§37
Irreducibility Criteria

In this paragraph, we develop some sufficient conditions for a polynomial to be irreducible. In general, given a specific polynomial, it is extremely difficult to determine whether it is irreducible. This is not surprising when we remember that it is also exceedingly difficult to determine whether a given specific integer is prime.

We start with Eisenstein's criterion, which is very simple to use (G. Eisenstein, a German mathematician (1823-1852)).

37.1 Lemma (Eisenstein's criterion): Let \( D \) be a unique factorization domain and let

\[
 f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0
\]

be a nonzero polynomial in \( D[x] \) with \( C(f) \equiv 1 \). If there is a prime (irreducible) element \( p \) in \( D \) such that

\[
 p \mid a_n, \quad p \mid a_{n-1}, \ldots, p \mid a_1, p \mid a_0, \quad p^2 \nmid a_0,
\]

then \( f \) is irreducible over \( D \).

**Proof:** Suppose, by way of contradiction, that \( f(x) \) is reducible over \( D \). Then its proper factors must have degrees \( \geq 0 \), because \( C(f) \equiv 1 \). Assume \( f(x) = g(x)h(x) \), where

\[
 g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \quad (b_m \neq 0, m \geq 1)
\]

\[
 h(x) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0 \quad (c_k \neq 0, k \geq 1)
\]

are polynomials in \( D[x] \).

Then \( a_0 = b_0 c_0 \). Since \( p \mid a_0 \) and so \( p \mid b_0 c_0 \) by hypothesis and \( p \) is prime, we see \( p \mid b_0 \) or \( p \mid c_0 \). Here both \( p \mid b_0 \) and \( p \mid c_0 \) cannot be simultaneously true, for then we would have \( p^2 \mid b_0 c_0 \), so \( p^2 \nmid a_0 \), against our hypothesis. Thus one and only one of \( p \mid b_0 \), \( p \mid c_0 \) is true. Let us assume, without loss of generality, that \( p \mid b_0 \) and \( p \nmid c_0 \).
Also \( a_n = b_m c_k \). Since \( p \nmid a_n \) and so \( p \nmid b_m c_k \) by hypothesis, we have \( p \nmid b_m \). Thus \( p \mid b_0 \) and \( p \nmid b_m \). Let \( r \) be the smallest index for which the coefficient \( b_r \) in \( g(x) \) is not divisible by \( p \), so that
\[
p \mid b_0, p \mid b_1, \ldots, p \mid b_{r-1}, p \nmid b_r
\]
(possibly \( r = 1 \) or \( r = m \)).

Now \( a_r = (b_0 c_r + b_1 c_{r-1} + \ldots + b_{r-1} c_1) + b_r c_0 \), and \( r \leq m < m + k = n \). So \( p \mid a_r \) by hypothesis and \( p \) divides the expression in ( ) by \((\ast)\), so \( p \mid b_r c_0 \). Then, since \( p \) is prime, this forces \( p \mid b_r \) or \( p \mid c_0 \), whereas \( p \nmid b_r \) and \( p \nmid c_0 \). This contradiction completes the proof.

37.2 Examples: (a) \( x^5 + 5x + 5 \in \mathbb{Z}[x] \) is irreducible over \( \mathbb{Z} \), because its content is 1 and
\[
5 \nmid 1,
5 \mid 0, 5 \mid 0, 5 \mid 5, 5 \mid 5,
5^2 \nmid 5.
\]

(b) Let \( D = \mathbb{Z}[i] \) and \( f(x) = 3x^3 + 2x^2 + (4 - 2i)x + (1 + i) \in D[x] \). Then \( D \) is a unique factorization domain and \( C(f) \equiv 1 \). Moreover \( 1 + i \in D \) is a prime element in \( D \) and
\[
1 + i \nmid 3,
1 + i \mid 2, 1 + i \mid 4 - 2i, 1 + i \mid 1 + i,
(1 + i)^2 \nmid 1 + i.
\]
Hence \( f(x) \) is irreducible over \( D \).

(c) Let \( D \) be a unique factorization domain and \( g(x,y) = x^n - y \in (D[y])[x] \). The content of \( g \) is \( 1 \in D[y] \), since \( g \) is in fact a monic polynomial. Also, \( y \) is irreducible in \( D[y] \) and
\[
y \nmid 1,
y \mid 0, y \mid 0, \ldots, y \mid 0, y \mid -y,
y^2 \nmid -y,
\]
hence \( g(x,y) = x^n + 0x^{n-1} + 0x^{n-2} + \cdots + 0x - y \in (D[y])[x] \) is irreducible over \( D[y] \).

(d) Let \( p \in \mathbb{N} \) be a prime number and \( \Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x] \). The polynomial \( \Phi_p(x) \) is known as the \( p \)-th cyclotomic polynomial. We show that \( \Phi_p(x) \) is irreducible over \( \mathbb{Z} \). Eisenstein’s criterion is not directly applicable, but we observe that
\[
(x - 1)\Phi_p(x) = x^p - 1,
\]
441
and, when we substitute \( x + 1 \) for \( x \) in both sides of this equation, we get

\[
x\Phi_p(x + 1) = (x + 1)^p - 1 = \sum_{k=0}^{p-1} \binom{p}{k} x^{p-k}
\]

by the binomial theorem (Theorem 29.16), so

\[
\Phi_p(x + 1) = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-1}
\]

and we will try to apply Eisenstein’s criterion to this polynomial. We note \( p \mid p! \), so \( p \mid (p - k)!k! \binom{p}{k} \). Since \( p \) is relatively prime to \( (p - k)!k! \) when \( 1 \leq k \leq p - 1 \), Theorem 5.12 gives \( p \mid \binom{p}{k} \) for \( k = 1, 2, \ldots, p - 1 \). So

\[
p \nmid 1,
\]

\[
p \mid \binom{p}{1}, \quad p \mid \binom{p}{2}, \ldots, \quad p \mid \binom{p}{p-1},
\]

and the content of \( \Phi_p(x + 1) = 1 \). Hence \( \Phi_p(x + 1) \) is irreducible over \( \mathbb{Z} \).

This implies that \( \Phi_p(x) \) is also irreducible over \( \mathbb{Z} \), since \( \Phi_p(x) \) is clearly not a unit in \( \mathbb{Z}[x] \) and any factorization \( \Phi_p(x) = f(x)g(x) \) of \( \Phi_p(x) \) into nonunit polynomials \( f(x), g(x) \in \mathbb{Z}[x] \) would give a factorization \( \Phi_p(x + 1) = f(x + 1)g(x + 1) = f_1(x)g_1(x) \) of \( \Phi_p(x + 1) \) into nonunit polynomials \( f_1(x), g_1(x) \) in \( \mathbb{Z}[x] \), contrary to the irreducibility of \( \Phi_p(x + 1) \) over \( \mathbb{Z} \).

The argument in the last example can be generalized.

37.3 Lemma: Let \( D \) be an integral domain, \( \alpha \) a unit in \( D \) and let \( \beta \) be an arbitrary element of \( D \).

(1) The mapping \( T: D[x] \to D[x] \) is a ring isomorphism such that \( \forall T = \gamma \)

\[
f(x) \to f(\alpha x + \beta)
\]

for all \( \gamma \in D \).

(2) \( \deg f(\alpha x + \beta) = \deg f(x) \) for any \( f(x) \in D[x]\setminus\{0\} \) (that is, \( T \) preserves degrees of polynomials).

(3) \( f(x) \) is irreducible over \( D \) if and only if \( f(\alpha x + \beta) \) is irreducible over \( D \).

(4) If, in addition, \( D \) is a unique factorization domain, then \( C(f(x)) \cong C(f(\alpha x + \beta)) \) for any \( f(x) \in D[x]\setminus\{0\} \) (that is, \( T \) preserves contents of polynomials).
Proof: (1) The mapping \( T: f(x) \rightarrow f(\alpha x + \beta) \) is just the substitution homomorphism \( T_{\alpha x+\beta} \) (Lemma 35.3 with \( D, D[x], \alpha x + \beta \) in place of \( R, S, s \), respectively). We are to show that \( T \) is one-to-one and onto. To this end, we need only find an inverse of \( T \) (Theorem 3.17(2)). This is quite easy. We are tempted to substitute \( (x - \beta)/\alpha \) for \( x \). This idea is correct, but we must formulate it properly. Since \( \alpha \) is a unit in \( D \), there is an inverse \( \alpha^{-1} \) of \( \alpha \) in \( D \), and we put \( S: D[x] \rightarrow D[x] \). Then we have

\[
f(x) = f(\alpha^{-1}(x - \beta))
\]

for all \( f(x) \in D[x] \). Hence \( TS = t_{D[x]} \) and \( T \) is therefore an isomorphism. Finally, polynomials of degree 0 and the polynomial 0 \( \in D[x] \) are not affected by the substitution \( x \rightarrow \alpha x + \beta \) and so \( \gamma T = \gamma \) for all \( \gamma \in D \).

(2) For any \( f(x) \in D[x]\{0\} \), if \( \deg f = n \) and

\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0
\]

with \( a_n \neq 0 \), we have

\[
f(\alpha x + \beta) = a_n (\alpha x + \beta)^n + a_{n-1} (\alpha x + \beta)^{n-1} + \cdots + a_1 (\alpha x + \beta) + a_0
\]

\[
= a_n \alpha^n x^n + \text{terms of lower degree},
\]

with \( a_n \alpha^n \neq 0 \) as the leading coefficient. So \( \deg f(\alpha x + \beta) = n \), as claimed.

(3) If \( f(x) \in D[x]\{0\} \) is not irreducible over \( D \), then either \( f(x) \) is a unit in \( D[x] \), hence \( f(x) \in D \) is a unit in \( D \) and \( f(\alpha x + \beta) = f(x) \) (by part (1)) is also a unit in \( D \) and in \( D[x] \); or \( f(x) = g(x)h(x) \) for some polynomials \( g(x), h(x) \) in \( D[x] \) with \( 1 \leq \deg g(x) < \deg f(x) \), and then \( f(\alpha x + \beta) = g(\alpha x + \beta)h(\alpha x + \beta) \) with \( g(\alpha x + \beta), h(\alpha x + \beta) \in D[x] \) and \( 1 \leq \deg g(x) = \deg g(\alpha x + \beta) = \deg g(x) < \deg f(x) = \deg f(\alpha x + \beta) \) (by part (2)), and thus \( f(\alpha x + \beta) \) has a proper divisor. In either case, \( f(\alpha x + \beta) \) is not irreducible over \( D \).

Repeating the same argument for the substitution \( x \rightarrow \alpha^{-1}(x - \beta) \), we conclude: if \( f(\alpha x + \beta) \) is not irreducible over \( D \), then \( f(x) \) is not irreducible over \( D \).

(4) Suppose now that \( D \) is a unique factorization domain, that \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \), and that \( \mathcal{C}(f(x)) = \gamma \). Then

\[
f(\alpha x + \beta) = \binom{n}{0} a_n \alpha^n x^n + \binom{n}{1} a_n \alpha^{n-1} \beta + \binom{n}{0} a_{n-1} \alpha^{n-1} x^{n-1}
\]
\[
+ \left( \binom{n}{2} a_n \alpha^{n-2} \beta^2 + \binom{n}{1} a_{n-1} \alpha^{n-1} \beta + \binom{n}{0} a_{n-2} \alpha^{n-2} \right) x^{n-2} + \cdots .
\]

A content \( \delta \) of \( f(\alpha x + \beta) \) divides \( \binom{n}{0} a_n \alpha^n \), hence \( \delta \mid a_n \) (\( \alpha \) and \( \alpha^n \) is a unit); and \( \delta \) divides the coefficient of \( x^{n-1} \), hence \( \delta \mid \binom{n}{1} a_{n-1} \alpha^{n-1} \), hence \( \delta \mid a_{n-1} \); and \( \delta \) divides the coefficient of \( x^{n-2} \), hence \( \delta \mid \binom{n}{0} a_{n-2} \alpha^{n-2} \), hence \( \delta \mid a_{n-2} \); etc. Proceeding in this way, we see that \( \delta \) divides all the coefficients of \( f(x) \). Since \( y \approx C(f(x)) \), we obtain \( \delta \mid y \). The same argument with \( f(\alpha x + \beta), f(x), T^{-1} \) in place of \( f(x), f(\alpha x + \beta), T \) shows that \( y \mid \delta \). Thus \( \delta \approx y \), as was to be proved.

When \( C(f(x)) \approx 1 \) but the divisibility conditions in Eisenstein's criterion are not satisfied, we might attempt to find a unit \( \alpha \) and an element \( \beta \) so that \( f(\alpha x + \beta) \) will satisfy the divisibility conditions. If we succeed in finding such \( \alpha, \beta \), then \( f(\alpha x + \beta) \) will be irreducible by Eisenstein's criterion (as \( C(f(\alpha x + \beta)) \approx 1 \) by Lemma 37.3(4)) and \( f(x) \) will be irreducible, too (by Lemma 37.3(3)). This is what we did in Example 37.2(d).

Eisenstein's criterion is a sufficient condition for irreducibility. It is not necessary, even if we extend it using Lemma 37.3(3). That is to say, \( f(x) \) may be irreducible and yet, for all units \( \alpha \) in \( D \) and for all elements \( \beta \) in \( D \), the polynomial \( f(\alpha x + \beta) \) may fail to satisfy the divisibility conditions in Eisenstein's criterion. In fact, a closer study of its proof reveals that we are essentially reading the polynomials mod \( D_p \), i.e., we are taking the images of polynomials in \( D[x] \) under the mapping \( \hat{\psi}: D[x] \rightarrow (D/Dp)[x] \) (see Lemma 33.7).

**37.4 Lemma:** Let \( D \) be an integral domain and let \( K \) be a field. Let \( \psi: D \rightarrow K \) be a ring homomorphism and let \( \hat{\psi}: D \rightarrow K \) be the homomorphism of Lemma 33.7.

(1) If \( f \in D[x] \) and \( f = gh \) with \( g, h \in D[x] \), then \( f \hat{\psi} = g \hat{\psi} h \hat{\psi} \).

(2) If \( f \in D[x] \setminus D \), \( \deg f = \deg f \hat{\psi} \) and \( f \hat{\psi} \) is irreducible in \( K[x] \), then \( f \) has no divisors \( g \) in \( D[x] \) such that \( 0 < \deg g < \deg f \).

**Proof:** (1) This follows from the fact that \( \hat{\psi} \) is a homomorphism.
(2) Suppose, on the contrary, that $f = gh$ in $D[x]$, with $0 < \deg g < \deg f$. Then $\hat{f} = \hat{g}\hat{h}$ by (1). Since $\hat{f}$ is irreducible in $K[x], \hat{f} \neq 0$, so $\hat{g} \neq 0 \neq \hat{h}$ and either $\deg \hat{g} = 0$ or $\deg \hat{h} = 0$. We get then
\[
\deg \hat{f} = \deg \hat{g}\hat{h} = \deg \hat{g} + \deg \hat{h} \\
\leq \deg g + \deg h = \deg gh = \deg f = \deg \hat{f},
\]
which forces $\deg \hat{g} = \deg g$ and $\deg \hat{h} = \deg h$. Thus either $\deg g = 0$ or $\deg h = 0$, and so either $0 = \deg g$ or $\deg g = \deg f$, against our hypothesis $0 < \deg g < \deg f$. 

In Lemma 37.4, we relaxed the hypothesis on $C(f)$ that was imposed in Eisenstein’s criterion. We pay for it, of course. Notice we did not claim that $f$ is irreducible over $D$. We claimed only that $f$ has no proper factor of positive degree less than $\deg f$. Here $f$ may have proper divisors, but any factorization of $f$ in $D[x]$ has the form $f = af_1$, where $a \in D$ and $\deg f_1 = \deg f$.

37.5 Examples: (a) Let $q(x) = x^3 + x + 1 = \overline{1}x^3 + \overline{x} + \overline{1} \in \mathbb{Z}_2[x]$. If $q(x)$ were reducible in $\mathbb{Z}_2[x]$, it would have a factor of degree $\leq 3/2$, so a factor of degree 1. So $q(x)$ would have a root in $\mathbb{Z}_2 = \{0, 1\}$ by the factor theorem (Theorem 35.6). But $q(0) = \overline{1} \neq 0$ and $q(1) = \overline{1} \neq 0$, so $q(x)$ is irreducible in $\mathbb{Z}_2[x]$.

Let $f(x) = x^3 + 2x^2 + x + 7 \in \mathbb{Z}[x]$. Under the mapping $\hat{v}: \mathbb{Z}[x] \to \mathbb{Z}_2[x]$, where $v: \mathbb{Z} \to \mathbb{Z}_2$ is the natural homomorphism, we have
\[
\hat{f} = \overline{1}x^3 + \overline{2}x^2 + \overline{x} + \overline{7} = x^3 + x + 1 = q(x) \in \mathbb{Z}_2[x],
\]
and so $\hat{f}$ is irreducible over $\mathbb{Z}_2$. By Lemma 37.4(2), $f$ has no polynomial divisors of degree 1, nor of degree 2. Since $f$ does not have any divisors of degree 0 either ($C(f) \approx 1$), $f$ is irreducible over $\mathbb{Z}$.

(b) Lemma 37.4 can be useful even if $\hat{f}$ is not irreducible. The factorization of $\hat{f}$ in $K[x]$ gives us information about possible factors of $f$ in $D[x]$ and restricts their number drastically.
As an illustration, consider \( f(x) = x^5 + 5x^4 + 4x^3 + 16x^2 + 8x + 1 \in \mathbb{Z}[x] \).
Under \( \hat{v} : \mathbb{Z}[x] \to \mathbb{Z}_3[x] \), where \( v : \mathbb{Z} \to \mathbb{Z}_3 \) is the natural homomorphism, we have (we drop the bars for ease of notation)
\[
f_\hat{v} = x^5 + 2x^4 + x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]
= (x^2 + 2x + 1)(x^3 + 1)
= (x + 1)^2(x + 1)(x^2 - x + 1)
= (x + 1)^2(x + 1)(x^2 + 2x + 1)
= (x + 1)^5,
\]
so any monic factor \( g \) of \( f \) in \( \mathbb{Z}[x] \) with \( 1 \leq \deg g \leq 2 \) satisfies
\[
g \hat{v} = x + 1 \in \mathbb{Z}_3[x] \quad \text{or} \quad g \hat{v} = (x + 1)^2 \in \mathbb{Z}_3[x]
\]
(\( \mathbb{Z}_3[x] \) is a unique factorization domain).

Does \( f \in \mathbb{Z}[x] \) have a divisor of degree one? If it had, it would have a rational root, and that root would be 1 or \(-1\) by Theorem 35.10. Since \( f(1) = 35 \neq 0 \) and \( f(-1) = 9 \neq 0 \), \( f \) has no rational root, and \( f \) has no divisor of degree one.

Does \( f \in \mathbb{Z}[x] \) have a divisor of degree two? If \( f \) has a monic divisor \( g = g(x) = ax^2 + bx + c \in \mathbb{Z}[x] \) of degree two, then \( g \hat{v} = x^2 + 2x + 1 \in \mathbb{Z}_3[x] \), and so \( a \equiv 1 \), \( b \equiv 2 \), \( c \equiv 1 \) (mod 3). Besides, \( a \) divides the leading coefficient of \( f \), and \( c \) divides the constant term in \( f \); thus \( a|1 \) and \( c|1 \). So \( a = 1 \) and \( c = 1 \). Without restricting generality, we may assume \( a = 1 \). The possible monic factors of \( f \) of second degree are therefore to be found among
\[
g_m(x) = x^2 + (3m + 2)x + 1, \quad h_m(x) = x^2 + (3m + 2)x - 1 \quad (m \in \mathbb{Z}).
\]
We check if any \( g_m \) or \( h_m \) divides \( f \). Supposing \( g_m(x)|f(x) \) in \( \mathbb{Z}[x] \), we get
\[
g_m(1)|f(1) \quad \text{in} \ \mathbb{Z}
3m + 4 \mid 35
3m + 4 \in \{1,5,7,35,-1,-5,-7,-35\}
3m + 4 = 1,7,-5,-35
3m + 2 = -1,5,-7,-37
\]
\[
g_m(x) = x^2 - x + 1 \quad \text{or} \quad x^2 + 5x + 1 \quad \text{or} \quad x^2 - 7x + 1 \quad \text{or} \quad x^2 + 37x + 1.
\]
Testing these four polynomials in turn, we find \( x^2 - x + 1 \) does not divide \( f(x) \), and \( x^2 + 5x + 1 \) divides \( f(x) \); in fact \( f(x) = (x^2 + 5x + 1)(x^3 + 3x + 1) \). [If none of the four polynomials divided \( f(x) \), we would repeat the argument with \( h_m \). In this way, we would find a divisor of \( f(x) \) or we would show that \( f(x) \) is irreducible.]
(c) Lemma 37.4 gives a very elegant proof of Eisenstein’s criterion. In case the underlying ring is a principal ideal domain. Suppose $D$ is a principal ideal domain and
\[ f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \]
is a nonzero polynomial in $D[x]$ with $C(f) \equiv 1$ and $p$ is a prime element $D$ such that
\[ p \mid a_n, \quad p \mid a_{n-1}, \ldots, p \mid a_1, p \mid a_0, \quad p^2 \nmid a_0. \]
Since $p$ is irreducible, the factor ring $D/Dp$ is a field (Theorem 32.25). We can use Lemma 37.4 with the natural homomorphism $\varphi: D \to D/Dp$. The divisibility conditions on the coefficients of $f$ imply
\[ \hat{f} = (a_n \varphi) x^n, \quad a_n \varphi \in D/Dp, \quad a_n \varphi \neq 0. \]
If $f$ had a proper factorization $f = gh$ in $D[x]$, where $0 < \deg g < n$, we would get
\[ g \hat{h} \hat{g} = f \hat{h} = (a_n \varphi) x^n \]
hence $g \hat{h} = b \varphi x^r, h \hat{g} = c \varphi x^s$ with $0 < r < n, 0 < s < n$ and $b \varphi c = a_n \varphi$. Then the constant terms of $g$ and $h$ would be divisible by $p$, and $p^2$ would be divide their product $a_0$, contrary to the hypothesis. Hence $f$ is irreducible over $D$.

The idea (that $g_m(x)|f(x) \Rightarrow g_m(1)|f(1)$) in Example 37.5(b) has been exploited by L. Kronecker (1823-1891). Let $D$ be an integral domain and let $f(x)$ be an arbitrary nonzero polynomial in $D[x]$. To find out whether $f$ is irreducible over $D$, one must check whether $g|f$ or $g \nmid f$ holds for all polynomials $g$ with $\deg g < \deg f$. If $D$ happens to be finite (and thus a field; Theorem 31.1), there are finitely many $g$’s with $\deg g < \deg f$, and the question whether $f$ is irreducible over $D$ can be decided by checking $g|f$ for these the finitely many $g$’s. If $D$ is not finite, this argument does not work, and we must, so it seems, check if $g|f$ for infinitely many polynomials $g \in D[x]$. Kronecker showed that, if $D$ is a unique factorization domain which possesses a finite number of units and if we have a method for finding the irreducible factors of any given nonzero element of $D$, then, to find out whether a given nonzero polynomial is irreducible or not, we need check $g|f$ for only a finite number of polynomials $g$ in $D[x]$. 

447
His idea is that, if \( g(x)/f(x) \) in \( D[x] \), then \( g(a)/f(a) \) in \( D \) for any \( a \in D \), and that a polynomial \( g \) is determined uniquely if its values are known at more than \( \text{deg} \ g \) elements of \( D \) (Lagrange's interpolation formula).

Let \( D \) be an infinite unique factorization domain. Assume there are finitely many units in \( D \), and assume that there is a method for finding the irreducible factors of any given nonzero element of \( D \). Let \( f \) be a nonzero polynomial in \( D[x] \) of degree \( n \). If \( n = 0 \), then \( f \in D \) and we can find the irreducible factors of \( f \) in \( D \) by assumption. If \( n = 1 \), then \( f = cf_1 \), where \( c = C(f) \) and \( f_1 \) is an irreducible polynomial in \( D[x] \). The irreducible factors of \( c \in D \) can be found by assumption, and thus the irreducible factors of \( f \), too, can be found effectively. If \( n \geq 2 \) and \( f \) is reducible, there is a factor \( g \in D[x] \) of \( f \) with \( \text{deg} \ g \leq n/2 \) (Lemma 33.3(3)). We put \( m := \lceil n/2 \rceil \). We take \( m + 1 \) distinct elements \( a_0, a_1, a_2, \ldots, a_m \) from \( D \) and evaluate \( f(a_0), f(a_1), f(a_2), \ldots, f(a_m) \in D \). If any \( f(a_i) \) happens to be \( 0 \in D \), then \( x - a_i \) is a factor of \( f \) (Theorem 35.6). Therefore we may assume that \( f(a_0), f(a_1), f(a_2), \ldots, f(a_m) \) are all distinct from zero. Each one of them has finitely many divisors in \( D \), because \( D \) is a unique factorization domain and \( D \) has finitely many units. There is assumed to be a method of finding those divisors. Let \( N_i \) be the number of factors of \( f(a_i) \). A factor \( g \) of \( f \in D[x] \) with \( \text{deg} \ g \leq m \) satisfies one of the \( N_0 N_1 N_2 \ldots N_m \) systems of equations

\[
g(a_0) = c_0, \quad g(a_1) = c_1, \quad g(a_2) = c_2, \quad \ldots, \quad g(a_m) = c_m,
\]

where \( c_0, c_1, c_2, \ldots, c_m \) run independently over the divisors of the elements \( f(a_0), f(a_1), f(a_2), \ldots, f(a_m) \), respectively. For each one of these \( N_0 N_1 N_2 \ldots N_m \) choices of \( c_0, c_1, c_2, \ldots, c_m \), we build the unique polynomial \( g \) satisfying (†).

This is done by Lagrange's interpolation formula; but this formula requires that the underlying ring be in fact a field. Thus Lagrange's interpolation formula gives us a list of \( N_0 N_1 N_2 \ldots N_m \) polynomials \( g \) in \( F[x] \), where \( F \) is the field of fractions of \( D \), one for each choice \( c_0, c_1, c_2, \ldots, c_m \) of the divisors of \( f(a_0), f(a_1), f(a_2), \ldots, f(a_m) \).

From this list of polynomials, we delete those which are not in \( D[x] \). If any polynomial \( g \) remains, we divide \( f \) by \( g \) in \( F[x] \). Then \( f = qg + r \), with \( q, r \in F[x] \). If \( r \neq 0 \) or \( r = 0 \) but \( q \notin D[x] \), we delete \( g \) from our list. We delete \( g \) from our list also the the polynomials which are units in \( D \). If any polynomial \( g \) survives, it is a factor of \( f \). Otherwise, \( f \) is irreducible over \( D \).
When a proper divisor \( g \) of \( f \) is found in this way, the same procedure can be applied to \( g \) and \( f/g \). Repeating this process, we can find all irreducible factors of \( f \).

\( \mathbb{Z} \) satisfies the conditions imposed on \( D \) in Kronecker's method. Thus the irreducibility of a polynomial in \( \mathbb{Z}[x] \) can be determined effectively. This in turn implies that the irreducibility of a polynomial in \( \mathbb{Z}[x][y] \) can be determined effectively. By repeated application of Kronecker's method, we can always decide whether a given polynomial in \( \mathbb{Z}[x_1,x_2, \ldots, x_n] \) is irreducible or reducible. The same holds for polynomials in the rings \( \mathbb{Z}[i][x_1,x_2, \ldots, x_n] \) and \( \mathbb{Z}[\omega][x_1,x_2, \ldots, x_n] \).

Kronecker's method is very long and very cumbersome in any specific case. However, it is important philosophically, because it assures that the irreducibility or reducibility of a polynomial can be determined effectively in a finite number of steps.

Exercises

1. Using Eisenstein's criterion, show that the following polynomials are irreducible over the rings indicated:
   
   \[
   \begin{align*}
   x^4 - 6x^3 + 24x^2 - 30x + 14 & \quad \text{over } \mathbb{Z}, \\
   x^4 + 6x^3 - 42x^2 + 57x + 78 & \quad \text{over } \mathbb{Z}, \\
   3x^5 + (21 - i)x^4 + (14 - 5i)x^3 + (-10 + 11i) & \quad \text{over } \mathbb{Z}[i], \\
   x^5 - 7x^4 + (3 + 2\omega)x^3 + (2 - \omega)x + (1 - 4\omega) & \quad \text{over } \mathbb{Z}[\omega].
   \end{align*}
   \]

2. Let \( f = x^6 - 2x^5 + 3x^4 - 2x^3 + 3x^2 - 2x + 2 \in \mathbb{Z}[x] \). Either prove that \( f \) is irreducible over \( \mathbb{Z} \) or find all irreducible factors of \( f \) in \( \mathbb{Z}[x] \).

3. Do Ex. 2 for the polynomials \( x^4 - 2x^3 - 2x^2 + 15x + 30 \) and \( x^5 + 8x^4 + 25x^3 + 39x^2 + 30x + 7 \) in \( \mathbb{Z}[x] \).