the subset $\{1, x, x^2, x^3, \ldots, x^i, \ldots\}$. (Note that $(-1) \cdot a(x)$ is the additive inverse of the polynomial $a(x)$.)

constant polynomial

scalar polynomial

We therefore see that, as with the integers, the only thing that keeps $F[x]$ from being a field is the lack of multiplicative inverses. Every nonzero scalar polynomial in $F[x]$ has a multiplicative inverse, but as we shall see below no other polynomial of $F[x]$ does. Again like the integers, $F[x]$ does satisfy the cancellation law and so is an integral domain. These last two claims follow from some results of independent interest. To prove them we first need a (once again familiar) definition. The *degree* of the polynomial $a(x)$ of $F[x]$ is the largest power of x occurring in $a(x)$ with a nonzero coefficient. Thus $a(x) = \sum_{i=0}^{d} a_i x^i$ has degree d provided that a_d is not 0. In this case we write $\deg(a(x)) = d$. This defines a degree for all nonzero polynomials. By convention we define the degree of the scalar polynomial 0 to be $-\infty$.

degree

Every polynomial $a(x)$ of degree d not equal to $-\infty$ has a unique scalar multiple whose x^d term has coefficient 1. (Indeed if $a(x) = \sum_{i=0}^{d} a_i x^i$, then the appropriate multiple is $a_d^{-1} a(x)$.) A polynomial whose highest degree term has coefficient 1 is called *monic*.

monic

(A.2.1) PROPOSITION. *Let $a(x)$ and $b(x)$ be polynomials of $F[x]$, for F a field.*

(1) $\deg(a(x)) + \deg(b(x)) = \deg(a(x)b(x))$;

(2) $\deg(a(x) + b(x)) \leq \max\Big(\deg(a(x)), \deg(b(x))\Big)$. □

(A.2.2) PROBLEM. *Prove the proposition.*

(A.2.3) COROLLARY. *Let F be a field.*

(1) *An element of $F[x]$ has a multiplicative inverse if and only if it has degree 0.*

(2) *If $a(x) \cdot b(x) = 0$, then $a(x) = 0$ or $b(x) = 0$.*

(3) *If $a(x)$ is nonzero and $a(x)b(x) = a(x)c(x)$ in $F[x]$, then $b(x) = c(x)$.*

PROOF. (1) We have already mentioned that polynomials of degree 0 (*i.e.*, nonzero scalars) have inverses. Suppose that $b(x)$ is the inverse of the polynomial

$a(x)$. Then $a(x)b(x) = 1$, so examining degrees we have $\deg(a(x)) + \deg(b(x)) = 0$. The two terms on the left must be either $-\infty$ or nonnegative integers. We see that the only possibility is that both are 0, as claimed.

(2) The righthand side has degree $-\infty$, so at least one of the factors on the lefthand side has degree $-\infty$ as well.

(3) Apply (2) to the equation $a(x)(b(x) - c(x)) = 0$. □

(A.2.4) PROBLEM. *Let $a(x), b(x), c(x), d(x)$ be nonzero polynomials in $F[x]$, for F a field. Suppose that $a(x) = b(x)c(x)$ and $b(x) = a(x)d(x)$. Prove that $c(x) = c$ is a constant polynomial and that $d(x) = c^{-1}$ is also constant.*

A.2.2 The division algorithm and roots

In the previous section we noted that, like the integers, polynomial rings over fields are integral domains. Continuing the parallel with the integers, we note that although in general polynomials do not have inverses, we can still perform division with remainder terms.

(A.2.5) THEOREM. *(THE DIVISION ALGORITHM.) Let F be a field, and let $a(x)$ and $b(x)$ be two polynomials of $F[x]$, $b(x)$ not 0. Then there are unique polynomials $q(x)$ and $r(x)$ satisfying*
(1) $a(x) = b(x)q(x) + r(x)$;
(2) $\deg(r(x)) < \deg(b(x))$. □

This is to be compared with the standard result in the integers that for integers a, b with $b \neq 0$ there are unique q and r with $a = bq + r$ and $0 \leq r < b$. The division algorithm is absolutely essential for us, but its proof is largely mechanical, composed of a verification that standard "polynomial long-division" works, as expected. There is a subtlety here, however. In particular, the division algorithm is not valid for polynomials with coefficients from the integers rather than fields. The difficulty is not hard to see. If $a(x) = \sum_{i=0}^{m} a_i x^i$ and $b(x) = \sum_{j=0}^{n} b_j x^j$, where $m = \deg(a(x))$ is larger than $n = \deg(b(x))$, then to carry out the first step of the long-division we must subtract from $a(x)$ the multiple $(a_m/b_n)x^{m-n}b(x)$ of $b(x)$. This requires the ability to divide by b_n in F, and this for arbitrary nonzero b_n in F, if the division algorithm is to be true in general.

Of course, the most important case is when the remainder term $r(x)$ is 0. If, for nonzero polynomials $a(x)$ and $b(x)$ of $F[x]$, there is a polynomial $q(x) \in F[x]$ with $a(x) = b(x)q(x)$, then we say that $b(x)$ is a *factor* of $a(x)$, that $a(x)$ is a *multiple* of $b(x)$, and that $b(x)$ *divides* $a(x)$.

factor
multiple
divides

(A.2.6) PROBLEM. *Prove Theorem A.2.5.*
(HINT: For existence, subtract $(a_m b_n^{-1})x^{m-n}b(x)$ from $a(x)$, then use induction to divide $b(x)$ into the resulting polynomial of smaller degree than $a(x)$. For uniqueness subtract one such answer from the other to get 0, and from this conclude first that the two remainder terms are equal and then that the two dividends are equal. It is important here that $F[x]$ is an integral domain.)

For an α in F and polynomial $p(x) = \sum_i p_i x^i$ in $F[x]$, we write $p(\alpha)$ for $\sum_i p_i \alpha^i$. We call this *evaluation* of $p(x)$ at α, or, more loosely, substituting α for x in $p(x)$.

evaluation

(A.2.7) PROBLEM. *Prove that if $p(x) + q(x) = a(x)$ and $p(x)q(x) = b(x)$ in $F[x]$, then $p(\alpha) + q(\alpha) = a(\alpha)$ and $p(\alpha)q(\alpha) = b(\alpha)$ in F.*

An easy consequence of the division algorithm is

(A.2.8) LEMMA. *For $p(x)$ a polynomial of $F[x]$, F a field, and $\alpha \in F$, $p(x) = (x - \alpha)q(x) + p(\alpha)$.*

PROOF. By the Division Algorithm A.2.5 there are polynomials $q(x)$ and $r(x)$ such that $p(x) = (x-\alpha)q(x) + r(x)$ with $\deg(r(x)) < \deg(x-a) = 1$. The polynomial $r(x)$ must therefore be a constant r. We find the exact value of r by substituting α for x: $p(\alpha) = (\alpha-\alpha)q(\alpha) + r = 0 + r = r$. □

Notice that a particular consequence of Lemma A.2.8 is that $p(\alpha)$ is 0 if and
root only if $x-\alpha$ is a factor of $p(x)$. If this is the case, then we say that α is a *root* of $p(x)$.

(A.2.9) LEMMA. *Let $p(x) = a(x)b(x)$ where $a(x), b(x), p(x)$ are polynomials of $F[x]$ for F a field. If $\alpha \in F$ is a root of $p(x)$, then it is a root of either $a(x)$ or $b(x)$.*

PROOF. $0 = p(\alpha) = a(\alpha)b(\alpha)$. As F is a field, this forces either $a(\alpha) = 0$ or $b(\alpha) = 0$. □

(A.2.10) PROPOSITION. *Let $p(x)$ be a nonzero polynomial in $F[x]$, F a field, of degree d. Then $p(x)$ has at most d distinct roots in F.*

PROOF. The proof proceeds by induction on d. The result is clearly true for $d = 0, 1$. Assume now that $d > 1$ and that the proposition is true for all polynomials of degree less than d. Consider a polynomial $p(x)$ of degree d. If $p(x)$ has no roots in F, then the proposition clearly holds for $p(x)$ (as $0 < d$). Thus we may assume that $p(x)$ has at least one root, α say. Then by Lemma A.2.8 $p(x) = (x-\alpha)q(x)$, for some $q(x)$ of degree $d-1$ (by Proposition A.2.1). By Lemma A.2.9 any root of $p(x)$ other than α must also be a root of $q(x)$. However by induction $q(x)$ has at most $d-1$ roots. Therefore $p(x)$ has at most $1 + (d-1) = d$ roots, as claimed. This completes the induction. □

(A.2.11) THEOREM. *(*LAGRANGE INTERPOLATION.*) Let $f(x)$ be a polynomial of degree d in $F[x]$, F a field. Assume that, for distinct $\alpha_1, \ldots, \alpha_n$ of F with $d < n$, we have $f(\alpha_i) = \beta_i$. Then*

$$f(x) = \sum_{i=1}^{n} \beta_i \left(\prod_{j \neq i} \frac{x - \alpha_j}{\alpha_i - \alpha_j} \right)$$

PROOF. Let $g(x)$ be the righthand side of the equation, a polynomial of degree at most $n-1$ with $g(\alpha_i) = \beta_i$, for $i = 1, \ldots, n$. Therefore $f(x) - g(x)$ has degree at most $n-1$ but has at least n distinct roots $\alpha_1, \ldots, \alpha_n$. Thus $f(x) - g(x)$ is the zero polynomial by Proposition A.2.10. That is, $f(x) = g(x)$. □

(A.2.12) PROBLEM. *Let $a_0, \ldots, a_m, b_0, ..., b_m$ be elements of the field F with the a_i nonzero. Then the columns of the matrix*

$$P = \begin{bmatrix} a_0 b_0^0 & a_1 b_1^0 & \cdots & a_m b_m^0 \\ a_0 b_0^1 & a_1 b_1^1 & \cdots & a_m b_m^1 \\ \vdots & \vdots & \ddots & \vdots \\ a_0 b_0^m & a_1 b_1^m & \cdots & a_m b_m^m \end{bmatrix}$$

*are linearly independent over F if and only if the b_j are distinct. (*HINT: *By Proposition A.1.12 the columns of square P are linearly independent if and only if its rows are linearly independent. Prove that a linear dependence of the rows of P corresponds to a polynomial that has each b_j as a root.)*

REMARK. If in P we choose $a_i = 1$, for all i, the result is the usual matrix of Vandermonde type. Then Problem A.2.12 asserts the well-known fact that the determinant of a Vandermonde matrix is nonzero. The matrix P can also be viewed as a generalization of the usual discrete Fourier transform matrix.

A.2.3 Modular polynomial arithmetic

Starting with the infinite integral domain $\mathbb{Z}$ we found finite rings by doing arithmetic modulo specific fixed integers. This gave us finite alphabets with good arithmetic structure. We would now like to extend this by giving structure to strings of alphabet members. This is achieved by doing arithmetic in the integral domain $F[x]$, F a field, modulo a specific fixed polynomial.

Let d be any positive integer. For any field F, let $F[x]_d$ be the set of all polynomials of $F[x]$ of degree less than d, that is,

$$F[x]_d = \{f_0 + f_1 x + f_2 x^2 + \cdots + f_{d-1}x^{d-1} \mid f_0, f_1, f_2, \ldots, f_{d-1} \in F\}.$$

Then with the usual scalar multiplication and polynomial addition $F[x]_d$ is a vector space over F of dimension d. Can we define a multiplication on $F[x]_d$ to make it into a ring? Using the division algorithm we can (in fact in several different ways).

Let $m(x)$ be a fixed polynomial of $F[x]$ of degree d. By the Division Algorithm A.2.5, for any polynomial $p(x)$ there is a unique polynomial $r(x)$ determined by:

(i) $\deg(r(x)) < d$;

(ii) $p(x) - r(x)$ is a multiple of $m(x)$ in $F[x]$.

Now we may define a multiplication on $F[x]_d$. For $a(x), b(x)$ in $F[x]_d$ we define multiplication modulo $m(x)$ by

$$a(x) \cdot b(x) = r(x) \pmod{m(x)}$$

where $r(x)$ is the remainder of $a(x)b(x)$ upon division by $m(x)$. We write $F[x] \pmod{m(x)}$ for the set $F[x]_d$ equipped with the operations of usual polynomial addition and multiplication modulo the polynomial $m(x)$ of degree d. It is now routine to check that these operations satisfy the first six axioms of Section A.1.1, giving:

$F[x] \pmod{m(x)}$

(A.2.13) Lemma. *For any nonconstant polynomial $m(x)$, $F[x] \pmod{m(x)}$ is a commutative ring.* □

It should be noted that Lemma A.2.13 is not a purely trivial observation, but its subtlety is largely embedded in the original definition. The least obvious fact is that we are able to define multiplication consistently. The division algorithm is required to do that. Checking multiplicative associativity and distributivity also requires some care.

For the integers we found that modular arithmetic produced a field (indeed an integral domain) precisely when the modulus was a prime. What is the counterpart to a prime for polynomial rings? A polynomial $m(x) \in F[x]$ of degree d (> 0) is a *prime polynomial* if whenever $m(x)$ divides the product $a(x)b(x)$ of the two polynomials $a(x)$ and $b(x)$, then in fact it divides at least one of $a(x)$ and $b(x)$.

prime polynomial

The following theorem is the counterpart for polynomial rings over fields of the earlier result Theorem A.1.1 for the integers.

(A.2.14) THEOREM. *Let F be a finite field and $m(x)$ a nonconstant polynomial of $F[x]$. The following are equivalent:*

(1) *$m(x)$ is prime;*

(2) *$F[x] \pmod{m(x)}$ is an integral domain;*

(3) *$F[x] \pmod{m(x)}$ is a field.*

PROOF. *(3) implies (2)* by the definitions, and *(2) implies (3)* by Exercise A.1.2, since the integral domain under discussion is finite with $|F|^{\deg(m(x))}$ elements.

(2) implies (1): If $m(x)$ divides the product $a(x)b(x)$, then it must also divide the product $a_1(x)b_1(x)$, where $a_1(x)$ is the remainder of $a(x)$ upon division by $m(x)$ and $b_1(x)$ is the remainder of $b(x)$ upon division by $m(x)$. Here both $a_1(x)$ and $b_1(x)$ have smaller degree than $m(x)$. But then we have $a_1(x) \cdot b_1(x) = 0 \pmod{m(x)}$, so either $a_1(x) = 0 \pmod{m(x)}$ or $b_1(x) = 0 \pmod{m(x)}$ in the integral domain $F[x] \pmod{m(x)}$. One of the remainders is 0, and $m(x)$ divides $a(x)$ or $b(x)$.

(1) implies (2): Let $g(x)$ and $h(x)$ be members of $F[x] \pmod{m(x)}$, that is, polynomials of degree less than that of the prime polynomial $m(x)$. If $g(x)h(x) = 0 \pmod{m(x)}$, then the product $g(x)h(x)$ is a multiple of $m(x)$. Since $m(x)$ is prime, either $g(x)$ or $h(x)$ is a multiple of $m(x)$. That is, $g(x) = 0 \pmod{m(x)}$ or $h(x) = 0 \pmod{m(x)}$.

The theorem is in fact true without the assumption that $|F|$ is finite, a fact used here only in the proof that (2) implies (3). A strengthened version of the theorem will appear later as Theorem A.2.22.

Related to the modular arithmetic statement

$$p(x) = q(x) \pmod{m(x)} \quad \text{in} \quad F[x] \pmod{m(x)}$$

is the *modular congruence* statement

modular congruence

$$p(x) \equiv q(x) \pmod{m(x)} \quad \text{in} \quad F[x]\,,$$

which, by definition, says that

$$p(x) - q(x) = f(x)m(x)\,,$$

for some polynomial $f(x) \in F[x]$. That is, $p(x)$ and $q(x)$ are congruent modulo $m(x)$ precisely when their difference is a multiple of $m(x)$. Equivalently, $p(x)$ and $q(x)$ have the same remainder upon division by $m(x)$.

We are familiar with congruence statements over the integers, where, for instance, the even integers are precisely those integers congruent to 0 modulo 2 and the odd integers consist of those integers congruent to 1 modulo 2. Arithmetic in the integers modulo 2, $\mathbb{Z}_2$, can be interpreted as making statements about the relationship between the set of even integers (represented by 0) and the set of odd integers (represented by 1). For instance, we have

"The sum of an odd integer and an even integer is odd."

"The product of two odd integers is odd."

Similar statements hold for arithmetic done modulo any integer:

> "The product of two numbers each 2 more than a multiple of 3
> is a number that is 1 more than a multiple of 3."

That is, the product of two numbers, each congruent to 2 modulo 3 is a number congruent to 1 modulo 3.

Polynomial modular arithmetic has a similar relationship to polynomial modular congruences, as the following problem demonstrates.

(A.2.15) PROBLEM.
Prove that, if $a_1(x) \equiv a(x) \pmod{m(x)}$ *and* $b_1(x) \equiv b(x) \pmod{m(x)}$, *then*
(*a*) $a_1(x) + b_1(x) \equiv a(x) + b(x) \pmod{m(x)}$; *and*
(*b*) $a_1(x)b_1(x) \equiv a(x)b(x) \pmod{m(x)}$.

We see that the statement

$$a(x) + b(x) = c(x) \pmod{m(x)}$$

is a special case of

$$a(x) + b(x) \equiv c(x) \pmod{m(x)}\,;$$

and, similarly,

$$a(x)b(x) = c(x) \pmod{m(x)}$$

is a special case of

$$a(x)b(x) \equiv c(x) \pmod{m(x)}\,.$$

With this in mind, we will usually use the symbol $=$ in place of $\equiv$, abusing our notation by writing

$$a(x)b(x) = c(x) \pmod{m(x)}$$

even when the polynomials $a(x)$, $b(x)$, and $c(x)$ have degree larger than that of $m(x)$.

A.2.4 Greatest common divisors and unique factorization

We introduce the important concept of the greatest common divisor of a pair (or set) of polynomials.

(A.2.16) THEOREM. *In $F[x]$, F a field, let $a(x)$ and $b(x)$ be two polynomials not both equal to 0. Then there is a unique monic polynomial $g(x)$ in $F[x]$ such that:*

(i) $a(x)$ and $b(x)$ are multiples of $g(x)$;

(ii) if $n(x)$ divides both $a(x)$ and $b(x)$ then $g(x)$ is a multiple of $n(x)$.

Indeed $g(x)$ is the unique monic polynomial of minimal degree in the set

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

PROOF. Choose in the set G a monic polynomial $g(x) = s(x)a(x) + t(x)b(x)$ of smallest degree. This determines $g(x)$ uniquely, since if $g^*(x) = s^*(x)a(x) + t^*(x)b(x)$ were a different monic polynomial in G of the same degree as $g(x)$, then

$$g(x) - g^*(x) = \big(s(x) - s^*(x)\big)a(x) + \big(t(x) - t^*(x)\big)b(x)$$

would have a monic multiple of smaller degree that still belonged to G.

If $n(x)$ divides $a(x)$ and $b(x)$, then it certainly divides $g(x) = s(x)a(x) + t(x)b(x)$, giving (ii).

It remains to check (i). By the Division Algorithm A.2.5 there are polynomials $q(x)$ and $r(x)$ with $a(x) = q(x)g(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$. Here

$$\begin{aligned} r(x) &= a(x) - q(x)g(x) \\ &= 1 \cdot a(x) - q(x)(s(x)a(x) + t(x)b(x)) \\ &= \big(1 - q(x)s(x)\big)\, a(x) + \big(-q(x)t(x)\big)\, b(x)\,. \end{aligned}$$

Therefore $r(x)$ is a member of G with smaller degree than that of $g(x)$. Our choice of $g(x)$ now forces $r(x) = 0$. Thus $a(x) = q(x)g(x)$ is a multiple of $g(x)$, as desired. Similarly, $b(x)$ is a multiple of $g(x)$, giving (i). □

The polynomial $g(x)$ of Theorem A.2.16 is called the *greatest common divisor* of $a(x)$ and $b(x)$. In this case we often write $g(x) = \gcd(a(x), b(x))$. Notice that, for nonzero $a(x)$, $\gcd(a(x), 0)$ is the unique monic scalar multiple of $a(x)$. If $a(x) = b(x) = 0$, then $g(x) = 0$ satisfies (1) and (2) trivially, so we set $\gcd(0, 0) = 0$ (even though it is not monic).

greatest common divisor

If $\gcd(a(x), b(x)) = 1$, we say that $a(x)$ and $b(x)$ are *relatively prime*. We have immediately

relatively prime

(A.2.17) COROLLARY. *The polynomials $a(x), b(x) \in F[x]$ are relatively prime if and only if there are $s(x), t(x) \in F[x]$ with $s(x)a(x) + t(x)b(x) = 1$.* □

The corollary implies that

$$s(x)a(x) = 1 \pmod{b(x)}\,,$$

that is, $s(x)$ is the multiplicative inverse of $a(x)$ modulo $b(x)$; and we sometimes then even write

$$s(x) = a(x)^{-1} = \frac{1}{a(x)} \pmod{b(x)}\,.$$

To repeat, if $a(x)$ and $b(x)$ are relatively prime, then we can invert $a(x)$ modulo $b(x)$. Indeed $a(x)$ is invertible modulo $b(x)$ if and only if $a(x)$ and $b(x)$ are relatively prime.

An argument similar to that of Theorem A.2.16 gives the more general and fundamental result

(A.2.18) THEOREM. *Let F be a field and*

$$S = \{f_i(x) \,|\, i \in I\}$$

a (possibly infinite) set of polynomials in $F[x]$, not all equal to 0. Consider the set

$$G = \left\{ \sum_{i \in I} a_i f_i(x) \,|\, a_i \in F \right\}$$

Here, when the index set I is infinite, it should be understood that all but a finite number of the a_i must be 0 in any particular sum. Then

(1) *G contains a unique monic polynomial $g(x)$ of minimal degree;*

(2) *$g(x)$ has the two properties:*

(i) every member of S is a multiple of $g(x)$;

(ii) if $n(x)$ divides every member of S then $g(x)$ is a multiple of $n(x)$. □

greatest common divisor

The polynomial $g(x)$ of Theorem A.2.18 is called the *greatest common divisor* of the set of polynomials S, and we write $g(x) = \gcd(S)$. By convention, the gcd of any empty set of polynomials is 1, and again $\gcd(\{0\}) = 0$.

(A.2.19) PROBLEM. *Let F be a field and*

$$S = \{f_1(x), \ldots, f_i(x), \ldots, f_m(x)\}$$

a finite set of polynomials in $F[x]$, not all equal to 0.

Set

$$L = \{f(x) \,|\, f(x) \text{ is a multiple of } f_i(x), \text{ for } i = 1, \ldots, m\}\,,$$

and let $l(x)$ be the greatest common divisor of the set L. Prove that $l(x)$ has the two properties:

(i) $l(x)$ is a multiple of $f_i(x)$ for $i = 1, \ldots, n$;

(ii) if $n(x)$ is a multiple of $f_i(x)$ for $i = 1, \ldots, n$, then $n(x)$ is a multiple of $l(x)$.

least common multiple

This polynomial $l(x)$ is called the least common multiple *of S, written* $\operatorname{lcm}(S)$.

(A.2.20) LEMMA. *Let F be a field, and let $p(x), q(x), m(x) \in F[x]$. Suppose $m(x)$ divides the product $p(x)q(x)$ but $m(x)$ and $p(x)$ are relatively prime, $\gcd(m(x), p(x)) = 1$. Then $m(x)$ divides $q(x)$.*

PROOF. By Corollary A.2.17 there are polynomials $s(x)$ and $t(x)$ such that $1 = s(x)m(x) + t(x)p(x)$. Therefore

$$\begin{aligned} q(x) &= 1 \cdot q(x) \\ &= \Big(s(x)m(x) + t(x)p(x)\Big)q(x) \\ &= \Big(s(x)q(x)\Big)m(x) + t(x)\Big(p(x)q(x)\Big). \end{aligned}$$

Here $m(x)$ divides both terms of the righthand side, so $m(x)$ divides $q(x)$. □

Let $m(x)$ be a polynomial in $F[x]$ of degree $d > 0$. Then $m(x)$ is *reducible* in $F[x]$ if there are polynomials $a(x) \in F[x]$ with $0 < \deg(a(x)) < d$ and $b(x) \in F[x]$ with $0 < \deg(b(x)) < d$ such that $m(x) = a(x)b(x)$. That is, $m(x)$ is reducible if it can be written as a product of polynomials of smaller degree. Otherwise $m(x)$ is *irreducible*. (Constant polynomials are neither reducible nor irreducible.) If irreducible $m(x) = a(x)b(x)$, then one of the factors is a nonzero constant, say $a(x) = a$, and the other factor $b(x) = a^{-1}m(x)$ has the same degree as $m(x)$.

reducible

irreducible

Recall that in Section A.2.3 we defined $m(x)$ to be prime if whenever $m(x)$ divides the product $a(x)b(x)$, it must in fact divide one of $a(x)$ and $b(x)$. If prime $m(x) = a(x)b(x)$, then $m(x)$ must divide either $a(x)$ or $b(x)$; so they can not both have degree less than that of $m(x)$. Thus every prime is irreducible. We use Lemma A.2.20 to prove the converse.

(A.2.21) LEMMA. *In $F[x]$ with F a field, every irreducible polynomial is prime.*

PROOF. Suppose irreducible $m(x)$ divides the product $a(x)b(x)$. If we have $\gcd(m(x), a(x)) = 1$, then by Lemma A.2.20 the polynomial $b(x)$ is divisible by $m(x)$, as required. So we may assume that $m(x)$ and $a(x)$ are not relatively prime. As $m(x)$ is irreducible, its divisor $\gcd(m(x), a(x)) \neq 1$ must therefore be $c \cdot m(x)$, for some constant c. In particular, $m(x) = c^{-1}\gcd(m(x), a(x))$ divides $a(x)$. □

We are now in a position to give the strengthened version of Theorem A.2.14.

(A.2.22) THEOREM. *Let F be a field and $m(x)$ a nonconstant polynomial of $F[x]$. The following are equivalent:*

(1) *$m(x)$ is irreducible;*

(2) *$F[x]$ (mod $m(x)$) is an integral domain;*

(3) *$F[x]$ (mod $m(x)$) is a field.*

PROOF. By Lemma A.2.21 the present (1) is equivalent to that of Theorem A.2.14.

In Theorem A.2.14 we assumed that the field F was finite; but, as noted there, the assumption was only used in the proof that (2) implies (3). In particular from Theorem A.2.14 we know that (3) implies (2) and (2) implies (1).

We now prove that (1) implies (3), giving the theorem. Let $f(x) \in F[x]$ of degree less than that of $m(x)$. This implies that $f(x)$ and irreducible $m(x)$ are relatively prime. There exist polynomials $s(x)$ and $t(x)$ with $f(x)s(x) + m(x)t(x) = 1$. Therefore $f(x)s(x) = 1 \pmod{m(x)}$. If $g(x)$ is the remainder of $s(x)$ upon division by $m(x)$, then again $f(x)g(x) = 1$ in $F[x] \pmod{m(x)}$. That is, $f(x)$ is invertible in $F[x] \pmod{m(x)}$, as required for (3). □

In the integers, we have unique factorization into primes. To be precise, every nonzero integer is plus or minus a product of positive prime numbers, this factorization being unique up to the order in which the primes appear. Essentially the same result is true for polynomial rings over fields.

(A.2.23) THEOREM. (UNIQUE FACTORIZATION OF POLYNOMIALS.) *Let F be a field, and $f(x)$ a nonzero member of $F[x]$. Then $f(x)$ can be written as a product $f(x) = c\prod_{i=1}^{n} f_i(x)$ of a nonzero constant c and a collection of monic irreducible polynomials $f_i(x)$. This factorization is unique up to the order in which the irreducibles $f_i(x)$ are taken.* □

We sketch a proof with the details left to Problem A.2.24. The existence of factorizations into irreducibles is easy to see, as is the uniqueness of factorization into primes. Since, by Lemma A.2.21, in this situation all irreducibles are primes, the result follows.

(A.2.24) PROBLEM. *Prove Theorem A.2.23.*

*(*HINT: *Deal first with existence. Every nonzero polynomial $f(x)$ is a product $cg(x)$ with c a nonzero constant and $g(x)$ monic, so assume that $f(x)$ is monic. If $f(x)$ is not irreducible, then it can be factored as a product $g_1(x)g_2(x)$ of two monic polynomials of smaller degree. Either they are irreducible or they can be split further as products. Proceed in this fashion; use induction. As the degrees decrease at each stage, this process must stop with $f(x)$ written as a product of irreducible polynomials.*

Now consider uniqueness. Let $f(x) = d\prod_{j=1}^{m} g_j(x)$ be a second factorization into monic irreducibles. Then $c = d$ is the coefficient of the highest degree term. The monic irreducible $f_1(x)$ divides the product $g_1(x)(\prod_{j=2}^{m} g_j(x))$. By Lemma A.2.21 irreducibles are prime, so either $f_1(x) = g_1(x)$ or $f_1(x)$ divides $\prod_{j=2}^{m} g_j(x)$. In the second case $f_1(x)$ divides $\prod_{j=2}^{m} g_j(x) = g_2(x)(\prod_{j=3}^{m} g_j(x))$; so as before either $f_1(x)$ equals $g_2(x)$ or it divides $\prod_{j=3}^{m} g_j(x)$. Proceeding in this fashion, $f_1(x)$ is equal to one of the irreducible monic factors $g_j(x)$; use induction again. A similar argument shows that $f_2(x)$ is also equal to one of the $g_j(x)$, and indeed that each $f_i(x)$ is equal to one of the $g_j(x)$. Compare degrees to conclude finally that $n = m$.)

(A.2.25) PROBLEM. *Let*

$$S = \{f_1(x), ..., f_i(x), ..., f_m(x)\}$$

be a finite set of polynomials, as in Problem A.2.19 above. Suppose there are constants c_i, distinct monic irreducible polynomials $p_j(x)$, and nonnegative integers $e_{i,j}$, $1 \leq j \leq n$, such that, for each i,

$$f_i(x) = c_i \prod_{j=1}^{n} p_j(x)^{e_{i,j}} \ .$$

For each j, let $d_j = \max_i(e_{i,j})$. Prove that $\mathrm{lcm}(S) = \prod_{j=1}^{n} p_j(x)^{d_j}$.

(A.2.26) PROBLEM. *For the polynomial* $p(x) = \sum_{i=0}^{k} p_i x^i \in F[x]$*, define the* formal derivative *of* $p(x)$*, denoted* $p'(x)$*, by* $p'(x) = \sum_{i=1}^{k} i p_i x^{i-1}$*. Prove the usual product rule for derivatives:* $(a(x)b(x))' = a(x)b'(x) + a'(x)b(x)$. formal derivative

(A.2.27) PROBLEM. *Consider the polynomial ring* $F[x]$*,* F *a field; and let* $\alpha \in F$ *be a root of* $p(x) \in F[x]$*. Prove that* $(x-\alpha)^2$ *divides* $p(x)$ *if and only if* $x - \alpha$ *divides the formal derivative* $p'(x)$*.*

(A.2.28) PROBLEM. *A polynomial* $f(x)$ *is* square free *in* $F[x]$ *if there are no nonconstant polynomials* $g(x) \in F[x]$ *for which* $g(x)^2$ *divides* $f(x)$*. Prove that in* $F[x]$*, the polynomial* $f(x)$ *is square free if and only if we have* $\gcd(f(x), f'(x)) = 1$. square free

In particular, over $\mathbb{F}_2$ *all derivatives are squares.*