PROOF By Theorem 16.1, we know that $F[x]$ is an integral domain. Now, let I be an ideal in $F[x]$. If $I = \{0\}$, then $I = \langle 0 \rangle$. If $I \neq \{0\}$, then among all the elements of I, let $g(x)$ be one of minimum degree. We will show that $I = \langle g(x) \rangle$. Since $g(x) \in I$, we have $\langle g(x) \rangle \subseteq I$. Now let $f(x) \in I$. Then, by the division algorithm, we may write $f(x) = g(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Since $r(x) = f(x) - g(x)q(x) \in I$, the minimality of $\deg g(x)$ implies that the latter condition cannot hold. So, $r(x) = 0$ and, therefore, $f(x) \in \langle g(x) \rangle$. This shows that $I \subseteq \langle g(x) \rangle$. ∎

The proof of Theorem 16.4 also establishes the following.

Theorem 16.5 Criterion for $I = \langle g(x) \rangle$

Let F be a field, I a nonzero ideal in $F[x]$, and $g(x)$ an element of $F[x]$. Then, $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.

As an application of the First Isomorphism Theorem for Rings (Theorem 15.3) and Theorem 16.5, we verify the remark we made in Example 12 in Chapter 14 that the ring $\mathbf{R}[x]/\langle x^2 + 1 \rangle$ is isomorphic to the ring of complex numbers.

EXAMPLE 3 Consider the homomorphism ϕ from $\mathbf{R}[x]$ onto $\mathbf{C}$ given by $f(x) \to f(i)$ (that is, evaluate a polynomial in $\mathbf{R}[x]$ at i). Then $x^2 + 1 \in \text{Ker } \phi$ and is clearly a polynomial of minimum degree in $\text{Ker } \phi$. Thus, $\text{Ker } \phi = \langle x^2 + 1 \rangle$ and $\mathbf{R}[x]/\langle x^2 + 1 \rangle$ is isomorphic to $\mathbf{C}$. ∎

Exercises

If I feel unhappy, I do mathematics to become happy. If I am happy, I do mathematics to keep happy.

Paul Turán

1. Let $f(x) = 4x^3 + 2x^2 + x + 3$ and $g(x) = 3x^4 + 3x^3 + 3x^2 + x + 4$, where $f(x), g(x) \in Z_5[x]$. Compute $f(x) + g(x)$ and $f(x) \cdot g(x)$.
2. In $Z_3[x]$, show that the distinct polynomials $x^4 + x$ and $x^2 + x$ determine the same function from Z_3 to Z_3.
3. Show that $x^2 + 3x + 2$ has four zeros in Z_6.
4. If R is a commutative ring, show that the characteristic of $R[x]$ is the same as the characteristic of R.

5. Prove Corollary 1 of Theorem 16.2.
6. List all the polynomials of degree 2 in $Z_2[x]$. Which of these are equal as functions from Z_2 to Z_2?
7. Find two distinct cubic polynomials over Z_2 that determine the same function from Z_2 to Z_2.
8. For any positive integer n, how many polynomials are there of degree n over Z_2? How many distinct polynomial functions from Z_2 to Z_2 are there?
9. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ in $Z_7[x]$. Determine the quotient and remainder upon dividing $f(x)$ by $g(x)$.
10. Let R be a commutative ring. Show that $R[x]$ has a subring isomorphic to R.
11. If $\phi: R \to S$ is a ring homomorphism, define $\overline{\phi}: R[x] \to S[x]$ by $(a_n x^n + \cdots + a_0) \to \phi(a_n)x^n + \cdots + \phi(a_0)$. Show that $\overline{\phi}$ is a ring homomorphism. (This exercise is referred to in Chapter 33.)
12. If the rings R and S are isomorphic, show that $R[x]$ and $S[x]$ are isomorphic. (The converse to not true–see [1].)
13. Prove Corollary 2 of Theorem 16.2.
14. Let $f(x)$ and $g(x)$ be cubic polynomials with integer coefficients such that $f(a) = g(a)$ for four integer values of a. Prove that $f(x) = g(x)$. Generalize.
15. Show that the polynomial $2x + 1$ in $Z_4[x]$ has a multiplicative inverse in $Z_4[x]$.
16. Are there any nonconstant polynomials in $Z[x]$ that have multiplicative inverses? Explain your answer.
17. Let p be a prime. Are there any nonconstant polynomials in $Z_p[x]$ that have multiplicative inverses? Explain your answer.
18. Show that Theorem 16.4 is false for any commutative ring that has a zero divisor.
19. (Degree Rule) Let D be an integral domain and $f(x), g(x) \in D[x]$. Prove that $\deg (f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$. Show, by example, that for commutative ring R it is possible that $\deg f(x)g(x) < \deg f(x) + \deg g(x)$, where $f(x)$ and $g(x)$ are nonzero elements in $R[x]$. (This exercise is referred to in this chapter, Chapter 17, and Chapter 18.)
20. Prove that the ideal $\langle x \rangle$ in $Q[x]$ is maximal.
21. Let $f(x)$ belong to $F[x]$, where F is a field. Let a be a zero of $f(x)$ of multiplicity n, and write $f(x) = (x - a)^n q(x)$. If $b \neq a$ is a zero of $q(x)$, show that b has the same multiplicity as a zero of $q(x)$ as it does for $f(x)$. (This exercise is referred to in this chapter.)

22. Prove that for any positive integer n, a field F can have at most a finite number of elements of multiplicative order at most n.
23. Let F be a field, and let $f(x)$ and $g(x)$ belong to $F[x]$ and not both zero. If there is no polynomial of positive degree in $F[x]$ that divides both $f(x)$ and $g(x)$ [in this case, $f(x)$ and $g(x)$ are said to be *relatively prime*], prove that there exist polynomials $h(x)$ and $k(x)$ in $F[x]$ with the property that $f(x)h(x) + g(x)k(x) = 1$. (This exercise is referred to in Chapter 20.)
24. Let F be an infinite field and let $f(x), g(x) \in F[x]$. If $f(a) = g(a)$ for infinitely many elements a of F, show that $f(x) = g(x)$.
25. Let F be a field and let $p(x) \in F[x]$. If $f(x)$, $g(x) \in F[x]$ and $\deg f(x) < \deg p(x)$ and $\deg g(x) < \deg p(x)$, show that $f(x) + \langle p(x)\rangle = g(x) + \langle p(x)\rangle$ implies $f(x) = g(x)$. (This exercise is referred to in Chapter 20.)
26. Prove that $Z[x]$ is not a principal ideal domain. (Compare this with Theorem 16.3.)
27. Find a polynomial with integer coefficients that has $1/2$ and $-1/3$ as zeros.
28. Let $f(x) \in \mathbf{R}[x]$. Suppose that $f(a) = 0$ but $f'(a) \neq 0$, where $f'(x)$ is the derivative of $f(x)$. Show that a is a zero of $f(x)$ of multiplicity 1.
29. Show that Corollary 2 of Theorem 16.2 is true over any commutative ring with unity.
30. Show that Theorem 16.4 is true for polynomials over integral domains.
31. Let F be a field and let
$$I = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \mid a_n, a_{n-1}, \ldots, a_0 \in F \text{ and } a_n + a_{n-1} + \cdots + a_0 = 0\}.$$
Show that I is an ideal of $F[x]$ and find a generator for I.
32. Let F be a field and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$. Prove that $x - 1$ is a factor of $f(x)$ if and only if $a_n + a_{n-1} + \cdots + a_0 = 0$.
33. Let m be a fixed positive integer. For any integer a, let $\bar{a}$ denote $a \bmod m$. Show that the mapping of ϕ: $Z[x] \to Z_m[x]$ given by
$$\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = \bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0$$
is a ring homomorphism. (This exercise is referred to in Chapters 17 and 33.)
34. Find infinitely many polynomials $f(x)$ in $Z_3[x]$ such that $f(a) = 0$ for all a in Z_3.

35. For every prime p, show that

$$x^{p-1} - 1 = (x - 1)(x - 2) \cdots [x - (p - 1)]$$

in $Z_p[x]$.

36. Let ϕ be the ring homomorphism from $Z[x]$ to Z given by $\phi(f(x)) = f(1)$. Find a polynomial $g(x)$ in $Z[x]$ such that Ker $\phi = \langle g(x) \rangle$. Is there more than one possibility for $g(x)$? To what familiar ring is $Z[x]/\text{Ker } \phi$ isomorphic? Do this exercise with Z replaced by Q.

37. Give an example of a field that properly contains the field of complex numbers $\mathbf{C}$.

38. (Wilson's Theorem) For every integer $n > 1$, prove that $(n - 1)! \bmod n = n - 1$ if and only if n is prime.

39. For every prime p, show that $(p - 2)! \bmod p = 1$.

40. Find the remainder upon dividing 98! by 101.

41. Prove that $(50!)^2 \bmod 101 = -1 \bmod 101$.

42. If I is an ideal of a ring R, prove that $I[x]$ is an ideal of $R[x]$.

43. Give an example of a commutative ring R with unity and a maximal ideal I of R such that $I[x]$ is not a maximal ideal of $R[x]$.

44. Let R be a commutative ring with unity. If I is a prime ideal of R, prove that $I[x]$ is a prime ideal of $R[x]$.

45. Let F be an infinite field and let $f(x) \in F[x]$. If $f(a) = 0$ for infinitely many elements a of F, show that $f(x) = 0$.

46. Prove that $Q[x]/\langle x^2 - 2 \rangle$ is ring-isomorphic to $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$.

47. Let $f(x) \in \mathbf{R}[x]$. If $f(a) = 0$ and $f'(a) = 0$ [$f'(a)$ is the derivative of $f(x)$ at a], show that $(x - a)^2$ divides $f(x)$.

48. Let F be a field and let $I = \{f(x) \in F[x] \mid f(a) = 0 \text{ for all } a \text{ in } F\}$. Prove that I is an ideal in $F[x]$. Prove that I is infinite when F is finite and $I = \{0\}$ when F is infinite. When F is finite, find a monic polynomial $g(x)$ such that $I = \langle g(x) \rangle$.

49. Let $g(x)$ and $h(x)$ belong to $Z[x]$ and let $h(x)$ be monic. If $h(x)$ divides $g(x)$ in $Q[x]$, show that $h(x)$ divides $g(x)$ in $Z[x]$. (This exercise is referred to in Chapter 33.)

50. Let R be a ring and x be an indeterminate. Prove that the rings $R[x]$ and $R[x^2]$ are ring-isomorphic.

51. Let $f(x)$ be a nonconstant element of $Z[x]$. Prove that $f(x)$ takes on infinitely many values in Z.

52. Let $f(x)$ be a nonconstant element in $Z[x]$. Prove that $\langle f(x) \rangle$ is not maximal in $Z[x]$.

53. Suppose that F is a field and there is a ring homomorphism from Z onto F. Show that F is isomorphic to Z_p for some prime p.
54. Let $f(x)$ belong to $Z_p[x]$. Prove that if $f(b) = 0$, then $f(b^p) = 0$.
55. Suppose $f(x)$ is a polynomial with odd integer coefficients and even degree. Prove that $f(x)$ has no rational zeros.
56. Find the remainder when x^{51} is divided by $x + 4$ in $Z_7[x]$.
57. Let F be a field. Show that there exist $a, b \in F$ with the property that $x^2 + x + 1$ divides $x^{43} + ax + b$.
58. Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ belong to $Q[x]$ and suppose that $f(x)g(x)$ belongs to $Z[x]$. Prove that $a_i b_j$ is an integer for every i and j.
59. Let $f(x)$ belong to $Z[x]$. If $a \bmod m = b \bmod m$, prove that $f(a) \bmod m = f(b) \bmod m$. Prove that if both $f(0)$ and $f(1)$ are odd, then f has no zero in Z.
60. For any field F, recall that $F(x)$ denotes the field of quotients of the ring $F[x]$. Prove that there is no element in $F(x)$ whose square is x.
61. Show that 1 is the only solution of $x^{25} - 1 = 0$ in Z_{37}.

Suggested Reading

M. Hochster, "Nonuniqueness of Coefficient Rings in a Polynomial Ring," *Proceedings of American Mathematical Society*, 34 (1972): 81–82.

The author gives an example of non-isomorphic commutative rings R and S with property that the ring $R[x]$ and $S[x]$ are isomorphic.

$$x(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

so that the left-hand side of Equation (1) has the irreducible factorization

$$x^2(x + 1)^2(x^2 + x + 1)^2(x^2 - x + 1)^2.$$

So, by Theorem 17.6, this means that these factors are the only possible irreducible factors of $P(x) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6}$. Thus, $P(x)$ has the form

$$x^q(x + 1)^r(x^2 + x + 1)^t(x^2 - x + 1)^u,$$

where $0 \leq q, r, t, u \leq 2$.

To restrict further the possibilities for these four parameters, we evaluate $P(1)$ in two ways. $P(1) = 1^{a_1} + 1^{a_2} + \cdots + 1^{a_6} = 6$ and $P(1) = 1^q 2^r 3^t 1^u$. Clearly, this means that $r = 1$ and $t = 1$. What about q? Evaluating $P(0)$ in two ways shows that $q \neq 0$. On the other hand, if $q = 2$, the smallest possible sum one could roll with the corresponding labels for dice would be 3. Since this violates our assumption, we have now reduced our list of possibilities for q, r, t, and u to $q = 1$, $r = 1$, $t = 1$, and $u = 0, 1, 2$. Let's consider each of these possibilities in turn.

When $u = 0$, $P(x) = x^4 + x^3 + x^3 + x^2 + x^2 + x$, so the die labels are 4, 3, 3, 2, 2, 1—a Sicherman die.

When $u = 1$, $P(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x$, so the die labels are 6, 5, 4, 3, 2, 1—an ordinary die.

When $u = 2$, $P(x) = x^8 + x^6 + x^5 + x^4 + x^3 + x$, so the die labels are 8, 6, 5, 4, 3, 1—the other Sicherman die.

This proves that the Sicherman dice do give the same probabilities as ordinary dice *and* that they are the *only* other pair of dice that have this property. ∎

Exercises

No matter how good you are at something, there's always about a million people better than you.

Homer Simpson

1. Verify the assertion made in Example 2.
2. Suppose that D is an integral domain and F is a field containing D. If $f(x) \in D[x]$ and $f(x)$ is irreducible over F but reducible over D, what can you say about the factorization of $f(x)$ over D?
3. Show that a nonconstant polynomial from $Z[x]$ that is irreducible over Z is primitive. (This exercise is referred to in this chapter.)
4. Suppose that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in Z[x]$. If r is rational and $x - r$ divides $f(x)$, show that r is an integer.

5. Let F be a field and let a be a nonzero element of F.
   a. If $af(x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.
   b. If $f(ax)$ is irreducible over F, prove that $f(x)$ is irreducible over F.
   c. If $f(x + a)$ is irreducible over F, prove that $f(x)$ is irreducible over F.
   d. Use part c to prove that $8x^3 - 6x + 1$ is irreducible over Q.
   (This exercise is referred to in this chapter.)
6. Let F be a field and $f(x) \in F[x]$. Show that, as far as deciding upon the irreducibility of $f(x)$ over F is concerned, we may assume that $f(x)$ is monic. (This assumption is useful when one uses a computer to check for irreducibility.)
7. Suppose there is a real number r with the property that $r + 1/r$ is an odd integer. Prove that r is irrational.
8. Show that the equation $x^2 + y^2 = 2003$ has no solutions in the integers.
9. Explain how the Mod p Irreducibility Test (Theorem 17.3) can be used to test members of $Q[x]$ for irreducibility.
10. Suppose that $f(x) \in Z_p[x]$ and $f(x)$ is irreducible over Z_p, where p is a prime. If $\deg f(x) = n$, prove that $Z_p[x]/\langle f(x)\rangle$ is a field with p^n elements.
11. Construct a field of order 25.
12. Construct a field of order 27.
13. Show that $x^3 + x^2 + x + 1$ is reducible over Q. Does this fact contradict the corollary to Theorem 17.4?
14. Determine which of the polynomials below is (are) irreducible over Q.
   a. $x^5 + 9x^4 + 12x^2 + 6$
   b. $x^4 + x + 1$
   c. $x^4 + 3x^2 + 3$
   d. $x^5 + 5x^2 + 1$
   e. $(5/2)x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + 3/14$
15. Show that $x^4 + 1$ is irreducible over Q but reducible over $\mathbf{R}$. (This exercise is referred to in this chapter.)
16. Prove that $x^4 + 15x^3 + 7$ is irreducible over Q
17. Show that $x^4 + 1$ is reducible over Z_p for every prime p. (This exercise is referred to in this chapter.)
18. Show that $x^2 + x + 4$ is irreducible over Z_{11}.
19. Let $f(x) = x^3 + 6 \in Z_7[x]$. Write $f(x)$ as a product of irreducible polynomials over Z_7.
20. Let $f(x) = x^3 + x^2 + x + 1 \in Z_2[x]$. Write $f(x)$ as a product of irreducible polynomials over Z_2.

21. Find all the zeros and their multiplicities of $x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1$ over Z_5.

22. Find all zeros of $f(x) = 3x^2 + x + 4$ over Z_7 by substitution. Find all zeros of $f(x)$ by using the quadratic formula $(-b \pm \sqrt{b^2 - 4ac}) \cdot (2a)^{-1}$ (all calculations are done in Z_7). Do your answers agree? Should they? Find all zeros of $g(x) = 2x^2 + x + 3$ over Z_5 by substitution. Try the quadratic formula on $g(x)$. Do your answers agree? State necessary and sufficient conditions for the quadratic formula to yield the zeros of a quadratic from $Z_p[x]$, where p is a prime greater than 2.

23. Let p be a prime.

a. Show that the number of reducible polynomials over Z_p of the form $x^2 + ax + b$ is $p(p + 1)/2$.

b. Determine the number of reducible quadratic polynomials over Z_p.

24. Let p be a prime.

a. Determine the number of irreducible polynomials over Z_p of the form $x^2 + ax + b$.

b. Determine the number of irreducible quadratic polynomials over Z_p.

25. Show that for every prime p there exists a field of order p^2.

26. Prove that, for every positive integer n, there are infinitely many polynomials of degree n in $Z[x]$ that are irreducible over Q.

27. Show that the field given in Example 11 in this chapter is isomorphic to the field given in Example 9 in Chapter 13.

28. Let $f(x) \in Z_p[x]$. Prove that if $f(x)$ has no factor of the form $x^2 + ax + b$, then it has no quadratic factor over Z_p.

29. Find all monic irreducible polynomials of degree 2 over Z_3.

30. Given that π is not the zero of a nonzero polynomial with rational coefficients, prove that π^2 cannot be written in the form $a\pi + b$, where a and b are rational.

31. (Rational Root Theorem) Let

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

and $a_n \neq 0$. Prove that if r and s are relatively prime integers and $f(r/s) = 0$, then $r \mid a_0$ and $s \mid a_n$.

32. Let F be a field and let $p(x), a_1(x), a_2(x), \ldots, a_k(x) \in F[x]$, where $p(x)$ is irreducible over F. If $p(x) \mid a_1(x)a_2(x) \cdots a_k(x)$, show that $p(x)$ divides some $a_i(x)$. (This exercise is referred to in the proof of Theorem 17.6.)

33. Let F be a field and $p(x) \in F[x]$. Use Theorem 14.4 to prove that if $\langle p(x) \rangle$ is a maximal ideal in $F[x]$, then $p(x)$ is irreducible over F (see Theorem 17.5).

34. If p is a prime, prove that $x^{p-1} - x^{p-2} + x^{p-3} - \cdots - x + 1$ is irreducible over Q.
35. Let F be a field and let $p(x)$ be irreducible over F. If E is a field that contains F and there is an element a in E such that $p(a) = 0$, show that the mapping ϕ: $F[x] \to E$ given by $f(x) \to f(a)$ is a ring homomorphism with kernel $\langle p(x) \rangle$. (This exercise is referred to in Chapter 20.)
36. Prove that the ideal $\langle x^2 + 1 \rangle$ is prime in $Z[x]$ but not maximal in $Z[x]$.
37. Let F be a field and let $p(x)$ be irreducible over F. Show that $\{a + \langle p(x) \rangle \mid a \in F\}$ is a subfield of $F[x]/\langle p(x) \rangle$ isomorphic to F. (This exercise is referred to in Chapter 20.)
38. Let F be a field and let $f(x)$ be a polynomial in $F[x]$ that is reducible over F. Prove that $\langle f(x) \rangle$ is not a prime ideal in $F[x]$.
39. Example 1 in this chapter shows the converse of Theorem 17.2 is not true. That is, a polynomial $f(x)$ in $Z[x]$ can be reducible over Z but irreducible over Q. State a condition on $f(x)$ that makes the converse true.
40. Carry out the analysis given in Example 12 for a pair of tetrahedrons instead of a pair of cubes. (Define ordinary tetrahedral dice as the ones labeled 1 through 4.)
41. Suppose in Example 12 that we begin with n ($n > 2$) ordinary dice each labeled 1 through 6, instead of just two. Show that the only possible labels that produce the same probabilities as n ordinary dice are the labels 1 through 6 and the Sicherman labels.
42. Show that one two-sided die labeled with 1 and 4 and another 18-sided die labeled with 1, 2, 2, 3, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 7, 7, 8 yield the same probabilities as an ordinary pair of cubes labeled 1 through 6. Carry out an analysis similar to that given in Example 12 to derive these labels.
43. In the game of Monopoly, would the probabilities of landing on various properties be different if the game were played with Sicherman dice instead of ordinary dice? Why?

Computer Exercises

Computer exercises for this chapter are available at the website:

http://www.d.umn.edu/~jgallian

We conclude this chapter with an example of an integral domain that is not a unique factorization domain.

■ **EXAMPLE 8** The ring $Z[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in Z\}$ is an integral domain but not a unique factorization domain. It is straightforward that $Z[\sqrt{-5}]$ is an integral domain (see Exercise 11 in Chapter 13). To verify that unique factorization does not hold, we mimic the method used in Example 1 with $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Since $N(xy) = N(x)N(y)$ and $N(x) = 1$ if and only if x is a unit (see Exercise 1), it follows that the only units of $Z[\sqrt{-5}]$ are ± 1.

Now consider the following factorizations:

$$46 = 2 \cdot 23,$$
$$46 = (1 + 3\sqrt{-5})(1 - 3\sqrt{-5}).$$

We claim that each of these four factors is irreducible over $Z[\sqrt{-5}]$. Suppose that, say, $2 = xy$, where $x, y \in Z[\sqrt{-5}]$ and neither is a unit. Then $4 = N(2) = N(x)N(y)$ and, therefore, $N(x) = N(y) = 2$, which is impossible. Likewise, if $23 = xy$ were a nontrivial factorization, then $N(x) = 23$. Thus, there would be integers a and b such that $a^2 + 5b^2 = 23$. Clearly, no such integers exist. The same argument applies to $1 \pm 3\sqrt{-5}$. ■

In light of Examples 7 and 8, one can't help but wonder for which $d < 0$ is $Z[\sqrt{d}]$ a unique factorization domain. The answer is only when $d = -1$ or -2 (see [1], p. 297). The case where $d = -1$ was first proved, naturally enough, by Gauss.

Exercises

I tell them that if they will occupy themselves with the study of mathematics they will find in it the best remedy against lust of the flesh.

Thomas Mann, *The Magic Mountain*

1. For the ring $Z[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in Z\}$, where $d \neq 1$ and d is not divisible by the square of a prime, prove that the norm $N(a + b\sqrt{d}) = |a^2 - db^2|$ satisfies the four assertions made preceding Example 1. (This exercise is referred to in this chapter.)
2. In an integral domain, show that a and b are associates if and only if $\langle a \rangle = \langle b \rangle$.
3. Show that the union of a chain $I_1 \subset I_2 \subset \cdots$ of ideals of a ring R is an ideal of R. (This exercise is referred to in this chapter.)

4. In an integral domain, show that the product of an irreducible and a unit is an irreducible.
5. Suppose that a and b belong to an integral domain and $b \neq 0$. Show that $\langle ab \rangle$ is a proper subset of $\langle b \rangle$ if and only if a is not a unit. This exercise is referred to in this chapter.
6. Let D be an integral domain. Define $a \sim b$ if a and b are associates. Show that this defines an equivalence relation on D.
7. In the notation of Example 7, show that $d(xy) = d(x)d(y)$.
8. Let D be a Euclidean domain with measure d. Prove that u is a unit in D if and only if $d(u) = d(1)$.
9. Let D be a Euclidean domain with measure d. Show that if a and b are associates in D, then $d(a) = d(b)$.
10. Let D be a principal ideal domain and let $p \in D$. Prove that $\langle p \rangle$ is a maximal ideal in D if and only if p is irreducible.
11. Trace through the argument given in Example 7 to find q and r in $Z[i]$ such that $3 - 4i = (2 + 5i)q + r$ and $d(r) < d(2 + 5i)$.
12. Let D be a principal ideal domain. Show that every proper ideal of D is contained in a maximal ideal of D.
13. In $Z[\sqrt{-5}]$, show that 21 does not factor uniquely as a product of irreducibles.
14. Show that $1 - i$ is an irreducible in $Z[i]$.
15. Show that $Z[\sqrt{-6}]$ is not a unique factorization domain. (*Hint:* Factor 10 in two ways.) Why does this show that $Z[\sqrt{-6}]$ is not a principal ideal domain?
16. Give an example of a unique factorization domain with a subdomain that does not have a unique factorization.
17. In $Z[i]$, show that 3 is irreducible but 2 and 5 are not.
18. Prove that 7 is irreducible in $Z[\sqrt{6}]$, even though $N(7)$ is not prime.
19. Prove that if p is a prime in Z that can be written in the form $a^2 + b^2$, then $a + bi$ is irreducible in $Z[i]$. Find three primes that have this property and the corresponding irreducibles.
20. Prove that $Z[\sqrt{-3}]$ is not a principal ideal domain.
21. In $Z[\sqrt{-5}]$, prove that $1 + 3\sqrt{-5}$ is irreducible but not prime.
22. In $Z[\sqrt{5}]$, prove that both 2 and $1 + \sqrt{5}$ are irreducible but not prime.
23. Prove that $Z[\sqrt{5}]$ is not a unique factorization domain.
24. Let F be a field. Show that in $F[x]$ a prime ideal is a maximal ideal.
25. Let d be an integer less than -1 that is not divisible by the square of a prime. Prove that the only units of $Z[\sqrt{d}]$ are $+1$ and -1.

26. In $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$, show that every element of the form $(3 + 2\sqrt{2})^n$ is a unit, where n is a positive integer.

27. If a and b belong to $Z[\sqrt{d}]$, where d is not divisible by the square of a prime and ab is a unit, prove that a and b are units.

28. For a commutative ring with unity we may define associates, irreducibles, and primes exactly as we did for integral domains. With these definitions, show that both 2 and 3 are prime in Z_{12} but 2 is irreducible and 3 is not.

29. Let n be a positive integer and p a prime that divides n. Prove that p is prime in Z_n. (See Exercise 28).

30. Let p be a prime divisor of a positive integer n. Prove that p is irreducible in Z_n if and only if p^2 divides n. (See Exercise 28).

31. Prove or disprove that if D is a principal ideal domain, then $D[x]$ is a principal ideal domain.

32. Determine the units in $Z[i]$.

33. Let p be a prime in an integral domain. If $p \mid a_1 a_2 \cdots a_n$, prove that p divides some a_i. (This exercise is referred to in this chapter.)

34. Show that $3x^2 + 4x + 3 \in Z_5[x]$ factors as $(3x + 2)(x + 4)$ and $(4x + 1)(2x + 3)$. Explain why this does not contradict the corollary of Theorem 18.3.

35. Let D be a principal ideal domain and p an irreducible element of D. Prove that $D/\langle p \rangle$ is a field.

36. Show that an integral domain with the property that every strictly decreasing chain of ideals $I_1 \supset I_2 \supset \cdots$ must be finite in length is a field.

37. An ideal A of a commutative ring R with unity is said to be *finitely generated* if there exist elements $a_1, a_2, \ldots, a_n$ of A such that $A = \langle a_1, a_2, \ldots, a_n \rangle$. An integral domain R is said to satisfy the *ascending chain condition* if every strictly increasing chain of ideals $I_1 \subset I_2 \subset \cdots$ must be finite in length. Show that an integral domain R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.

38. Prove or disprove that a subdomain of a Euclidean domain is a Euclidean domain.

39. Show that for any nontrivial ideal I of $Z[i]$, $Z[i]/I$ is finite.

40. Find the inverse of $1 + \sqrt{2}$ in $Z[\sqrt{2}]$. What is the multiplicative order of $1 + \sqrt{2}$?

41. In $Z[\sqrt{-7}]$, show that $N(6 + 2\sqrt{-7}) = N(1 + 3\sqrt{-7})$ but $6 + 2\sqrt{-7}$ and $1 + 3\sqrt{-7}$ are not associates.

42. Let $R = Z \oplus Z \oplus \cdots$ (the collection of all sequences of integers under componentwise addition and multiplication). Show that R has ideals $I_1, I_2, I_3, \ldots$ with the property that $I_1 \subset I_2 \subset I_3 \subset \cdots$. (Thus R does not have the ascending chain condition.)
43. Prove that in a unique factorization domain, an element is irreducible if and only if it is prime.
44. Let F be a field and let R be the integral domain in $F[x]$ generated by x^2 and x^3. (That is, R is contained in every integral domain in $F[x]$ that contains x^2 and x^3.) Show that R is not a unique factorization domain.
45. Prove that for every field F, there are infinitely many irreducible elements in $F[x]$.
46. Prove that $Z[\sqrt{-2}]$ and $Z[\sqrt{2}]$ are unique factorization domains. (*Hint*: Mimic Example 7 in Chapter 18.)
47. Express both 13 and $5 + i$ as products of irreducibles from $Z[i]$.
48. Find a mistake in the statement shown in Figure 18.2.

Computer Exercise

Software for a computer exercise is available at the website:

http://www.d.umn.edu/~jgallian

References

1. H. M. Stark, *An Introduction to Number Theory*, Chicago: Markham, 1970.
2. J. C. Wilson, "A Principal Ideal Ring That Is Not a Euclidean Ring," *Mathematics Magazine* 46 (1973): 34–38.

Suggested Readings

Oscar Campoli, "A Principal Ideal Domain That Is Not a Euclidean Domain," *The American Mathematical Monthly* 95 (1988): 868–871.

The author shows that $\{a + b\theta \mid a, b \in Z, \theta = (1 + \sqrt{-19})/2\}$ is a PID that is not an ED.

Gina Kolata, "At Last, Shout of 'Eureka!' in Age-Old Math Mystery," *The New York Times*, June 24, 1993.

This front-page article reports on Andrew Wiles's announced proof of Fermat's Last Theorem.