Proof We have seen that all ideals in $\mathbb{Z}$ are of the form $n\mathbb{Z} = \langle n \rangle$ for $n \in \mathbb{Z}$. Thus $\mathbb{Z}$ is a PID, and Theorem 34.18 applies. ◆

It is worth noting that the proof that $\mathbb{Z}$ is a PID was really way back in Corollary 6.7. We proved Theorem 6.6 by using the division algorithm for $\mathbb{Z}$ exactly as we proved, in Theorem 31.24, that $F[x]$ is a PID by using the division algorithm for $F[x]$. In Section 35, we shall examine this parallel more closely.

If D Is a UFD, Then $D[x]$ Is a UFD

We now start the proof of Theorem 34.30, our second main result for this section. The idea of the argument is as follows. Let D be a UFD. We can form a field of quotients F of D. Then $F[x]$ is a UFD by Theorem 28.21, and we shall show that we can recover a factorization for $f(x) \in D[x]$ from its factorization in $F[x]$. It will be necessary to compare the irreducibles in $F[x]$ with those in $D[x]$, of course. This approach, which we prefer as more intuitive than some more efficient modern ones, is essentially due to Gauss.

34.20 Definition Let D be a UFD and let $a_1, a_2, \cdots, a_n$ be nonzero elements of D. An element d of D is a **greatest common divisor** (abbreviated gcd) **of all of the** a_i if $d \mid a_i$ for $i = 1, \cdots, n$ and any other $d' \in D$ that divides all the a_i also divides d. ■

In this definition, we called d "a" gcd rather than "the" gcd because gcd's are only defined up to units. Suppose that d and d' are two gcd's of a_i for $i = 1, \cdots, n$. Then $d \mid d'$ and $d' \mid d$ by our definition. Thus $d = q'd'$ and $d' = qd$ for some $q, q' \in D$, so $1d = q'qd$. By cancellation in D, we see that $q'q = 1$ so q and q' are indeed units.

The technique in the example that follows shows that gcd's exist in a UFD.

34.21 Example Let us find a gcd of 420, -168, and 252 in the UFD $\mathbb{Z}$. Factoring, we obtain $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, $-168 = 2^3 \cdot (-3) \cdot 7$, and $252 = 2^2 \cdot 3^2 \cdot 7$. We choose one of these numbers, say 420, and find the highest power of each of its irreducible factors (up to associates) that divides all the numbers, 420, -168, and 252 in our case. We take as gcd the product of these highest powers of irreducibles. For our example, these powers of irreducible factors of 420 are $2^2, 3^1, 5^0$, and 7^1 so we take as gcd $d = 4 \cdot 3 \cdot 1 \cdot 7 = 84$. The only other gcd of these numbers in $\mathbb{Z}$ is -84, because 1 and -1 are the only units. ▲

Execution of the technique in Example 34.21 depends on being able to factor an element of a UFD into a product of irreducibles. This can be a tough job, even in $\mathbb{Z}$. Section 35 will exhibit a technique, the Euclidean Algorithm, that will allow us to find gcd's without factoring in a class of UFD's that includes $\mathbb{Z}$ and $F[x]$ for a field F.

34.22 Definition Let D be a UFD. A nonconstant polynomial

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

in $D[x]$ is **primitive** if 1 is a gcd of the a_i for $i = 0, 1, \cdots, n$. ■

34.23 Example In $\mathbb{Z}[x]$, $4x^2 + 3x + 2$ is primitive, but $4x^2 + 6x + 2$ is not, since 2, a nonunit in $\mathbb{Z}$, is a common divisor of 4, 6, and 2. ▲

Observe that every nonconstant irreducible in $D[x]$ must be a primitive polynomial.

34.24 Lemma If D is a UFD, then for every nonconstant $f(x) \in D[x]$ we have $f(x) = (c)g(x)$, where $c \in D, g(x) \in D[x]$, and $g(x)$ is primitive. The element c is unique up to a unit factor in D and is the **content of** $f(x)$. Also $g(x)$ is unique up to a unit factor in D.

Proof Let $f(x) \in D[x]$ be given where $f(x)$ is a nonconstant polynomial with coefficients $a_0, a_1, \cdots, a_n$. Let c be a gcd of the a_i for $i = 0, 1, \cdots, n$. Then for each i, we have $a_i = cq_i$ for some $q_i \in D$. By the distributive law, we have $f(x) = (c)g(x)$, where no irreducible in D divides all of the coefficients $q_0, q_1, \cdots, q_n$ of $g(x)$. Thus $g(x)$ is a primitive polynomial.

For uniqueness, if also $f(x) = (d)h(x)$ for $d \in D, h(x) \in D[x]$, and $h(x)$ primitive, then each irreducible factor of c must divide d and conversely. By setting $(c)g(x) = (d)h(x)$ and canceling irreducible factors of c into d, we arrive at $(u)g(x) = (v)h(x)$ for a unit $u \in D$. But then v must be a unit of D or we would be able to cancel irreducible factors of v into u. Thus u and v are both units, so c is unique up to a unit factor. From $f(x) = (c)g(x)$, we see that the primitive polynomial $g(x)$ is also unique up to a unit factor. ◆

34.25 Example In $\mathbb{Z}[x]$,

$$4x^2 + 6x - 8 = (2)(2x^2 + 3x - 4),$$

where $2x^3 + 3x - 4$ is primitive. ▲

34.26 Lemma **(Gauss's Lemma)** If D is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive.

Proof Let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

and

$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

be primitive in $D[x]$, and let $h(x) = f(x)g(x)$. Let p be an irreducible in D. Then p does not divide all a_i and p does not divide all b_j, since $f(x)$ and $g(x)$ are primitive. Let a_r be the first coefficient of $f(x)$ not divisible by p; that is, $p \mid a_i$ for $i < r$, but $p \nmid a_r$ (that is, p does not divide a_r). Similarly, let $p \mid b_j$ for $j < s$, but $p \nmid b_s$. The coefficient of x^{r+s} in $h(x) = f(x)g(x)$ is

$$c_{r+s} = (a_0b_{r+s} + \cdots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0).$$

Now $p \mid a_i$ for $i < r$ implies that

$$p \mid (a_0b_{r+s} + \cdots + a_{r-1}b_{s+1}),$$

and also $p \mid b_j$ for $j < s$ implies that

$$p \mid (a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0).$$

But p does not divide a_r or b_s, so p does not divide a_rb_s, and consequently p does not divide c_{r+s}. This shows that given an irreducible $p \in D$, there is some coefficient of $f(x)g(x)$ not divisible by p. Thus $f(x)g(x)$ is primitive. ◆

34.27 Corollary If D is a UFD, then a finite product of primitive polynomials in $D[x]$ is again primitive.

Proof This corollary follows from Lemma 34.26 by induction. ◆

Now let D be a UFD and let F be a field of quotients of D. By Theorem 28.21, $F[x]$ is a UFD. As we said earlier, we shall show that $D[x]$ is a UFD by carrying a factorization in $F[x]$ of $f(x) \in D[x]$ back into one in $D[x]$. The next lemma relates the nonconstant irreducibles of $D[x]$ to those of $F[x]$. This is the last important step.

34.28 Lemma Let D be a UFD and let F be a field of quotients of D. Let $f(x) \in D[x]$, where (degree $f(x)) > 0$. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.

Proof Suppose that a nonconstant $f(x) \in D[x]$ factors into polynomials of lower degree in $F[x]$, that is,

$$f(x) = r(x)s(x)$$

for $r(x), s(x) \in F[x]$. Then since F is a field of quotients of D, each coefficient in $r(x)$ and $s(x)$ is of the form a/b for some $a, b \in D$. By clearing denominators, we can get

$$(d)f(x) = r_1(x)s_1(x)$$

for $d \in D$, and $r_1(x), s_1(x) \in D[x]$, where the degrees of $r_1(x)$ and $s_1(x)$ are the degrees of $r(x)$ and $s(x)$, respectively. By Lemma 34.24, $f(x) = (c)g(x)$, $r_1(x) = (c_1)r_2(x)$, and $s_1(x) = (c_2)s_2(x)$ for primitive polynomials $g(x)$, $r_2(x)$, and $s_2(x)$, and $c, c_1, c_2 \in D$. Then

$$(dc)g(x) = (c_1c_2)r_2(x)s_2(x),$$

and by Lemma 34.26, $r_2(x)s_2(x)$ is primitive. By the uniqueness part of Lemma 34.24, $c_1c_2 = dcu$ for some unit u in D. But then

$$(dc)g(x) = (dcu)r_2(x)s_2(x),$$

so

$$f(x) = (c)g(x) = (cu)r_2(x)s_2(x).$$

We have shown that if $f(x)$ factors nontrivially in $F[x]$, then $f(x)$ factors nontrivially into polynomials of the same degrees in $D[x]$. Thus if $f(x) \in D[x]$ is irreducible in $D[x]$, it must be irreducible in $F[x]$.

A nonconstant $f(x) \in D[x]$ that is primitive in $D[x]$ and irreducible in $F[x]$ is also irreducible in $D[x]$, since $D[x] \subseteq F[x]$. ◆

Lemma 34.28 shows that if D is a UFD, the irreducibles in $D[x]$ are precisely the irreducibles in D, together with the nonconstant primitive polynomials that are irreducible in $F[x]$, where F is a field of quotients of $D[x]$.

The preceding lemma is very important in its own right. This is indicated by the following corollary, a special case of which was our Theorem 28.12. (We admit that it does not seem very sensible to call a special case of a corollary of a lemma a theorem. The label assigned to a result depends somewhat on the context in which it appears.)

34.29 Corollary If D is a UFD and F is a field of quotients of D, then a nonconstant $f(x) \in D[x]$ factors into a product of two polynomials of lower degrees r and s in $F[x]$ if and only if it has a factorization into polynomials of the same degrees r and s in $D[x]$.

Proof It was shown in the proof of Lemma 34.28 that if $f(x)$ factors into a product of two polynomials of lower degree in $F[x]$, then it has a factorization into polynomials of the same degrees in $D[x]$ (see the next-to-last sentence of the first paragraph of the proof).

The converse holds since $D[x] \subseteq F[x]$. ◆

We are now prepared to prove our main theorem.

34.30 Theorem If D is a UFD, then $D[x]$ is a UFD.

Proof Let $f(x) \in D[x]$, where $f(x)$ is neither 0 nor a unit. If $f(x)$ is of degree 0, we are done, since D is a UFD. Suppose that $(\text{degree } f(x)) > 0$. Let

$$f(x) = g_1(x)g_2(x) \cdots g_r(x)$$

be a factorization of $f(x)$ in $D[x]$ having the greatest number r of factors of positive degree. (There is such a greatest number of such factors because r cannot exceed the degree of $f(x)$.) Now factor each $g_i(x)$ in the form $g_i(x) = c_ih_i(x)$ where c_i is the content

of $g_i(x)$ and $h_i(x)$ is a primitive polynomial. Each of the $h_i(x)$ is irreducible, because if it could be factored, none of the factors could lie in D, hence all would have positive degree leading to a corresponding factorization of $g_i(x)$, and then to a factorization of $f(x)$ with more than r factors of positive degree, contradicting our choice of r. Thus we now have

$$f(x) = c_1 h_1(x) c_2 h_2(x) \cdots c_r h_r(x)$$

where the $h_i(x)$ are irreducible in $D[x]$. If we now factor the c_i into irreducibles in D, we obtain a factorization of $f(x)$ into a product of irreducibles in $D[x]$.

The factorization of $f(x) \in D[x]$, where $f(x)$ has degree 0, is unique since D is a UFD; see the comment following Lemma 34.28. If $f(x)$ has degree greater than 0, we can view any factorization of $f(x)$ into irreducibles in $D[x]$ as a factorization in $F[x]$ into units (that is, the factors in D) and irreducible polynomials in $F[x]$ by Lemma 34.28. By Theorem 28.21, these polynomials are unique, except for possible constant factors in F. But as an irreducible in $D[x]$, each polynomial of degree >0 appearing in the factorization of $f(x)$ in $D[x]$ is primitive. By the uniqueness part of Lemma 34.24, this shows that these polynomials are unique in $D[x]$ up to unit factors, that is, associates. The product of the irreducibles in D in the factorization of $f(x)$ is the content of $f(x)$, which is again unique up to a unit factor by Lemma 34.24. Thus all irreducibles in $D[x]$ appearing in the factorization are unique up to order and associates. ◆

34.31 Corollary If F is a field and $x_1, \cdots, x_n$ are indeterminates, then $F[x_1, \cdots, x_n]$ is a UFD.

Proof By Theorem 28.21, $F[x_1]$ is a UFD. By Theorem 34.30, so is $(F[x_1])[x_2] = F[x_1, x_2]$. Continuing in this procedure, we see (by induction) that $F[x_1, \cdots, x_n]$ is a UFD. ◆

We have seen that a PID is a UFD. Corollary 34.31 makes it easy for us to give an example that shows that *not every* UFD *is a* PID.

34.32 Example Let F be a field and let x and y be indeterminates. Then $F[x, y]$ is a UFD by Corollary 34.30. Consider the set N of all polynomials in x and y in $F[x, y]$ having constant term 0. Then N is an ideal, but not a principal ideal. Thus $F[x, y]$ is not a PID. ▲

Another example of a UFD that is not a PID is $\mathbb{Z}[x]$, as shown in Exercise 12, Section 35.

EXERCISES 34

Computations

In Exercises 1 through 8, determine whether the element is an irreducible of the indicated domain.

1. 5 in $\mathbb{Z}$

2. -17 in $\mathbb{Z}$

3. 14 in $\mathbb{Z}$

4. $2x - 3$ in $\mathbb{Z}[x]$

5. $2x - 10$ in $\mathbb{Z}[x]$

6. $2x - 3$ in $\mathbb{Q}[x]$

7. $2x - 10$ in $\mathbb{Q}[x]$

8. $2x - 10$ in $\mathbb{Z}_{11}[x]$

9. If possible, give four different associates of $2x - 7$ viewed as an element of $\mathbb{Z}[x]$; of $\mathbb{Q}[x]$; of $\mathbb{Z}_{11}[x]$.

10. Factor the polynomial $4x^2 - 4x + 8$ into a product of irreducibles viewing it as an element of the integral domain $\mathbb{Z}[x]$; of the integral domain $\mathbb{Q}[x]$; of the integral domain $\mathbb{Z}_{11}[x]$.

In Exercises 11 through 13, find all gcd's of the given elements of $\mathbb{Z}$.

11. 234, 3250, 1690

12. 784, -1960, 448

13. 2178, 396, 792, 594

In Exercises 14 through 17, express the given polynomial as the product of its content with a primitive polynomial in the indicated UFD.

14. $18x^2 - 12x + 48$ in $\mathbb{Z}[x]$

15. $18x^2 - 12x + 48$ in $\mathbb{Q}[x]$

16. $2x^2 - 3x + 6$ in $\mathbb{Z}[x]$

17. $2x^2 - 3x + 6$ in $\mathbb{Z}_7[x]$

Concepts

In Exercises 18 through 20, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

18. Two elements a and b in an integral domain D are *associates* in D if and only if their quotient a/b in D is a unit.

19. An element of an integral domain D is an *irreducible* of D if and only if it cannot be factored into a product of two elements of D.

20. An element of an integral domain D is a *prime* of D if and only if it cannot be factored into a product of two smaller elements of D.

21. Determine whether each of the following is true or false.

a. Every field is a UFD.

b. Every field is a PID.

c. Every PID is a UFD.

d. Every UFD is a PID.

e. $\mathbb{Z}[x]$ is a UFD.

f. Any two irreducibles in any UFD are associates.

g. If D is a PID, then $D[x]$ is a PID.

h. If D is a UFD, then $D[x]$ is a UFD.

i. In any UFD, if $p \mid a$ for an irreducible p, then p itself appears in every factorization of a.

j. A UFD has no divisors of 0.

22. Let D be a UFD. Describe the irreducibles in $D[x]$ in terms of the irreducibles in D and the irreducibles in $F[x]$, where F is a field of quotients of D.

23. Lemma 34.28 states that if D is a UFD with a field of quotients F, then a nonconstant irreducible $f(x)$ of $D[x]$ is also an irreducible of $F[x]$. Show by an example that a $g(x) \in D[x]$ that is an irreducible of $F[x]$ need not be an irreducible of $D[x]$.

24. All our work in this section was restricted to integral domains. Taking the same definition in this section but for a commutative ring with unity, consider factorizations into irreducibles in $\mathbb{Z} \times \mathbb{Z}$. What can happen? Consider in particular $(1, 0)$.

Theory

25. Prove that if p is a prime in an integral domain D, then p is an irreducible.

26. Prove that if p is an irreducible in a UFD, then p is a prime.

27. For a commutative ring R with unity show that the relation $a \sim b$ if a is an associate of b (that is, if $a = bu$ for u a unit in R) is an equivalence relation on R.

28. Let D be an integral domain. Exercise 39, Section 22 showed that $\langle U, \cdot \rangle$ is a group where U is the set of units of D. Show that the set $D^* - U$ of nonunits of D excluding 0 is closed under multiplication. Is this set a group under the multiplication of D?

29. Let D be a UFD. Show that a nonconstant divisor of a primitive polynomial in $D[x]$ is again a primitive polynomial.

30. Show that in a PID, every proper ideal is contained in a maximal ideal. [*Hint:* Use Lemma 34.10.]

31. Factor $x^3 - y^3$ into irreducibles in $\mathbb{Q}[x, y]$ and prove that each of the factors is irreducible.

There are several other concepts often considered that are similar in character to the ascending chain condition on ideals in a ring. The following three exercises concern some of these concepts.