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 45.27. By Theorem 23.20, 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 45.23, 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 45.23. Thus all irreducibles in $D[x]$ appearing in the factorization are unique up to order and associates. ◆

45.30 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 23.20, $F[x_1]$ is a UFD. By Theorem 45.29, 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 45.30 makes it easy for us to give an example that shows that *not every* UFD *is a* PID.

45.31 Example Let F be a field and let x and y be indeterminates. Then $F[x, y]$ is a UFD by Corollary 45.30. 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 46.

EXERCISES 45

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. Mark each of the following 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 | 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 45.26 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 37, Section 18 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 ideal is contained in a maximal ideal. [*Hint:* Use Lemma 45.10.]

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.

32. Let R be any ring. The **ascending chain condition** (ACC) **for ideals** holds in R if every strictly increasing sequence $N_1 \subset N_2 \subset N_3 \subset \cdots$ of ideals in R is of finite length. The **maximum condition** (MC) **for ideals** holds in R if every nonempty set S of ideals in R contains an ideal not properly contained in any other ideal of the set S. The **finite basis condition** (FBC) **for ideals** holds in R if for each ideal N in R, there is a finite set $B_N = \{b_1, \cdots, b_n\} \subseteq N$ such that N is the intersection of all ideals of R containing B_N. The set B_N is a **finite generating set for** N.

Show that for every ring R, the conditions ACC, MC, and FBC are equivalent.

33. Let R be any ring. The **descending chain condition** (DCC) **for ideals** holds in R if every strictly decreasing sequence $N_1 \supset N_2 \supset N_3 \supset \cdots$ of ideals in R is of finite length. The **minimum condition** (mC) **for ideals** holds in R if given any set S of ideals of R, there is an ideal of S that does not properly contain any other ideal in the set S.

Show that for every ring, the conditions DCC and mC are equivalent.

34. Give an example of a ring in which ACC holds but DCC does not hold. (See Exercises 32 and 33.)

SECTION 46 EUCLIDEAN DOMAINS

We have remarked several times on the importance of division algorithms. Our first contact with them was the *division algorithm for* $\mathbb{Z}$ in Section 6. This algorithm was immediately used to prove the important theorem that a subgroup of a cyclic group is cyclic, that is, has a single generator. Of course, this shows at once that $\mathbb{Z}$ is a PID. The *division algorithm for* $F[x]$ appeared in Theorem 23.1 and was used in a completely analogous way to show that $F[x]$ is a PID. Now a modern technique of mathematics is to take some clearly related situations and to try to bring them under one roof by abstracting the important ideas common to them. The following definition is an illustration of this technique, as is this whole text! Let us see what we can develop by starting with the existence of a fairly general division algorithm in an integral domain.

46.1 Definition A **Euclidean norm** on an integral domain D is a function ν mapping the nonzero elements of D into the nonnegative integers such that the following conditions are satisfied:

1. For all $a, b \in D$ with $b \neq 0$, there exist q and r in D such that $a = bq + r$, where either $r = 0$ or $\nu(r) < \nu(b)$.
2. For all $a, b \in D$, where neither a nor b is 0, $\nu(a) \leq \nu(ab)$.

An integral domain D is a **Euclidean domain** if there exists a Euclidean norm on D. ■

The importance of Condition 1 is clear from our discussion. The importance of Condition 2 is that it will enable us to characterize the units of a Euclidean domain D.

46.2 Example The integral domain $\mathbb{Z}$ is a Euclidean domain, for the function ν defined by $\nu(n) = |n|$ for $n \neq 0$ in $\mathbb{Z}$ is a Euclidean norm on $\mathbb{Z}$. Condition 1 holds by the division algorithm for $\mathbb{Z}$. Condition 2 follows from $|ab| = |a||b|$ and $|a| \geq 1$ for $a \neq 0$ in $\mathbb{Z}$. ▲

46.3 Example If F is a field, then $F[x]$ is a Euclidean domain, for the function ν defined by $\nu(f(x)) =$ (degree $f(x)$) for $f(x) \in F[x]$, and $f(x) \neq 0$ is a Euclidean norm. Condition 1 holds by Theorem 23.1, and Condition 2 holds since the degree of the product of two polynomials is the sum of their degrees. ▲