SECTION 28 FACTORIZATION OF POLYNOMIALS OVER A FIELD

Recall that we are concerned with finding zeros of polynomials. Let E and F be fields, with $F \leq E$. Suppose that $f(x) \in F[x]$ factors in $F[x]$, so that $f(x) = g(x)h(x)$ for $g(x), h(x) \in F[x]$ and let $\alpha \in E$. Now for the evaluation homomorphism ϕ_α, we have

$$f(\alpha) = \phi_\alpha(f(x)) = \phi_\alpha(g(x)h(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha).$$

Thus if $\alpha \in E$, then $f(\alpha) = 0$ if and only if either $g(\alpha) = 0$ or $h(\alpha) = 0$. The attempt to find a zero of $f(x)$ is reduced to the problem of finding a zero of a factor of $f(x)$. This is one reason why it is useful to study factorization of polynomials.

The Division Algorithm in $F[x]$

The following theorem is the basic tool for our work in this section. Note the similarity with the division algorithm for $\mathbb{Z}$ given in Theorem 6.2, the importance of which has been amply demonstrated.

We prove the following lemma, which is used in our proof of the division algorithm.

28.1 Lemma Let F be a field and $f(x), g(x), s(x) \in F[x]$ with $g(x) \neq 0$. If

$$\deg(f(x) - g(x)s(x)) \geq \deg(g(x)),$$

then there is a polynomial $s_1(x) \in F[x]$ such that either

$$\deg(f(x) - g(x)s_1(x)) < \deg(f(x) - g(x)s(x))$$

or

$$f(x) - g(x)s_1(x) = 0.$$

Proof Let $n = \deg(f(x) - g(x)s(x))$. We can write $(f(x) - g(x)s(x)) = a_nx^n + r(x)$ where $a_n \neq 0$ and either $r(x) = 0$ or $\deg(r(x)) < n$. Similarly, since $g(x) \neq 0$, we can write $g(x) = b_kx^k + g_1(x)$ where $b_k \neq 0$ and either $g_1(x) = 0$ or $\deg(g_1(x)) < k$.

We let $s_1(x) = s(x) + \frac{a_n}{b_k}x^{n-k}$. Then

$$\begin{aligned} f(x) - g(x)s_1(x) &= f(x) - g(x)s(x) - g(x)\frac{a_n}{b_k}x^{n-k} \\ &= a_nx^n + r(x) - b_kx^k\frac{a_n}{b_k}x^{n-k} - g_1(x)\frac{a_n}{b_k}x^{n-k} \\ &= r(x) - g_1(x)\frac{a_n}{b_k}x^{n-k}. \end{aligned}$$

Each polynomial $r(x)$ and $g_1(x)\frac{a_n}{b_k}x^{n-k}$ is either 0 or has degree less than n. Thus $r(x) - g_1(x)\frac{a_n}{b_k}x^{n-k} = 0$ or $\deg(r(x) - g_1(x)\frac{a_n}{b_k}x^{n-k}) < n = \deg(f(x) - g(x)s(x))$, which completes the proof. ◆

28.2 Theorem **(Division Algorithm for $F[x]$)** Let

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and

$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0$$

be two elements of $F[x]$, with a_n and b_m both nonzero elements of F and $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Proof Consider the set $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$. If $0 \in S$ then there exists an $s(x)$ such that $f(x) - g(x)s(x) = 0$, so $f(x) = g(x)s(x)$. Taking $q(x) = s(x)$ and $r(x) = 0$, we are done. Otherwise, let $r(x)$ be an element of minimal degree in S. Then

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

for some $q(x) \in F[x]$. By Lemma 28.1, the degree of $r(x)$ is less than the degree of $g(x)$ since if the degree of $r(x)$ were at least as large as the degree of $g(x)$, then $r(x)$ would not have minimal degree in S.

For uniqueness, if

$$f(x) = g(x)q_1(x) + r_1(x)$$

and

$$f(x) = g(x)q_2(x) + r_2(x),$$

then subtracting we have

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$

Because either $r_2(x) - r_1(x) = 0$ or the degree of $r_2(x) - r_1(x)$ is less than the degree of $g(x)$, this can hold only if $q_1(x) - q_2(x) = 0$ so $q_1(x) = q_2(x)$. Then we must also have $r_2(x) - r_1(x) = 0$ so $r_1(x) = r_2(x)$. ◆

We can compute the polynomials $q(x)$ and $r(x)$ of Theorem 28.2 by long division just as we divided polynomials in $\mathbb{R}[x]$ in high school.

28.3 Example Let us work with polynomials in $\mathbb{Z}_5[x]$ and divide

$$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$$

by $g(x) = x^2 - 2x + 3$ to find $q(x)$ and $r(x)$ of Theorem 28.2. The long division should be easy to follow, but remember that we are in $\mathbb{Z}_5[x]$, so, for example, $4x - (-3x) = 2x$.

$$
\begin{array}{r|rrrrr}
 & & & x^2 & -\,x & -\,3 \\ \cline{2-6}
x^2 - 2x + 3 & x^4 & -\,3x^3 & +\,2x^2 & +\,4x & -\,1 \\
 & x^4 & -\,2x^3 & +\,3x^2 & & \\ \cline{2-4}
 & & -\,x^3 & -\,x^2 & +\,4x & \\
 & & -\,x^3 & +\,2x^2 & -\,3x & \\ \cline{3-5}
 & & & -\,3x^2 & +\,2x & -\,1 \\
 & & & -\,3x^2 & +\,x & -\,4 \\ \cline{4-6}
 & & & & x & +\,3
\end{array}
$$

Thus

$$q(x) = x^2 - x - 3, \quad \text{and} \quad r(x) = x + 3.$$ ▲

We give three important corollaries of Theorem 28.2. The first one appears in high school algebra for the special case $F[x] = \mathbb{R}[x]$. We phrase our proof in terms of the mapping (homomorphism) approach described in Section 27.

28.4 Corollary **(Factor Theorem)** An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.

Proof Suppose that for $a \in F$ we have $f(a) = 0$. By Theorem 28.2, there exist $q(x)$, $r(x) \in F[x]$ such that

$$f(x) = (x - a)q(x) + r(x),$$

where either $r(x) = 0$ or the degree of $r(x)$ is less than 1. Thus we must have $r(x) = c$ for $c \in F$, so

$$f(x) = (x - a)q(x) + c.$$

Applying our evaluation homomorphism, $\phi_a : F[x] \to F$ of Theorem 27.4, we find

$$0 = f(a) = 0q(a) + c,$$

so it must be that $c = 0$. Then $f(x) = (x - a)q(x)$, so $x - a$ is a factor of $f(x)$.

Conversely, if $x - a$ is a factor of $f(x)$ in $F[x]$, where $a \in F$, then applying our evaluation homomorphism ϕ_a to $f(x) = (x - a)q(x)$, we have $f(a) = 0q(a) = 0$. ◆

28.5 Example Working again in $\mathbb{Z}_5[x]$, note that 1 is a zero of

$$(x^4 + 3x^3 + 2x + 4) \in \mathbb{Z}_5[x].$$

Thus by Corollary 28.4, we should be able to factor $x^4 + 3x^3 + 2x + 4$ into $(x - 1)q(x)$ in $\mathbb{Z}_5[x]$. Let us find the factorization by long division.

$$
\begin{array}{r|l}
 & x^3 + 4x^2 + 4x + 1 \\ \hline
x - 1 & x^4 + 3x^3 + \qquad\quad 2x + 4 \\
 & \underline{x^4 - x^3} \\
 & \qquad 4x^3 \\
 & \qquad \underline{4x^3 - 4x^2} \\
 & \qquad\qquad 4x^2 + 2x \\
 & \qquad\qquad \underline{4x^2 - 4x} \\
 & \qquad\qquad\qquad x + 4 \\
 & \qquad\qquad\qquad \underline{x - 1} \\
 & \qquad\qquad\qquad\quad\;\; 0
\end{array}
$$

Thus $x^4 + 3x^3 + 2x + 4 = (x - 1)(x^3 + 4x^2 + 4x + 1)$ in $\mathbb{Z}_5[x]$. Since 1 is seen to be a zero of $x^3 + 4x^2 + 4x + 1$ also, we can divide this polynomial by $x - 1$ and get

$$
\begin{array}{r|l}
 & x^2 + 4 \\ \hline
x - 1 & x^3 + 4x^2 + 4x + 1 \\
 & \underline{x^3 - x^2} \\
 & \qquad 0 \;\; + 4x + 1 \\
 & \qquad\qquad \underline{4x - 4} \\
 & \qquad\qquad\qquad 0
\end{array}
$$

Since $x^2 + 4$ still has 1 as a zero, we can divide again by $x - 1$ and get

$$
\begin{array}{r|l}
 & x + 1 \\ \hline
x - 1 & x^2 \qquad + 4 \\
 & \underline{x^2 - x} \\
 & \qquad x + 4 \\
 & \qquad \underline{x - 1} \\
 & \qquad\quad\; 0
\end{array}
$$

Thus $x^4 + 3x^3 + 2x + 4 = (x - 1)^3(x + 1)$ in $\mathbb{Z}_5[x]$. ▲

The next corollary should also look familiar.

28.6 Corollary A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

Proof The preceding corollary shows that if $a_1 \in F$ is a zero of $f(x)$, then

$$f(x) = (x - a_1)q_1(x),$$

where, of course, the degree of $q_1(x)$ is $n - 1$. A zero $a_2 \in F$ of $q_1(x)$ then results in a factorization

$$f(x) = (x - a_1)(x - a_2)q_2(x).$$

Continuing this process, we arrive at

$$f(x) = (x - a_1) \cdots (x - a_r)q_r(x),$$

where $q_r(x)$ has no further zeros in F. Since the degree of $f(x)$ is n, at most n factors $(x - a_i)$ can appear on the right-hand side of the preceding equation, so $r \leq n$. Also, if $b \neq a_i$ for $i = 1, \cdots, r$ and $b \in F$, then

$$f(b) = (b - a_1) \cdots (b - a_r)q_r(b) \neq 0,$$

since F has no divisors of 0 and none of $b - a_i$ or $q_r(b)$ are 0 by construction. Hence the a_i for $i = 1, \cdots, r \leq n$ are all the zeros in F of $f(x)$. ◆

Our final corollary is concerned with the structure of the multiplicative group F^* of nonzero elements of a field F, rather than with factorization in $F[x]$. It may at first seem surprising that such a result follows from the division algorithm in $F[x]$, but recall that the result that a subgroup of a cyclic group is cyclic follows from the division algorithm in $\mathbb{Z}$.

28.7 Corollary If G is a finite subgroup of the multiplicative group $\langle F^*, \cdot \rangle$ of a field F, then G is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof By Theorem 9.12 as a finite abelian group, G is isomorphic to a direct product $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$, where each d_i is a power of a prime. Let us think of each of the $\mathbb{Z}_{d_i}$ as a cyclic group of order d_i in *multiplicative* notation. Let m be the least common multiple of all the d_i for $i = 1, 2, \cdots, r$; note that $m \leq d_1 d_2 \cdots d_r$. If $a_i \in \mathbb{Z}_{d_i}$, then $a_i^{d_i} = 1$, so $a_i^m = 1$ since d_i divides m. Thus for all $\alpha \in G$, we have $\alpha^m = 1$, so every element of G is zero of $x^m - 1$. But G has $d_1 d_2 \cdots d_r$ elements, while $x^m - 1$ can have at most m zeros in the field F by Corollary 28.6, so $m \geq d_1 d_2 \cdots d_r$. Hence $m = d_1 d_2 \cdots d_r$, so the primes involved in the prime powers $d_1, d_2, \cdots, d_r$ are distinct, and the group G is isomorphic to the cyclic group $\mathbb{Z}_m$. ◆

Exercises 5 through 8 ask us to find all generators of the cyclic groups of units for some finite fields. The fact that the multiplicative group of units of a finite field is cyclic has been applied in algebraic coding and combinatorial designs.

Irreducible Polynomials

Our next definition singles out a type of polynomial in $F[x]$ that will be of utmost importance to us. The concept is probably already familiar. We really *are* doing high school algebra in a more general setting.

28.8 Definition A nonconstant polynomial $f(x) \in F[x]$ is **irreducible over** F or is an **irreducible polynomial in** $F[x]$ if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than the degree of $f(x)$. If $f(x) \in F[x]$ is a nonconstant polynomial that is not irreducible over F, then $f(x)$ is **reducible over** F. ■