Chapter 11
Irreducible Polynomials

Let $F[x]$ be the polynomial ring over a field F. If $f(x) \in F[x]$, we can now discuss some conditions under which $f(x)$ is irreducible.

11.1 Irreducibility and Roots

For any field F, we recall that the polynomial ring $F[x]$ is a UFD (see Example 10.17). Also, by Exercise 10.4, the units in $F[x]$ are the nonzero elements of F. Thus, every polynomial of degree greater than 0 is a product of one or more irreducibles. Here, a polynomial $f(x)$ of degree greater than 0 is irreducible over F if, whenever $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$, either $g(x)$ or $h(x)$ is an element of F. Otherwise, $f(x)$ is reducible. Note that irreducibility depends very much upon the particular field.

Example 11.1. The polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}$, but reducible over $\mathbb{R}$, since $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. If $r \in F$, we can **evaluate** $f(x)$ at r, and obtain

$$f(r) = a_0 + a_1r + a_2r^2 + \cdots + a_nr^n.$$

In this way, we obtain a function (not a homomorphism!) $\alpha : F \to F$ given by $\alpha(r) = f(r)$. In dealing with polynomials in $\mathbb{R}[x]$, we are accustomed to identifying the polynomial $f(x)$ with this function α. But over a more general field, we cannot do this. Indeed, two different polynomials can induce the same function.

Example 11.2. In $\mathbb{Z}_5[x]$, the polynomials $f(x) = x^3 + x + 1$ and $g(x) = x^5 + x^3 + 1$ induce the same function. That is, $f(r) = g(r)$ for all $r \in \mathbb{Z}_5$. (There are only five elements in $\mathbb{Z}_5$, so this is easily checked.)

It is worth mentioning that we do obtain a homomorphism if we fix an element r of the field and consider evaluating polynomials at r.

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_11

Lemma 11.1. *Let R be a commutative ring and fix $r \in R$. Then the function $\alpha : R[x] \to R$ given by $\alpha(f(x)) = f(r)$ is a homomorphism.*

Proof. Let $f(x) = a_0 + \cdots + a_n x^n$ and $g(x) = b_0 + \cdots + b_n x^n$ be arbitrary polynomials in $R[x]$ (adding in terms with coefficient zero if necessary). Then

$$\begin{aligned}\alpha(f(x) + g(x)) &= a_0 + b_0 + a_1 r + b_1 r + \cdots + a_n r^n + b_n r^n \\ &= (a_0 + \cdots + a_n r^n) + (b_0 + \cdots + b_n r^n) \\ &= \alpha(f(x)) + \alpha(g(x)).\end{aligned}$$

Also, writing $f(x)g(x) = c_0 + \cdots + c_{2n}x^{2n}$, where $c_i = a_0 b_i + \cdots + a_i b_0$, we have

$$\alpha(f(x)g(x)) = c_0 + \cdots + c_{2n} r^{2n},$$

whereas

$$\alpha(f(x))\alpha(g(x)) = (a_0 + \cdots + a_n r^n)(b_0 + \cdots + b_n r^n).$$

But for any i,

$$a_0 b_i r^i + a_1 r b_{i-1} r^{i-1} + \cdots + a_i r^i b_0 = c_i r^i,$$

and so $\alpha(f(x)g(x)) = \alpha(f(x))\alpha(g(x))$. □

We can now use the division algorithm to write a polynomial over a field F as a multiple of $x - a$, for any $a \in F$, plus a constant.

Theorem 11.1 (Remainder Theorem). *Let F be a field and $f(x) \in F[x]$. Take any $a \in F$. Then there exists a $q(x) \in F[x]$ such that*

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

Proof. By the division algorithm for polynomials, $f(x) = (x - a)q(x) + r(x)$, where $q(x), r(x) \in F[x]$, and either $r(x)$ is the zero polynomial, or $\deg(r(x)) < \deg(x - a) = 1$. That is, $r(x)$ is some constant, $b \in F$. By the preceding lemma,

$$f(a) = (a - a)q(a) + b = b.$$

□

It is crucial for us to know if a polynomial has any roots.

Definition 11.1. Let F be a field and $f(x) \in F[x]$. If $a \in F$, then we say that a is a **root** of $f(x)$ if $f(a) = 0$.

Example 11.3. The polynomial $x^2 - 2$ has no roots in $\mathbb{Q}$. However, if we regard it as a polynomial over $\mathbb{R}$, we see that $\sqrt{2}$ and $-\sqrt{2}$ are roots.

Recall that if $f(x), g(x) \in F[x]$, we say that $f(x)$ divides $g(x)$, and write $f(x)|g(x)$, if there exists an $h(x) \in F[x]$ such that $g(x) = f(x)h(x)$.

Theorem 11.2 (Factor Theorem). *Let F be a field and $f(x) \in F[x]$. Take any $a \in F$. Then a is a root of $f(x)$ if and only if $(x - a)|f(x)$.*

Proof Suppose that a is a root of $f(x)$. By the Remainder Theorem, we have $f(x) = (x - a)q(x)$, and hence $(x - a)|f(x)$. Conversely, suppose that $(x - a)|f(x)$. Then $f(x) = (x - a)g(x)$, for some $g(x) \in F[x]$. In this case, $f(a) = (a - a)g(a) = 0$, and hence a is a root. □

Example 11.4. In $\mathbb{Z}_7[x]$, let $f(x) = 3x^3+5x^2+4x+4$. We note that 2 is a root. Thus, $x-2$ (in other words, $x+5$) must divide $f(x)$. In fact, $f(x) = (x-2)(3x^2+4x+5)$.

Corollary 11.1. *Let F be a field and $f(x) \in F[x]$. If $\deg(f(x)) > 1$ and $f(x)$ has a root in F, then $f(x)$ is reducible over F.*

Proof. Let a be a root of $f(x)$. By the Factor Theorem, $f(x) = (x - a)g(x)$, for some $g(x) \in F[x]$. Since $\deg(f(x)) > 1$, we note that $g(x)$ is not a constant. Thus, $f(x)$ is reducible. □

The converse is false!

Example 11.5. In $\mathbb{R}[x]$, let $f(x) = x^4+2x^2+1$. For any $a \in \mathbb{R}$, we have $f(a) \geq 1$; thus, $f(x)$ has no real roots. However, $f(x) = (x^2 + 1)^2$. Thus, $f(x)$ is reducible.

However, for polynomials of degree 2 and 3, the converse does hold.

Corollary 11.2. *Let F be a field and $f(x) \in F[x]$. Then*

1. *if $\deg(f(x)) = 1$, then $f(x)$ is irreducible over F; and*
2. *if $f(x)$ has degree 2 or 3, then $f(x)$ is irreducible over F if and only if it has no roots in F.*

Proof. (1) If $f(x) = g(x)h(x)$, then by Theorem 10.2, either $g(x)$ or $h(x)$ has degree 0.

(2) If $f(x)$ is irreducible, then the preceding corollary tells us that $f(x)$ has no roots. Suppose that $f(x)$ is reducible, say $f(x) = g(x)h(x)$ for some nonconstant polynomials $g(x)$ and $h(x)$ in $F[x]$. As the sum of their degrees is 2 or 3, either $g(x)$ or $h(x)$ must have degree 1. Without loss of generality, say $g(x) = ax+b$, with $a, b \in F$ and $a \neq 0$. But then notice that $f(-a^{-1}b) = (a(-a^{-1}b) + b)h(-a^{-1}b) = 0$. Thus, $-a^{-1}b$ is a root of $f(x)$. □

We can also put a limit on the number of roots of a polynomial.

Corollary 11.3. *Let F be a field and $f(x) \in F[x]$ a nonzero polynomial. If $f(x)$ has degree n, then $f(x)$ has at most n roots in F.*

Proof. We proceed by induction on n. If $n = 0$, then $f(x)$ is a nonzero constant polynomial, which clearly has no roots. Assume that our result is true for n, and let $\deg(f(x)) = n + 1$. If $f(x)$ has no roots, then we are done. Otherwise, let a be a root. By Theorem 11.2, $f(x) = (x - a)g(x)$, for some $g(x) \in F[x]$. Furthermore, by Theorem 10.2, $\deg(g(x)) = n$. Thus, our inductive hypothesis tells us that $g(x)$ has at most n roots. Let b be any root of $f(x)$. Then $0 = f(b) = (b - a)g(b)$. Therefore, either $b - a = 0$ (and $b = a$) or $g(b) = 0$ (and b is among the at most n roots of $g(x)$). Thus, $f(x)$ has at most $n + 1$ roots, as required. □

Exercises

11.1. Are the following polynomials irreducible in $\mathbb{Z}_7[x]$?

1. $x^3 + 5x^2 + 4x + 3$
2. $x^3 + x^2 + 1$
3. $x^4 + x^2 + 2$

11.2. Write each of the following as products of irreducibles in $\mathbb{Z}_5[x]$.

1. $x^3 + 3x^2 + 3x + 2$
2. $x^3 + 2x^2 + 4x + 2$
3. $x^4 + 2x^3 + 4x + 3$

11.3. Find every irreducible polynomial of degree 3 over $\mathbb{Z}_2$.

11.4. If we divide $3x^{59} + 4x^{16} + 2$ by $x + 5$ in $\mathbb{Z}_7[x]$, what is the remainder? (The answer must be in $\{0, 1, \ldots, 6\}$.)

11.5. Let F be an infinite field. If $f(x), g(x) \in F[x]$, and $f(a) = g(a)$ for all $a \in F$, show that $f(x) = g(x)$.

11.6. Let p be a prime. Find infinitely many polynomials $f_1(x), f_2(x), \ldots$ in $\mathbb{Z}_p[x]$ such that $f_i(a) = 0$ for all $a \in \mathbb{Z}_p$ and all positive integers i.

11.7. Is Lemma 11.1 still true for noncommutative rings?

11.8. Let R be an integral domain. Show that $U(R)$ has at most n elements of order n, for every positive integer n. Also give an example of a commutative ring R with identity which is not an integral domain for which this is not true.

11.9. Let p be a prime number. Show that the following are equivalent:

1. $x^2 + 1$ is reducible in $\mathbb{Z}_p[x]$; and
2. there exist nonnegative integers m and n such that $p = m + n$ and $p|(mn - 1)$.

11.10. Show that Theorems 11.1 and 11.2 remain true if F is replaced with an integral domain.

11.2 Irreducibility over the Rationals

If we have a polynomial $f(x) \in \mathbb{Q}[x]$, then by multiplying by a suitable positive integer, we obtain a polynomial in $\mathbb{Z}[x]$. It is often simpler to start with a polynomial with integer coefficients.

As we noted in the preceding section, a polynomial of degree greater than 1 in $\mathbb{Q}[x]$ is necessarily reducible if it has a root. Of course, there are infinitely many possible roots, so testing them all is impossible. However, we can narrow the possible roots down to a finite set of rational numbers.

Theorem 11.3 (Rational Roots Theorem). *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, with $a_n \neq 0$. Suppose that $q \in \mathbb{Q}$ is a root of $f(x)$. If $q = \frac{r}{s}$, with $r, s \in \mathbb{Z}$ and $(r, s) = 1$, then $r|a_0$ and $s|a_n$.*

Proof. We have

$$0 = f\left(\frac{r}{s}\right) = a_0 + \frac{a_1 r}{s} + \cdots + \frac{a_{n-1}r^{n-1}}{s^{n-1}} + \frac{a_n r^n}{s^n}.$$

Multiplying through by s^n, we obtain

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0.$$

As s divides every term except $a_n r^n$, it also divides $a_n r^n$. Since $(r, s) = 1$, Corollary 2.2 tells us that $s|a_n$. Similarly, r divides every term except $a_0 s^n$, so it also divides $a_0 s^n$. Since $(r, s) = 1$, we see that $r|a_0$. □

Example 11.6. Let $f(x) = 3x^3 + 2x^2 - 2x - 8$. In view of the Rational Roots Theorem, the only possible rational roots of $f(x)$ are $\pm 1, \pm 2, \pm 4, \pm 8, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}$ and $\pm\frac{8}{3}$. Trying them all, we see that the only rational root of $f(x)$ is $\frac{4}{3}$.

Of course, polynomials can be reducible without having roots. If we wish to restrict our attention to polynomials in $\mathbb{Z}[x]$, we must be sure that it makes sense to do so. At first blush, it seems conceivable that we could have a polynomial in $\mathbb{Z}[x]$ that factors into a product of polynomials of lower degree in $\mathbb{Q}[x]$, but not in $\mathbb{Z}[x]$. In fact, this does not happen. Let us see why.

Definition 11.2. If $f(x)$ is a nonzero polynomial in $\mathbb{Z}[x]$, then the **content** of $f(x)$ is the largest positive integer that divides every coefficient of $f(x)$. We say that $f(x)$ is **primitive** if its content is 1.

Example 11.7. The polynomial $6x^3 - 15x^2 + 81x - 12$ has content 3, whereas $5x^2 + 14x - 2$ is primitive.

We can now present a famous result due to Carl F. Gauss.

Lemma 11.2 (Gauss's Lemma). *The product of two primitive polynomials in $\mathbb{Z}[x]$ is also primitive.*

Proof. Let $f(x) = a_0 + \cdots + a_n x^n$ and $g(x) = b_0 + \cdots + b_m x^m$ be primitive. Suppose that $f(x)g(x)$ is not primitive. Let p be a prime dividing the content of $f(x)g(x)$. As p cannot divide all of the coefficients of $f(x)$, let i be the smallest nonnegative integer such that p does not divide a_i. Similarly, let j be the smallest nonnegative integer such that b_j is not divisible by p. Then the coefficient of x^{i+j} in $f(x)g(x)$ is

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j-1} b_1 + a_{i+j} b_0,$$

where we add terms with coefficient zero if necessary. Now, this coefficient must be divisible by p. Also, p divides a_k, $0 \leq k < i$, and p divides b_l, $0 \leq l < j$. Thus, every term in the sum is divisible by p except $a_i b_j$, which means that $p | a_i b_j$ as well. But this contradicts Theorem 2.7. □

As a consequence, we can see that if a polynomial in $\mathbb{Z}[x]$ is reducible in $\mathbb{Q}[x]$, then it is reducible in $\mathbb{Z}[x]$ as well.

Theorem 11.4. *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$, and suppose that $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Q}[x]$. Then there is a positive rational number q such that $qg(x)$ and $\frac{1}{q}h(x)$ lie in $\mathbb{Z}[x]$.*

Proof. Assume, first of all, that $f(x)$ is primitive. Choose positive integers a and b such that $ag(x), bh(x) \in \mathbb{Z}[x]$. Then $abf(x) = (ag(x))(bh(x))$.

Let c be the content of $ag(x)$ and d the content of $bh(x)$. Then $\frac{a}{c}g(x), \frac{b}{d}h(x) \in \mathbb{Z}[x]$, and both are primitive polynomials. By Gauss's lemma, their product, $\frac{ab}{cd}f(x)$, is also primitive. Thus, the content of $abf(x)$ is cd. But as $f(x)$ is primitive, the content of $abf(x)$ is also ab. Thus, $ab = cd$, and hence letting $q = \frac{a}{c}$, we see that $\frac{b}{d} = \frac{1}{q}$.

Suppose that $f(x)$ is not primitive. If it is the zero polynomial, then either $g(x)$ or $h(x)$ must be as well. Without loss of generality, say that $h(x)$ is the zero polynomial. Then let q be a positive integer such that $qg(x) \in \mathbb{Z}[x]$. On the other hand, if $f(x)$ is not the zero polynomial, then let k be its content. Writing $f(x) = kf_1(x)$, with $f_1(x) \in \mathbb{Z}[x]$, we have $f_1(x) = \left(\frac{1}{k}g(x)\right)h(x)$. By the argument above, there exists a positive rational number q such that $\frac{q}{k}g(x), \frac{1}{q}h(x) \in \mathbb{Z}[x]$. But then $qg(x), \frac{1}{q}h(x) \in \mathbb{Z}[x]$ as well. □

Example 11.8. The polynomial $f(x) = 3x^3 + 2x^2 - 2x - 8$ has $\frac{4}{3}$ as a rational root. Thus, by Theorem 11.2, $g(x) = x - \frac{4}{3}$ is a divisor of $f(x)$ in $\mathbb{Q}[x]$. Performing polynomial long division, we see that $f(x) = g(x)h(x)$, where $h(x) = 3x^2 + 6x + 6$. Using $q = 3$ in the above theorem, we find that $f(x) = (3x - 4)(x^2 + 2x + 2)$, and we have a factorization in $\mathbb{Z}[x]$.

Even if a polynomial has coefficients in $\mathbb{Z}$, it can still be difficult to tell if it is irreducible over $\mathbb{Q}$. One nice result that can be rather helpful is attributed to F. Gotthold M. Eisenstein, although a proof was first published by Theodor Schönemann.

Theorem 11.5 (Eisenstein's Criterion). *Let $f(x) = a_0 + a_1 + \cdots + a_n x^n \in \mathbb{Z}[x]$, with $n \geq 1$ and $a_n \neq 0$. Suppose that there exists a prime p such that $p|a_i$, $0 \leq i < n$, but $p \nmid a_n$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. If $f(x)$ is reducible, then by Theorem 11.4, there exist nonconstant polynomials $g(x) = b_0 + \cdots + b_l x^l$ and $h(x) = c_0 + \cdots + c_m x^m$ in $\mathbb{Z}[x]$, with $b_l \neq 0 \neq c_m$ and $f(x) = g(x)h(x)$. Now, p divides $a_0 = b_0 c_0$, but p^2 does not. Thus, p divides exactly one of $\{b_0, c_0\}$. Without loss of generality, say $p|b_0$. But p does not divide $a_n = b_l c_m$. Thus, p divides neither b_l nor c_m. Let i be the smallest positive integer such that $p \nmid b_i$. Then

$$a_i = b_0 c_i + b_1 c_{i-1} + \cdots + b_{i-1} c_1 + b_i c_0.$$

Now, $p|b_j$, $0 \leq j < i$. Furthermore, as $i \leq l < n$, we know that $p|a_i$. Thus, $p|b_i c_0$. But p divides neither b_i nor c_0, and we have a contradiction. □

Example 11.9. The polynomial $13x^3 - 42x^2 + 81x - 15$ is irreducible over $\mathbb{Q}$, using Eisenstein's criterion with $p = 3$.

Example 11.10. For any positive integer n and any prime p, we observe that $x^n - p$ is irreducible over $\mathbb{Q}$.

Note that if F is a subfield of K, and $f(x)$ is a reducible polynomial in $F[x]$, then it is also necessarily reducible in $K[x]$ (just using the same factorization). Of course, the fact that it is reducible in $K[x]$ does not imply that it is reducible in $F[x]$, as we illustrated in Example 11.3.

But the relationship between $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ is backwards. Indeed, we have seen that if a polynomial in $\mathbb{Z}[x]$ is reducible in $\mathbb{Q}[x]$, then it is also reducible in $\mathbb{Z}[x]$. The other direction does not work!

Example 11.11. Let $f(x) = 2x - 6$. Then by Corollary 11.2, $f(x)$ is irreducible in $\mathbb{Q}[x]$. But $f(x)$ is reducible in $\mathbb{Z}[x]$; indeed, $f(x) = 2(x - 3)$, and neither 2 nor $x - 3$ is a unit in $\mathbb{Z}[x]$.

The problem, then, is that the nonzero constants are not necessarily units in $\mathbb{Z}[x]$, and this affects irreducibility.

Lemma 11.3. *Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if either*

1. *$f(x)$ is a (positive or negative) prime in $\mathbb{Z}$; or*
2. *$f(x)$ is a primitive polynomial that is irreducible in $\mathbb{Q}[x]$.*

Proof. Note that a unit in $\mathbb{Z}[x]$ is also a unit in $\mathbb{Q}[x]$, and hence a constant. But the only constants having inverses in $\mathbb{Z}[x]$ are ± 1, so those are the only units.

Suppose that $f(x)$ is a constant $c \in \mathbb{Z}$. If c is prime, then its only factorizations are $1 \cdot c$ and $(-1)(-c)$, so $f(x)$ is irreducible. Otherwise, c has some other factorization, and $f(x)$ is not irreducible.

So, let $\deg(f(x)) \geq 1$. Suppose that $f(x)$ is irreducible in $\mathbb{Z}[x]$. If $f(x)$ has content $d > 1$, then $f(x)$ has a factorization $d\left(\frac{1}{d}f(x)\right)$, and therefore $f(x)$ is reducible. So, we may assume that $f(x)$ is primitive. If it is reducible in $\mathbb{Q}[x]$, then by Theorem 11.4, it is reducible in $\mathbb{Z}[x]$ as well. Conversely, assume that $f(x)$ is irreducible in $\mathbb{Q}[x]$ and primitive. If $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbb{Z}[x]$, then we have a factorization in $\mathbb{Q}[x]$ as well, which would make $f(x)$ reducible over $\mathbb{Q}$, unless either $g(x)$ or $h(x)$ is a constant. Without loss of generality, let $g(x) = e \neq 0$. If $e = \pm 1$, then $g(x)$ is a unit in $\mathbb{Z}[x]$. If not, then $f(x)$ has content $|e|$ times the content of $h(x)$, contradicting the assumption that $f(x)$ is primitive. Thus, $f(x)$ is irreducible in $\mathbb{Z}[x]$ in this case. □

Let us now present the counterexample promised in Section 10.4. We already know that $\mathbb{Z}[x]$ is not a PID. But we have the following.

Theorem 11.6. *The ring $\mathbb{Z}[x]$ is a UFD.*

Proof. Let $f(x) \in \mathbb{Z}[x]$ be a nonzero nonunit. We will show that $f(x)$ is a product of irreducibles. First, suppose that $\deg(f(x)) = n \geq 1$. We claim that $f(x)$ is a product of polynomials in $\mathbb{Z}[x]$ that are irreducible in $\mathbb{Q}[x]$. Our proof is by strong induction on n. If $n = 1$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$ and there is nothing to do. Let $n \geq 2$, and suppose that our claim holds for polynomials of smaller degree. If $f(x)$ is irreducible in $\mathbb{Q}[x]$, then again, there is nothing to do. Otherwise, we know that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials of degree less than n in $\mathbb{Q}[x]$. By Theorem 11.4, we may choose $g(x)$ and $h(x)$ to be in $\mathbb{Z}[x]$. Then our inductive hypothesis tells us that $g(x)$ and $h(x)$ are products of polynomials in $\mathbb{Z}[x]$ that are irreducible in $\mathbb{Q}[x]$, and hence, so is $f(x)$, proving the claim.

If $f(x) = f_1(x) \cdots f_k(x)$, where each $f_i(x)$ is irreducible in $\mathbb{Q}[x]$, then let c_i be the content of $f_i(x)$. We now have

$$f(x) = (c_1 \cdots c_k)\left(\frac{1}{c_1}f_1(x)\right) \cdots \left(\frac{1}{c_k}f_k(x)\right),$$

where each $\frac{1}{c_i}f_i(x)$ is irreducible in $\mathbb{Z}[x]$, by the preceding lemma.

Thus, bringing the $\deg(f(x)) = 0$ possibility back into consideration, we see that $f(x)$ is either an integer not in $\{0, \pm 1\}$, or a nonzero integer multiplied by a product of irreducibles in $\mathbb{Z}[x]$.

It remains only to consider the case of an integer. But the Fundamental Theorem of Arithmetic tells us that any integer not in $\{0, \pm 1\}$ is a product of (positive or negative) primes, which are certainly irreducible in $\mathbb{Z}[x]$. We do still have to deal with $f(x) = (-1)g_1(x) \cdots g_k(x)$, where each $g_i(x)$ is irreducible, but then this is $(-g_1(x))g_2(x) \cdots g_k(x)$, and $-g_1(x)$ is irreducible as well.

Let us verify the uniqueness. Suppose that

$$f(x) = p_1 \cdots p_k g_1(x) \cdots g_l(x) = q_1 \cdots q_m h_1(x) \cdots h_n(x),$$

where each p_i and q_i is a (positive or negative) prime in $\mathbb{Z}$, and each $g_i(x)$ and $h_i(x)$ is a primitive polynomial which is irreducible in $\mathbb{Q}[x]$. (We allow the possibility that k, l, m or n may be zero.) By Gauss's lemma, the product of primitive polynomials is primitive. Thus, the content of $f(x)$ is $|p_1 \cdots p_k| = |q_1 \cdots q_l|$. By the Fundamental Theorem of Arithmetic, $k = l$ and after rearranging, each $p_i = \pm q_i$. Cancelling, we have $g_1(x) \cdots g_m(x) = \pm h_1(x) \cdots h_n(x)$. But these are products of irreducible polynomials in $\mathbb{Q}[x]$. As $\mathbb{Q}[x]$ is a UFD, $m = n$ and, after rearranging, each $g_i(x) = q_i h_i(x)$, for some $q_i \in \mathbb{Q}$. Write $q_i = \frac{r_i}{s_i}$, with $r_i, s_i \in \mathbb{Z}$ and $s_i \neq 0$. Then $s_i g_i(x) = r_i h_i(x)$. As $g_i(x)$ and $h_i(x)$ are primitive, looking at the content of each side of the equation, we have $|s_i| = |r_i|$, and hence $q_i \in \{1, -1\}$. We are done. □

Exercises

11.11. Find all rational roots of each of the following polynomials.

1. $x^3 - 7x^2 + 5x + 2$
2. $6x^4 - x^3 + 4x^2 - x - 2$

11.12. Are the following polynomials irreducible over $\mathbb{Q}$?

1. $3x^4 + 15x^3 - 25x^2 + 45x + 10$
2. $2x^3 + 5x^2 + x + 7$
3. $x^{14} - 75$

11.13. Write each of the following polynomials as a product of irreducibles in $\mathbb{Q}[x]$.

1. $x^4 - 10x^3 + 35x^2 - 48x + 18$
2. $x^4 + 2x^3 + x^2 + 3x + 2$

11.14. Write each of the following polynomials as a product of irreducibles in $\mathbb{Z}[x]$.

1. $6x^4 + 84x^3 - 126x$
2. $6x^4 - 3x^3 + 18x^2 - 3x - 3$

11.15. Let F be a field, $a \in F$ and $f(x) \in F[x]$. Show that $f(x)$ is irreducible if and only if $f(x + a)$ is irreducible.

11.16. Modify Eisenstein's criterion as follows, namely, insist that $p|a_i$, $1 \leq i \leq n$, but $p \nmid a_0$ and $p^2 \nmid a_n$. Show that the result still holds.

11.17. Is $7x^6 + 21x^5 - 49x^3 + 14x^2 + 7x + 2$ reducible or irreducible over $\mathbb{Q}$?

11.18. Let R be a Euclidean domain. If $f(x) \in R[x]$ is a nonzero polynomial, let us say that it is primitive if the only common divisors of its coefficients are the units of R. Show that Gauss's lemma holds in $R[x]$.

11.3 Irreducibility over the Real and Complex Numbers

While the real numbers may seem like a more natural field with which to work, the complex numbers have a more attractive algebraic structure. Indeed, we wish to consider the complex numbers, because there are nonconstant real polynomials, such as x^2+1, having no real roots. The complex numbers do not have this problem. Indeed, this is a famous result known as the Fundamental Theorem of Algebra. There are many different proofs of this theorem. Curiously, to the best of the author's knowledge, all of these proofs require results from outside of algebra. A proof that is mostly algebraic can be found in the advanced textbook of Dummit and Foote [1]. (Sadly, the algebra involved is somewhat beyond the scope of this course.)

Theorem 11.7 (Fundamental Theorem of Algebra). *Let $f(x)$ be a nonconstant polynomial in $\mathbb{C}[x]$. Then $f(x)$ has a root in $\mathbb{C}$.*

We say that the field of complex numbers is **algebraically closed**.

Corollary 11.4. *If $f(x) \in \mathbb{C}[x]$, then $f(x)$ is irreducible if and only if* $\deg(f(x)) = 1$.

Proof. Combine Theorem 11.7 with Corollaries 11.1 and 11.2. □

Corollary 11.5. *Let $f(x) \in \mathbb{C}[x]$ be a nonconstant polynomial. Then there exist $a, c_1, c_2, \ldots, c_n \in \mathbb{C}$ such that $f(x) = a(x-c_1)(x-c_2)\cdots(x-c_n)$.*

Proof. We proceed by induction on $\deg(f(x)) = n$. If $n = 1$, then $f(x) = ax+b = a(x-(-a^{-1}b))$, for some $a, b \in \mathbb{C}$, with $a \neq 0$. Suppose that the result is true for n, and let $\deg(f(x)) = n+1$. By Theorem 11.7, $f(x)$ has a root, $c_{n+1} \in \mathbb{C}$. But then Theorem 11.2 tells us that $f(x) = g(x)(x-c_{n+1})$, where $\deg(g(x)) = n$, by Theorem 10.2. Now apply our inductive hypothesis to $g(x)$. □

Thus, complex polynomials behave as nicely as we could possibly wish. What about real polynomials? The situation there is slightly more complicated.

Lemma 11.4. *Let $f(x) \in \mathbb{R}[x]$. If $c, d \in \mathbb{R}$, and $c+di$ is a complex root of $f(x)$, then so is $c-di$.*

Proof. Write $\overline{c+di} = c-di$. Let $f(x) = a_0 + \cdots + a_n x^n$, $a_i \in \mathbb{R}$. Then if $z = c+di$, we have

$$f(\bar{z}) = a_0 + a_1\bar{z} + a_2(\bar{z})^2 + \cdots + a_n(\bar{z})^n.$$

But by Example 9.13, the function mapping z to $\bar{z}$ is a homomorphism. Thus,

$$\begin{aligned} f(\bar{z}) &= a_0 + a_1\bar{z} + a_2\overline{z^2} + \cdots + a_n\overline{z^n} \\ &= \overline{a_0} + \overline{a_1}\bar{z} + \overline{a_2}\overline{z^2} + \cdots + \overline{a_n}\overline{z^n} \\ &= \overline{a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n} \\ &= \overline{f(z)} = \bar{0} = 0, \end{aligned}$$

making using of the fact that each $\overline{a_i} = a_i$, since $a_i \in \mathbb{R}$. □

We can use this to classify the irreducible real polynomials.

Theorem 11.8. *Let $f(x) \in \mathbb{R}[x]$. Then $f(x)$ is irreducible over $\mathbb{R}$ if and only if either*

1. $\deg(f(x)) = 1$*; or*
2. $f(x) = ax^2 + bx + c$*, where $a \neq 0$ and $b^2 < 4ac$.*

Proof. Since $\mathbb{R}$ is a field, constant polynomials are either 0 or a unit, and therefore need not be considered. If $\deg(f(x)) = 1$, then Corollary 11.2 tells us that $f(x)$ is indeed irreducible. Therefore, let $f(x)$ have degree at least 2. Suppose that $f(x)$ is irreducible.

By Theorem 11.7, $f(x)$ has a root $z = a+bi \in \mathbb{C}$. If $z \in \mathbb{R}$, then by Corollary 11.1, we have a contradiction. Assume otherwise. By Lemma 11.4, $a - bi$ is also a root. Expressing $f(x)$ as in Corollary 11.5, we see that $(x-(a+bi))(x-(a-bi))|f(x)$ in $\mathbb{C}[x]$. But $(x-(a+bi))(x-(a-bi)) = x^2 - 2ax + (a^2+b^2) \in \mathbb{R}[x]$. Thus, applying the division algorithm, we see that there exist $q(x), r(x) \in \mathbb{R}[x]$ such that $f(x) = (x^2 - 2ax + (a^2+b^2))q(x) + r(x)$, and $r(x) = 0$ or $\deg(r(x)) < 2$. By the uniqueness of the division algorithm in $\mathbb{C}[x]$, we must have $r(x) = 0$ and $x^2 - 2ax + (a^2+b^2)$ divides $f(x)$ in $\mathbb{R}[x]$. In particular, if $\deg(f(x)) > 2$, then $f(x)$ must be reducible.

Thus, we may assume that $f(x) = ax^2 + bx + c$, with $a \neq 0$. By Corollary 11.2, such a polynomial is irreducible over $\mathbb{R}$ if and only if it has no roots in $\mathbb{R}$. But the quadratic formula tells us that this happens if and only if $b^2 - 4ac < 0$. We are done. □

We can use this to recover a well-known fact from calculus.

Corollary 11.6. *Let $f(x) \in \mathbb{R}[x]$ be a polynomial of odd degree. Then $f(x)$ has a real root.*

Proof. We know that $\mathbb{R}[x]$ is a UFD. Thus, write $f(x)$ as a product of irreducible polynomials. By the preceding theorem, each such irreducible has degree 1 or 2. Since $f(x)$ has odd degree, at least one of these irreducible polynomials has degree 1. Therefore, there exist $a, b \in \mathbb{R}$, with $a \neq 0$, such that $ax + b$ divides $f(x)$. But then $-a^{-1}b$ is a root of $f(x)$. □

Exercises

11.19. Given that a is a root of $f(x)$, find all complex roots of $f(x)$.

1. $f(x) = x^3 - 11x^2 + 41x - 91, a = 2 + 3i$
2. $f(x) = x^4 + x^2 - 2x + 6, a = 1 - i$

11.20. Given that a is a root of $f(x)$, find all complex roots of $f(x)$.

1. $f(x) = x^3 + x^2 - 5x - 21, a = 3$
2. $f(x) = x^4 - 6x^3 + 33x^2 - 84x + 136, a = 1 + 4i$

11.21. Write each of the following polynomials as a product of irreducibles in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

1. $x^4 - 10$
2. $x^3 + x^2 + 5x - 22$

11.22. Write each of the following polynomials as a product of irreducibles in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

1. $x^3 + 12$
2. $x^4 + 4x^2 + 4$

11.23. Find a nonzero polynomial in $\mathbb{R}[x]$ having $2 - 5i$, $4 + i$ and 6 as roots.

11.24. Let $f(x)$ and $g(x)$ be nonzero polynomials in $\mathbb{Q}[x]$. Consider the gcds of $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$. Must these gcds be the same, or can they be different?

11.4 Irreducibility over Finite Fields

When our field is finite, we have the luxury of taking a brute force approach to factoring polynomials. That is, we can simply list all of the polynomials of suitable degrees, and see if the products work. Of course, we can save ourselves some effort by narrowing the possibilities first.

Example 11.12. Let $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$. We claim that $f(x)$ is irreducible over $\mathbb{Z}_2$. If not, there are two possibilities. First, $f(x)$ could be a product of a degree 1 polynomial and a degree 3 polynomial. But if it has a degree 1 polynomial as a factor, then it has a root. There are only two possible roots in $\mathbb{Z}_2$, namely, 0 and 1, and neither works. Second, $f(x)$ could be a product of two polynomials of degree 2. Now, the only possible coefficients are 0 and 1. Furthermore, the leading coefficients and the constant terms must multiply to give 1. Thus, the only possible factors are $x^2 + 1$ and $x^2 + x + 1$. But $x^2 + 1$ has 1 as a root, and $f(x)$ does not, so

only $x^2 + x + 1$ remains. However, $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f(x)$. Thus, $f(x)$ is indeed irreducible.

Example 11.13. Let $f(x) = 3x^5 + x^4 + 4x^3 + 4x^2 + 3x + 2 \in \mathbb{Z}_5[x]$. We would like to write $f(x)$ as a product of irreducibles. The first thing we should do is check for roots. We run through the five elements of $\mathbb{Z}_5$ and find that 3 is a root. Thus, $x - 3$ (or, equivalently, $x + 2$) divides $f(x)$. Performing polynomial long division, we find that $f(x) = (x + 2)(3x^4 + 4x^2 + x + 1)$. Let $g(x) = 3x^4 + 4x^2 + x + 1$. Evaluating $g(x)$ at each element of $\mathbb{Z}_5$, we see that $g(x)$ has no roots. Thus, if it is to be factored, it must be as a product of two polynomials of degree 2. Up to a unit in $\mathbb{Z}_5$, these factors would have to be $x^2 + ax + b$ and $3x^2 + cx + d$, for some $a, b, c, d \in \mathbb{Z}_5$. Furthermore, looking at the constant terms, we have $bd = 1$. Thus, once b is decided, $d = b^{-1}$. Looking at the coefficients of x^3, we have $3a + c = 0$. Thus, once a is decided, we have $c = 2a$. Trying the various possibilities for a and b, we have $g(x) = (x^2 + 2x + 3)(3x^2 + 4x + 2)$. Since $g(x)$ has no roots, this cannot be factored any further. Thus, $f(x) = (x + 2)(x^2 + 2x + 3)(3x^2 + 4x + 2)$ is a product of irreducibles in $\mathbb{Z}_5[x]$.

Our ability to handle polynomials over finite fields can be helpful when we consider polynomials in $\mathbb{Q}[x]$.

Theorem 11.9. *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Let p be a prime such that $p \nmid a_n$. Reducing all of the coefficients modulo p, if $[a_0] + [a_1]x + \cdots + [a_n]x^n$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Suppose $f(x)$ is reducible in $\mathbb{Q}[x]$. Then by Theorem 11.4, we must have $f(x) = g(x)h(x)$, where $g(x) = b_0 + \cdots + b_kx^k$ and $h(x) = c_0 + \cdots + c_mx^m$ are polynomials in $\mathbb{Z}[x]$, with $k, m > 0$ and $b_k \neq 0 \neq c_m$. Now, we have

$$a_i = b_0c_i + b_1c_{i-1} + \cdots + b_ic_0,$$

for each i. By Example 9.12, the function from $\mathbb{Z}$ to $\mathbb{Z}_p$ sending d to $[d]$ is a ring homomorphism. Thus,

$$[a_i] = [b_0][c_i] + [b_1][c_{i-1}] + \cdots + [b_i][c_0].$$

It now follows that

$$[a_0] + \cdots + [a_n]x^n = ([b_0] + \cdots + [b_k]x^k)([c_0] + \cdots + [c_m]x^m).$$

That is, $[a_0] + \cdots + [a_n]x^n$ is reducible, unless one of the factors is a constant polynomial. But as $p \nmid a_n$, we see that the degree of $[a_0] + \cdots + [a_n]x^n$ is $n = k + m$. The only way the product will have the correct degree is if $[b_k] \neq [0] \neq [c_m]$. This contradiction completes the proof. □

Note that the condition that p does not divide the leading coefficient is important. Indeed, $3x^2 + x - 4$ is reducible in $\mathbb{Q}[x]$, as it is $(x - 1)(3x + 4)$. But if we tried to use $p = 3$, we would obtain $x + 2 \in \mathbb{Z}_3[x]$, which is certainly irreducible. Also, the converse of the theorem is not true. For instance, $x^2 + 1$ is irreducible over $\mathbb{Q}$ (or, for that matter, $\mathbb{R}$), but in $\mathbb{Z}_5[x]$, we have $x^2 + 1 = (x + 2)(x + 3)$.

Example 11.14. We claim that $15x^4 - 29x^3 + 13x^2 + 33x - 201$ is irreducible over $\mathbb{Q}[x]$. Use Theorem 11.9 with $p = 2$. In $\mathbb{Z}_2[x]$, we obtain $x^4 + x^3 + x^2 + x + 1$ which, by Example 11.12, is irreducible.

Sometimes, we might have to try more than one prime.

Example 11.15. Let $f(x) = 5x^3 + 3x^2 + x + 1$. If we use $p = 2$, we obtain $x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$. But this polynomial has 1 as a root, so it is reducible. No help here! Let us try $p = 3$. Then we get $2x^3 + x + 1 \in \mathbb{Z}_3[x]$. By Corollary 11.2, it is irreducible if it has no roots. But trying 0, 1 and 2, we see that it has no roots in $\mathbb{Z}_3$. Thus, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Exercises

11.25. Are the following polynomials reducible or irreducible over the rationals?

1. $f(x) = x^3 + 5x^2 + 2x + 16$
2. $f(x) = 22x^4 - 9x^3 + 16x^2 + 18x + 20$

11.26. Are the following polynomials reducible or irreducible over the rationals?

1. $f(x) = 9x^4 - 15x^3 + 8x^2 - 6x + 25$
2. $f(x) = 2x^4 + 11x^3 + 16x^2 + 5x + 6$

11.27. Let F be a finite field with n elements. How many monic irreducible polynomials of degree 2 are there in $F[x]$?

11.28. Write each of the following polynomials as a product of irreducibles in $\mathbb{Z}_{11}[x]$.

1. $2x^3 + 3x^2 + 9x + 10$
2. $x^4 + 4x^3 + 5x^2 + x + 7$

11.29. Let p be an odd prime. Show that $x^4 + 1$ is reducible over $\mathbb{Z}_p$ in each of the following cases:

1. there exists an $a \in \mathbb{Z}_p$ such that $a^2 = p - 1$;
2. there exists an $a \in \mathbb{Z}_p$ such that $a^2 = p - 2$; or
3. there exists an $a \in \mathbb{Z}_p$ such that $a^2 = 2$.

11.30. Show that $x^4 + 1$ is irreducible in $\mathbb{Q}[x]$ but reducible in $\mathbb{Z}_p[x]$ for every prime p. (Thus, the converse of Theorem 11.9 is wildly false!)

Reference

1. Dummit, D.S., Foote, R.M.: Abstract Algebra, 3rd edn. Wiley, Hoboken (2004)