

§34

Divisibility in Polynomial Domains

We learned in Lemma 33.6 that some properties of a ring R are transferred to the polynomial ring $R[x]$. In particular, if R is an integral domain, so is $R[x]$. In any integral domain, we have a theory of divisibility (§32). In this paragraph, we want to investigate the divisibility properties of polynomials. Lemma 33.6 suggests the questions: Is $R[x]$ a Euclidean domain if R is a Euclidean domain? Is $R[x]$ a principal ideal domain if R is a principal ideal domain? Is $R[x]$ a unique factorization domain if R is a unique factorization domain? The answer to the first two questions is 'no'. For example, $\mathbb{Z}[x]$ is not a principal ideal domain, let alone a Euclidean domain, although \mathbb{Z} is Euclidean. On the other hand, the third question receives an affirmative answer: if R is a unique factorization domain, so is $R[x]$. This will be proved as Theorem 34.13.

Let us recollect the basic definitions. Assume D is an integral domain. Then $D[x]$ is an integral domain (Lemma 33.6). A polynomial $f \in D[x]$ is said to be *divisible* by a nonzero polynomial $g \in D[x]$ if there is a polynomial h in $D[x]$ such that $f = gh$. We write then $g|f$. Notice that the coefficients of h are required to be in D . The notation $g|f$ does not merely mean that $f = gh$ for some arbitrary polynomial h . It means $f = gh$ for some polynomial h **in** $D[x]$.

When $f \neq 0$ and $f = gh$, we have $\deg f = \deg gh = \deg g + \deg h \geq \deg g$:

34.1 Lemma: *Let D be an integral domain. If $g, f \in D[x]$, $g \neq 0 \neq f$ and $g|f$, then,*

$$\deg g \leq \deg f. \quad \square$$

A nonzero polynomial $e \in D[x]$ is a *unit of $D[x]$* if $eh = 1$ for some $h \in D[x]$, or, equivalently, if $e|f$ for all $f \in D[x]$. In this case, Lemma 33.3 yields

$$\begin{aligned} 0 = \deg 1 &= \deg eh = \deg e + \deg h \geq 0 + 0 = 0, \\ \deg e &= 0, \deg h = 0, \end{aligned}$$

$e \in D, \quad h \in D,$
 $eh = 1$ holds in $D,$
 e is a unit in $D.$

($e \neq 0 \neq h$, because $eh = 1 \neq 0$ and D is an integral domain.) So a unit in $D[x]$ is a unit in D : if a polynomial $e = \sum_{i=0}^m a_i x^i$ is a unit in $D[x]$, then $a_0 \in D$ is a unit in D and $a_1 = a_2 = \cdots = a_m = 0$. Conversely, if e is a unit in D so that $eh = 1$ for some $h \in D$, then of course $e, h \in D[x]$ and e is a unit in $D[x]$. We proved the following lemma.

34.2 Lemma: *Let D be an integral domain. Then $e \in D[x]$ is a unit in $D[x]$ if and only if $e \in D$ and e is a unit in D . In symbols, $D[x]^\times = D^\times$. \square*

Thus any unit in $D[x]$ has degree 0 and the associates of a polynomial in $D[x]$ have the same degrees as the polynomial itself. Any proper divisor of $f \in D[x]$ is therefore of degree distinct from 0 and $\deg f$.

A polynomial f in $D[x] \setminus \{0\}$ is irreducible if f is not a unit in $D[x]$ and if, in any factorization of f as $f = gh$ **in** $D[x]$, either g or h is a unit. This is Definition 32.7. We paraphrase this as follows: $f \in D[x] \setminus \{0\}$ is irreducible if $\deg f > 0$ and if there are no polynomials g, h **in** $D[x]$ such that $f = gh$ and $0 < \deg g, \deg h < \deg f$. The phrase "**in** $D[x]$ " is important. Suppose $D \subseteq D_1$, where D_1 is another integral domain. Then $f \in D_1[x]$, too. Now it is possible that

there exist no $g, h \in D[x]$ such that $f = gh, 0 < \deg g < \deg f$

and yet possibly

there exist some $g, h \in D_1[x]$ such that $f = gh, 0 < \deg g < \deg f$.

Then f is irreducible in $D[x]$, but not in $D_1[x]$. This shows that irreducibility of f is not an intrinsic property of f . It is a property of f *relative to* the polynomial domain $D[x]$. For this reason, we have to mention the domain D whenever we speak about irreducible polynomials. We say f is *irreducible over D* when f is irreducible in $D[x]$. For example, $x^2 + 1 \in$

$\mathbb{Q}[x]$ is irreducible over \mathbb{Q} since $x^2 + 1$ has no proper divisors in $\mathbb{Q}[x]$, but $x^2 + 1$ is reducible in $\mathbb{C}[x]$ since $x^2 + 1 = (x - i)(x + i)$, with $x - i, x + i \in \mathbb{C}[x]$ and $0 < 1 = \deg(x - i) < 2 = \deg(x^2 + 1)$.

We now compare the irreducibility of an element of D in D with its irreducibility in $D[x]$.

34.3 Lemma: *Let D be an integral domain and let a be any nonzero element of $D \subseteq D[x]$. Then a is irreducible in $D[x]$ if and only if a is irreducible in D .*

Proof: Suppose that a is irreducible in D . We prove that a is irreducible in $D[x]$. First we must show that a is not a unit in $D[x]$. Since a is irreducible in D , so not a unit in D , we have $a \notin D^\times = D[x]^\times$ (Lemma 34.2), so a is not a unit in $D[x]$. Secondly we must show that $a = bc$, where $b, c \in D[x]$, implies either b or c is a unit in $D[x]$. Indeed, if $a = bc$, then $0 = \deg a = \deg bc = \deg b + \deg c \geq 0$, so $\deg b = 0 = \deg c$. Then $a = bc$ is an equation in D . Since a is irreducible in D , either b or c is a unit in D , so, in view of Lemma 34.2, either b or c is a unit in $D[x]$. This proves that a is irreducible in $D[x]$.

Now the converse. We suppose that a is irreducible in $D[x]$ and show that a is irreducible in D . First we must show that a is not a unit in D . Since a is irreducible in $D[x]$, so not a unit in $D[x]$, we have $a \notin D[x]^\times = D^\times$ (Lemma 34.2), so a is not a unit in D . Secondly we must show that $a = bc$, where $b, c \in D$, implies either b or c is a unit in D . We read $a = bc$ as an equation in $D[x]$. Since a is irreducible in $D[x]$, either b or c is a unit in $D[x]$, so, in view of Lemma 34.2, either b or c is a unit in D . This proves that a is irreducible in D . \square

We want to find the integral domains D such that $D[x]$ is a unique factorization domain. What conditions must be imposed on D ? If $D[x]$ is to be a unique factorization domain, then each element of $D[x] \setminus \{0\}$ that is not a unit in $D[x]$, must be written as a product of irreducible elements of $D[x]$ in a unique way. In particular, each element of $D \setminus \{0\}$ that is not a unit in $D[x]$, must be written as a product of irreducible elements of $D[x]$ in a unique way. As any divisor in $D[x]$ of an element in D belongs to D

by degree considerations, the last statement means (Lemma 34.2, Lemma 34.3): each element of $D \setminus \{0\}$ that is not a unit in D , must be written as a product of irreducible elements of D in a unique way. Thus D must be a unique factorization domain. We shall prove conversely that $D[x]$ is a unique factorization domain whenever D is. The proof will make use of the polynomial ring $F[x]$, where F is the field of fractions of D (§31). $F[x]$ will turn out to be a Euclidean domain.

We show generally that $K[x]$ is a Euclidean domain if K is a field. In order to do that, let us remember, we must find a function $d: K[x] \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$ such that $d(f) \leq d(fg)$ for all $f, g \in K[x] \setminus \{0\}$ and such that, for any nonzero polynomials f, g in $K[x]$, there are polynomials $q, r \in K[x]$ with $f = qg + r$ and $r = 0$ or $\deg r < \deg g$. The degree of polynomials will work as the function d . First we prove a slightly more general theorem.

34.4 Theorem (Division algorithm): *Let D be an integral domain and let f, g be polynomials in $D[x]$. If the leading coefficient of g is a unit in D , then there are unique polynomials q, r in $D[x]$ such that*

$$f = qg + r, \quad r = 0 \text{ or } \deg r < \deg g.$$

Proof: First we prove the existence of q and r . This is nothing but the long division of polynomials. Suppose we divide $f = x^5 - 2x^4 + 3x^3 + x^2 - x + 2$ by $g = x^2 + x + 1$. What do we do? We subtract x^3 times g from f :

$$\begin{array}{r} x^5 - 2x^4 + 3x^3 + x^2 - x + 2 \quad x^2 + x + 1 \\ x^5 + x^4 + x^3 \quad x^3 \\ \hline -3x^4 + 2x^3 + x^2 - x + 2 \end{array}$$

and get the polynomial $f_1 = -3x^4 + 2x^3 + x^2 - x + 2$, whose degree is smaller than the degree of f . Then we subtract $-3x^2$ times g from f_1 and get a polynomial $f_2 = 5x^3 + 4x^2 - x + 2$, whose degree is smaller than the degree of f_1 . We continue this process until we get a polynomial r whose degree is smaller than the degree of $g = x^2 + x + 1$:

$$\begin{array}{r}
x^5 - 2x^4 + 3x^3 + x^2 - x + 2 \quad x^2 + x + 1 \\
x^5 + x^4 + x^3 \qquad \qquad \qquad x^3 - 3x^2 + 5x - 1 \\
\hline
-3x^4 + 2x^3 + x^2 - x + 2 \\
-3x^4 - 3x^3 - 3x^2 \\
\hline
5x^3 + 4x^2 - x + 2 \\
5x^3 + 5x^2 + 5x \\
\hline
-x^2 - 6x + 2 \\
-x^2 - x - 1 \\
\hline
-5x + 3.
\end{array}$$

Hence $f = (x^3 - 3x^2 + 5x - 1)g + (-5x + 3)$. In general, we have

$$\begin{array}{r}
f \\
ax^m g \\
\hline
f_1 = f - ax^m g
\end{array}$$

where a and $m \in \mathbb{N} \cup \{0\}$ are chosen appropriately, and $\deg f_1 < \deg f$. Then, by induction on the degree of f , we can divide f_1 (and hence f) by g and get a remainder r . This is essentially the proof.

Now let f, g be nonzero polynomials in $D[x]$ and suppose that the leading coefficient of g is a unit in D . We prove the existence of q and r by induction on $\deg f$.

I. Induction begins at 0. Suppose $\deg f = 0$. Then $f \in D \setminus \{0\}$. Since the leading coefficient of g is a unit in D by hypothesis, if $g \in D$, there is a $g^{-1} \in D$ such that $g^{-1}g = 1$, hence $fg^{-1} \in D$ and we can write

$$f = (fg^{-1})g + 0$$

If $g \in D[x] \setminus D$, then $\deg g \geq 1$ and we can write

$$f = 0g + f.$$

This proves the existence of q and r with

$$\begin{array}{lll}
q = fg^{-1}, & r = 0 & \text{in case } g \in D, \\
q = 0, & r = f & \text{in case } g \in D[x] \setminus D.
\end{array}$$

II. Now the inductive step. We use the principle of induction in the form 4.5. We assume that $\deg f = n \geq 1$ and that, for any nonzero

polynomial h with $\deg h < n$, there are polynomials q_1 and r_1 in $D[x]$ such that

$$h = q_1 g + r_1, \quad r_1 = 0 \text{ or } \deg r_1 < \deg g.$$

In case $\deg g > n$, we have

$$f = 0g + f \quad \deg f = n < \deg g$$

and this proves the existence of q and r with

$$q = 0, \quad r = f.$$

Having disposed of the case $\deg g > n$, we assume now $\deg g \leq n$. We subtract a suitable multiple of g from f to get a polynomial of degree smaller than n . If, say

$$\begin{aligned} f &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, & g &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0, \\ & & & b_m \text{ is a unit in } D, \\ & & & b_m b_m^{-1} = 1 \text{ for some } b_m^{-1} \in D, \\ & & & m \leq n, \end{aligned}$$

then we put $f_1 := f - a_n b_m^{-1} x^{n-m} g$. Here either $f_1 = 0$ and the the existence of q and r is proved with $q = a_n b_m^{-1} x^{n-m}$, $r = 0$; or

$$\begin{aligned} f_1 &= f - a_n b_m^{-1} x^{n-m} g \\ &= (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0) - a_n b_m^{-1} x^{n-m} (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0) \end{aligned}$$

is a polynomial in $D[x]$ of degree $< n$. By the induction hypothesis, there are polynomials q_1, r_1 in $D[x]$ such that

$$f_1 = q_1 g + r_1, \quad r_1 = 0 \text{ or } \deg r_1 < \deg g.$$

Hence

$$\begin{aligned} f &= f_1 + a_n b_m^{-1} x^{n-m} g \\ &= (q_1 g + r_1) + (a_n b_m^{-1} x^{n-m} g) \\ &= (q_1 + a_n b_m^{-1} x^{n-m}) g + r_1, \quad r_1 = 0 \text{ or } \deg r_1 < \deg g \end{aligned}$$

and this proves the existence of q and r with $q = q_1 + a_n b_m^{-1} x^{n-m}$, $r = r_1$ and completes the proof of the inductive step. The hypothesis that the leading coefficient of g be a unit has been used to construct the f_1 with $\deg f_1 < \deg f$.

The uniqueness of q and r . Suppose

$$f = qg + r = q'g + r'; \quad r = 0 \text{ or } \deg r < \deg g; \quad r' = 0 \text{ or } \deg r' < \deg g.$$

Then $(qg + r) - (q'g + r') = f - f = 0$,

$$(q - q')g = r' - r$$

and the assumption $q - q' \neq 0$ leads to the contradiction

$$\deg g \leq \deg (q - q') + \deg g = \deg (q - q')g$$

$$= \deg(r' - r) \leq \max\{\deg r', \deg r\} < \deg g$$

by Lemma 33.3. This forces $q - q' = 0$, so $q = q'$, so $r = f - qg = f - q'g = r$. Thus q and r are uniquely determined. \square

34.5 Theorem: *Let K be a field.*

(1) *For any nonzero polynomials f, g in $K[x]$, there are unique polynomials q and r in $K[x]$ such that*

$$f = qg + r, \quad r = 0 \text{ or } \deg r < \deg g.$$

(2) *$K[x]$ is a Euclidean domain.*

(3) *$K[x]$ is a unique factorization domain.*

Proof: (1) Since $g \neq 0$, it has a leading coefficient, which is distinct from $0 \in K$. Then the leading coefficient of g is a unit in K (Example 32.6(b)). The assertion follows now from Theorem 34.4.

(2) We prove that $\deg: K[x] \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$ satisfies the conditions in Definition 32.10. Certainly $\deg f$ is a nonnegative integer by definition and $\deg f \leq \deg fg$ for all $f, g \in K[x] \setminus \{0\}$ by Lemma 33.3. This proves the condition (i) in Definition 32.13. The condition (ii) is proved in part (1).

(3) This follows from Theorem 32.22. \square

We record some consequences of Theorem 34.5.

34.6 Theorem: *Let K be a field. Any two polynomials f, g in $K[x]$, not both zero, have a greatest common divisor d in $K[x]$. If d is a greatest common divisor of f and g , then there are polynomials h and l in $K[x]$ such that $d = hf + lg$. Any two greatest common divisors of f and g are associate. In particular, there is one and only one monic greatest common divisor of f and g . (This unique monic greatest common divisor of f and g is sometimes called *the* greatest common divisor of f and g). Any irreducible polynomial in $K[x]$ is prime in $K[x]$ (Definition 32.20). \square*

Theorem 34.5 is very satisfactory. If the underlying ring is a field, then the polynomial domain is a unique factorization domain. We turn our attention to polynomials with coefficients in a unique factorization domain. Let D be a unique factorization domain and let F be the field of fractions of D . We recall that the elements of F are fractions a/b of element $a, b \in D, b \neq 0$. We identify $a \in D$ with $a/1 \in F$ and thus regard D as a subring of F . In this way, $D[x] \subseteq F[x]$. (If you find this and the following discussion too abstract, you may just assume $D = \mathbb{Z}$ and $F = \mathbb{Q}$.)

Let $f \in D[x] \subseteq F[x]$. Now, a priori, f may be irreducible over D and not irreducible over F . See the comments preceding Lemma 34.3. In the case where D is a unique factorization domain and F is the field of fractions of D , it is in fact true that an irreducible polynomial in $D[x]$ is also irreducible in $F[x]$. After some preparation, this will be proved in Lemma 34.11. The hypothesis that D be a unique factorization domain is essential, for otherwise the following definition, which plays an important role in the proof of Lemma 34.11, does not make sense.

34.7 Definition: Let D be a unique factorization domain and let f be any nonzero polynomial in $D[x]$. A greatest common divisor of the coefficients of f is called a *content of f* .

Since greatest common divisors are uniquely determined to within ambiguity among associate elements, any two contents of f are associate. We write $C(f)$ for any content of f . Ignoring the distinction among associate elements, we sometimes call $C(f)$ *the content of f* by abuse of language.

The contents of $f = 2x^4 - 8x^2 + 2x + 6 \in \mathbb{Z}[x]$ and $g = 6x^2 - 9x + 18 \in \mathbb{Z}[x]$ are easily seen to be $C(f) = 2$ and $C(g) = 3$. The content of $fg = 12x^6 - 18x^5 - 12x^4 + 84x^3 - 126x^2 - 18x + 108$ is $C(fg) = 6 = 2 \cdot 3 = C(f)C(g)$. This is an example of a general phenomenon.

34.8 Lemma (Gauss' lemma): Let D be a unique factorization domain and let f, g be arbitrary nonzero polynomials in $D[x]$. Then $C(fg) \approx C(f)C(g)$.

Proof: First we remark that we cannot write $C(fg) = C(f)C(g)$, for contents are unique only up to associate elements.

f and g can be written as $f = C(f)f_1$ and $g = C(g)g_1$, where f_1 and g_1 are polynomials in $D[x]$ with $C(f_1) \approx 1$ and $C(g_1) \approx 1$. Similarly $fg = C(fg)h$, where $h \in D[x]$ and $C(h) \approx 1$. We have

$$\begin{aligned} C(f)f_1 \cdot C(g)g_1 &= fg = C(fg)h \\ C(f)C(g)f_1g_1 &= C(fg)h. \end{aligned}$$

Taking contents of both sides and observing $C(al) \approx aC(l)$ for $a \in D \setminus \{0\}$ and $l \in D[x] \setminus \{0\}$, we obtain

$$\begin{aligned} C(f)C(g)C(f_1g_1) &\approx C(fg)C(h) \\ C(f)C(g)C(f_1g_1) &\approx C(fg) \end{aligned}$$

and the theorem will be proved if we can show $C(f_1g_1) \approx 1$. Dropping the subscripts, we must prove:

$$\text{if } C(f) \approx 1 \text{ and } C(g) \approx 1, \text{ then } C(fg) \approx 1.$$

Suppose now $C(f) \approx 1$, $C(g) \approx 1$ and $C(fg)$ is not a unit. Then there is an *irreducible* element π in D with $\pi | C(fg)$. Since $C(f) \approx 1$ and $C(g) \approx 1$ by assumption, π cannot divide all the coefficients of

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

nor of

$$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0,$$

say. Let a_h be the coefficient of f with the largest index that is not divisible by π and let b_k have a similar meaning for g . Then

$$(1) \quad \begin{aligned} \pi | a_n, \pi | a_{n-1}, \dots, \pi | a_{h+1}, \pi \nmid a_h \\ \pi | b_m, \pi | b_{m-1}, \dots, \pi | b_{k+1}, \pi \nmid b_k. \end{aligned}$$

(2)

But π divides the coefficient

$$(\cdots + a_{h+2}b_{k-2} + a_{h+1}b_{k-1}) + a_h b_k + [a_{h-1}b_{k+1} + a_{h-2}b_{k+2} + \cdots]$$

of x^{h+k} in fg . Because of (1) and (2), π divides the expressions in () and []. So π divides $a_h b_k$ as well. Thus $\pi \nmid a_h$, $\pi \nmid b_m$ and $\pi | a_h b_k$, which tells us that π is not a prime element in D . On the other hand, D is a unique factorization domain and every irreducible element in D is prime (Lemma 32.24), hence π is prime. This is a contradiction. We conclude $C(fg) \approx 1$. \square

34.9 Lemma: Let D be a unique factorization domain and let F be the field of fractions of D . Let f, g be any nonzero polynomials in $D[x]$ with

$C(f) \approx C(g)$. Then f and g are associate in $F[x]$ if and only if f and g are associate in $D[x]$.

Proof: By Lemma 34.2,

$$\begin{aligned} e \text{ is a unit in } D[x] &\iff e \text{ is a unit in } D, \\ u \text{ is a unit in } F[x] &\iff u \text{ is a unit in } F \iff u \in F \setminus \{0\}. \end{aligned}$$

If f and g are associate in $D[x]$, then $f = eg$ for some unit e in $D[x]$. Then e is a unit in D , so e is a nonzero element of D , so e is a nonzero element of F , so e is a unit in F , so e is a unit in $F[x]$, so f and g are associate in $F[x]$.

If f and g are associate in $F[x]$, then $f = ug$ for some unit u in $F[x]$. Thus $u \in F \setminus \{0\}$ and so $u = a/b$, where $a, b \in D \setminus \{0\}$. So $bf = ag$. Thus

$$bC(f) \approx C(bf) \approx C(ag) \approx aC(g) \approx aC(f)$$

and $b \approx a$ in D . So $a/b = u$ is a unit in D . Hence u is a unit in $D[x]$ and f is associate to g in $D[x]$. \square

34.10 Lemma: Let D be a unique factorization domain and let F be the field of fractions of D . Let f be a nonzero polynomial in $D[x]$ with $C(f) \approx 1$ and assume

$$f = g_1 g_2 \cdots g_r$$

where g_1, g_2, \dots, g_r are polynomials in $F[x]$. Then there are polynomials h_1, h_2, \dots, h_r in $D[x]$ such that g_i is associate to h_i in $F[x]$ and $C(h_i) \approx 1$ (for all $i = 1, 2, \dots, r$) and

$$f = h_1 h_2 \cdots h_r$$

Proof: The coefficients of g_1, g_2, \dots, g_r are fractions of elements from D . We multiply each g_i by an appropriate element a_i in D , for example by the product of the "denominators" in the coefficients of g_i to get a polynomial $k_i \in D[x]$. Thus $a_i g_i = k_i \in D[x]$. We write $k_i = c_i h_i$, where $c_i \approx C(k_i) \in D$ and h_i is a polynomial in $D[x]$ with $C(h_i) \approx 1$. We have

$$a_1 a_2 \cdots a_r f = a_1 g_1 a_2 g_2 \cdots a_r g_r = k_1 k_2 \cdots k_r = c_1 c_2 \cdots c_r h_1 h_2 \cdots h_r$$

and, taking contents of both sides, and using Lemma 34.8 $r - 1$ times, we get

$$a_1 a_2 \cdots a_r C(f) = c_1 c_2 \cdots c_r C(h_1) C(h_2) \cdots C(h_r)$$

$$a_1 a_2 \cdots a_r \approx c_1 c_2 \cdots c_r.$$

Thus $e := c_1 c_2 \dots c_r / a_1 a_2 \dots a_r$ is a unit in D and

$$f = (eh_1)h_2 \dots h_r.$$

Observe that $h_i = (a_i/c_i)g_i$ is associate to g_i in $F[x]$, because $a_i/c_i \in F \setminus \{0\}$ is a unit in $F[x]$. When we make a slight change of notation and write h_1 for eh_1 , the proof is complete (eh_1 is also associate to g_1 in $F[x]$). \square

34.11 Lemma: *Let D be a unique factorization domain and let F be the field of fractions of D . Let f be a nonzero polynomial in $D[x]$ with $C(f) \approx 1$. Then f is irreducible in $F[x]$ if and only if f is irreducible in $D[x]$.*

Proof: Assume first that f is irreducible in $F[x]$. Then f is not a unit in $F[x]$, hence $\deg f \geq 1$, hence f is not a unit in $D[x]$. Also, if $g, h \in D[x]$ and $f = gh$, we read this equation in $F[x]$ and conclude that either g or h is associate to f in $F[x]$. We know $1 \approx C(f) \approx C(gh) \approx C(g)C(h)$, so $C(g) \approx 1 \approx C(f)$ and $C(h) \approx 1 \approx C(f)$. Using Lemma 34.9, we deduce that either g or h is associate to f in $D[x]$. Thus f is not a unit in $D[x]$ and has no proper divisors in $D[x]$. This means f is irreducible in $D[x]$.

Conversely, assume that f is irreducible in $D[x]$. Then f is not a unit in $D[x]$ and so not a unit in D . This gives $\deg f \geq 1$, for otherwise $f \approx C(f) \approx 1$ would be a unit in D . So $\deg f \geq 1$ and f is not a unit in $F[x]$. We now want to show that f has no proper divisors in $F[x]$. Assume $f = g_1 g_2$, where $g_1, g_2 \in F[x]$. By Lemma 34.10, $f = h_1 h_2$, where $h_1, h_2 \in D[x]$, $C(h_1) \approx 1 \approx C(f)$, $C(h_2) \approx 1 \approx C(f)$ and g_1, g_2 are respectively associate to h_1, h_2 in $F[x]$. Since f is irreducible in $D[x]$, either h_1 or h_2 is associate to f in $D[x]$ and thus, by Lemma 34.9, either h_1 or h_2 is associate to f in $F[x]$, hence either g_1 or g_2 is associate to f in $F[x]$. Thus f has no proper divisors in $F[x]$ and f is irreducible in $F[x]$. \square

We need one more lemma to prove that $D[x]$ is a unique factorization domain whenever D is. It comprises the main argument.

34.12 Lemma: Let D be a unique factorization domain and let f be a nonzero polynomial in $D[x]$ such that $C(f) \approx 1$ and $\deg f \geq 1$. Then f can be written as a product of irreducible polynomials in a unique way.

Proof: Let F be the field of fractions of D . We will use the fact that $F[x]$ is a unique factorization domain and the fact that irreducibility in $D[x]$ and in $F[x]$ coincide (Theorem 34.5, Lemma 34.11).

Consider f as a polynomial in $F[x]$. By Theorem 34.5,

$$f = g_1 g_2 \cdots g_r \quad g_1, g_2, \dots, g_r \in F[x]$$

where g_1, g_2, \dots, g_r are irreducible in $F[x]$. According to Lemma 34.10,

$$f = h_1 h_2 \cdots h_r \quad h_1, h_2, \dots, h_r \in D[x]$$

for some polynomials h_i in $D[x]$ with $C(h_i) \approx 1$ and h_i is associate to g_i in $F[x]$ ($i = 1, 2, \dots, r$). Hence h_i is irreducible in $F[x]$ and, by Lemma 34.11, h_i is also irreducible in $D[x]$. We proved that f can be written as a product of irreducible polynomials in $D[x]$.

Now uniqueness (up to the order of factors and ambiguity among associate polynomials). Let $f \in D[x]$ with $C(f) \approx 1$ and $\deg f \geq 1$, and let

$$f = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad p_i, q_j \in D[x]$$

(1)

be two representations of f as a product of irreducible polynomials

$p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ in $D[x]$. Taking contents and using Lemma 34.8, we get

$$C(p_1)C(p_2)\cdots C(p_r) \approx C(f) \approx 1 \approx C(q_1)C(q_2)\cdots C(q_s)$$

so that $C(p_i)$ and $C(q_s)$ are units in D . By Lemma 34.11, the polynomials p_i, q_j are irreducible in $F[x]$. Since $F[x]$ is a unique factorization domain, we deduce from (1) that $r = s$ and, eventually after reindexing the polynomials, p_i is associate to q_i in $F[x]$. Since $C(p_i) \approx C(q_i)$, Lemma 34.9 tells us that p_i is associate to q_i in $D[x]$ ($i = 1, 2, \dots, r$). This completes the proof. \square

34.13 Theorem: *If D is a unique factorization domain, then $D[x]$ is a unique factorization domain.*

Proof: Given any nonzero polynomial f in $D[x]$ which is not a unit in $D[x]$, we have to show that f can be written as a product of irreducible polynomials in $D[x]$, and that this representation is unique up to the order of factors and ambiguity between associate polynomials.

Now let $f \in D[x], f \neq 0, f \neq \text{unit in } D[x]$. If $\deg f = 0$, then $f \in D$ and, since D is a unique factorization domain, f can be written as a product of irreducible elements p_1, p_2, \dots, p_r of D . These elements are uniquely determined, and they are irreducible also in $D[x]$ (Lemma 34.3). So f can be written as a product of irreducible elements in a unique way if $\deg f = 0$.

Suppose next $\deg f \geq 1$. We write $f = cf_1$, where $c \approx C(f) \in D$ and $f_1 \in D[x]$ with $C(f_1) \approx 1, \deg f_1 \geq 1$. Here c and f_1 are uniquely determined up to a unit in D . Now $c \in D$ can be written as a product of irreducible elements in D , which are also irreducible in $D[x]$:

$$c = a_1 a_2 \dots a_r \quad a_i \text{ are irreducible in } D[x],$$

and a_i are uniquely determined. By Lemma 34.12, f_1 can be written as a product of irreducible polynomials in $D[x]$:

$$f_1 = q_1 q_2 \dots q_s \quad q_j \text{ are irreducible in } D[x]$$

and q_j are uniquely determined. Hence

$$f = a_1 a_2 \dots a_r q_1 q_2 \dots q_s$$

is a product of the irreducible polynomials a_i, q_j in $D[x]$, which are unique up to the order of factors and ambiguity between associate elements. \square

By repeated application of Theorem 34.13, we get

34.14 Theorem: *If D is a unique factorization domain, then $D[x_1, x_2, \dots, x_n]$ is a unique factorization domain.*

\square

In particular,

34.15 Theorem: *If K is a field, then $K[x_1, x_2, \dots, x_n]$ is a unique factorization domain.* □

Exercises

1. Prove that $x^4 + 1 \in \mathbb{Z}[x]$ is irreducible over \mathbb{Z} by comparing the coefficients of both sides in a hypothetical factorization $x^4 + 1 = fg$ and deriving a contradiction from it. Investigate the cases $\deg f = 1$, $\deg g = 3$ and $\deg f = 2 = \deg g$ separately.

2. Do Ex. 1 for $x^4 + 2$ and $x^4 + 3 \in \mathbb{Z}[x]$.

3. Show that $x^4 + 4$ is reducible over \mathbb{Z} .

4. Show that $x^4 + 1 \in \mathbb{Z}_2[x]$ is reducible over \mathbb{Z}_2 .

5. Show that $x^4 + 1 \in (\mathbb{Z}[\sqrt{2}])[x]$ is reducible over $\mathbb{Z}[\sqrt{2}]$ (see §32, Ex. 3).

6. Find a content of

$$(a) \quad 65x^4 + 26x^2 - 9x + 143 \quad \in \mathbb{Z}[x]$$

$$(b) \quad (5 + i)x^3 + (-1 + 5i)x + (-4 + 7i) \quad \in (\mathbb{Z}[i])[x]$$

$$(c) \quad (1 + \omega)x^4 + (-1 + 2\omega)x^3 + (1 - 2\omega)x^2 + 3x + (2 + 3\omega) \quad \in$$

$(\mathbb{Z}[\omega])[x]$

$$(d) \quad 8x^4 + 24x^3 - 32x^2 - 48x + 56 \quad \in \mathbb{Q}[x]$$

$$(e) \quad \bar{3}x^2 + \bar{5}x + \bar{7} \quad \in \mathbb{Z}_{97}[x].$$

7. Let D be a unique factorization domain and let F be the field of fractions of D . Let $f \in D[x]$ be a nonzero polynomial whose leading coefficient is a unit in D . Suppose that $g, h \in F[x]$ and $f = gh$. Prove that then $g \in D[x]$ and $h \in D[x]$.

8. Let D be a unique factorization domain and let $f, g \in D[x] \setminus D$. Prove that a greatest common divisor of f and g has degree ≥ 1 if and only if there are polynomials h, k in $D[x]$ satisfying $\deg h < \deg g$ and $\deg k < \deg f$ such that $fh = gk$.