10. **a.** Show that 2 is equal to the product of a unit and the square of an irreducible in $\mathbb{Z}[i]$.

b. Show that an odd prime p in $\mathbb{Z}$ is irreducible in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod 4$. (Use Theorem 36.10.)

11. Prove Lemma 36.2.

12. Prove that N of Example 36.9 is multiplicative, that is, that $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.

13. Let D be an integral domain with a multiplicative norm N such that $|N(\alpha)| = 1$ for $\alpha \in D$ if and only if α is a unit of D. Show that every nonzero nonunit of D has a factorization into irreducibles in D.

14. Use a Euclidean algorithm in $\mathbb{Z}[i]$ to find a gcd of $16 + 7i$ and $10 - 5i$ in $\mathbb{Z}[i]$. [*Hint:* Use the construction in the proof of Theorem 36.4.]

15. Let $\langle \alpha \rangle$ be a nonzero principal ideal in $\mathbb{Z}[i]$.

a. Show that $\mathbb{Z}[i]/\langle \alpha \rangle$ is a finite ring. [*Hint:* Use the division algorithm.]

b. Show that if σ is an irreducible of $\mathbb{Z}[i]$, then $\mathbb{Z}[i]/\langle \sigma \rangle$ is a field.

c. Referring to part (b), find the order and characteristic of each of the following fields.

i. $\mathbb{Z}[i]/\langle 3 \rangle$ **ii.** $\mathbb{Z}[i]/\langle 1 + i \rangle$ **iii.** $\mathbb{Z}[i]/\langle 1 + 2i \rangle$

16. Let $n \in \mathbb{Z}^+$ be square free, that is, not divisible by the square of any prime integer. Let $\mathbb{Z}[\sqrt{-n}] = \{a + ib\sqrt{n} \mid a, b \in \mathbb{Z}\}$.

a. Show that the norm N, defined by $N(\alpha) = a^2 + nb^2$ for $\alpha = a + ib\sqrt{n}$, is a multiplicative norm on $\mathbb{Z}[\sqrt{-n}]$.

b. Show that $N(\alpha) = 1$ for $\alpha \in \mathbb{Z}[\sqrt{-n}]$ if and only if α is a unit of $\mathbb{Z}[\sqrt{-n}]$.

c. Show that every nonzero $\alpha \in \mathbb{Z}[\sqrt{-n}]$ that is not a unit has a factorization into irreducibles in $\mathbb{Z}[\sqrt{-n}]$. [*Hint:* Use part (b).]

17. Repeat Exercise 16 for $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$ for square free $n > 1$, with N defined by $N(\alpha) = a^2 - nb^2$ for $\alpha = a + b\sqrt{n}$ in $\mathbb{Z}[\sqrt{n}]$. For part b show $|N(\alpha)| = 1$.

18. Show by a construction analogous to that given in the proof of Theorem 36.4 that the division algorithm holds in the integral domain $\mathbb{Z}[\sqrt{-2}]$ for $\nu(\alpha) = N(\alpha)$ for nonzero α in this domain (see Exercise 16). (Thus this domain is Euclidean. See Hardy and Wright [29] for a discussion of which domains $\mathbb{Z}[\sqrt{n}]$ and $\mathbb{Z}[\sqrt{-n}]$ are Euclidean.)

SECTION 37 †ALGEBRAIC GEOMETRY

This section gives a brief introduction to algebraic geometry. Algebraic geometry is the study of the common zeros of a finite collection of polynomials. For example, the zeros of the set of polynomials $\{x^2 + y^2 - 25, (x-6)^2 + y^2 - 25\}$ consist of just two points in $\mathbb{R}^2$, $(3, 4)$ and $(3, -4)$. In Section 38 we will develop a very useful algorithm that reduces a finite set of polynomials to a simpler set of polynomials whose zeros are identical to the zeros of the original set. In the example $\{x^2 + y^2 - 25, (x-6)^2 + y^2 - 25\}$, the algorithm yields $\{x - 3, y^2 - 16\}$ making it much easier to see the two zeros.

Algebraic Varieties and Ideals

Let F be a field. Recall that $F[x_1, x_2, \cdots, x_n]$ is the ring of polynomials in n indeterminants $x_1, x_2, \cdots, x_n$ with coefficients in F. We let F^n be the Cartesian product $F \times F \times \cdots \times F$ for n factors. For ease in writing, we denote an element $(a_1, a_2, \cdots, a_n)$ of F^n by $\mathbf{a}$, in bold type. Using similar economy, we let $F[\mathbf{x}] = F[x_1, x_2, \cdots, x_n]$. For each $\mathbf{a} \in F^n$, we have an evaluation homomorphism $\phi_{\mathbf{a}}: F[\mathbf{x}] \to F$ just as in Theorem 27.4. That is, for $f(\mathbf{x}) = f(x_1, x_2, \cdots, x_n) \in F[\mathbf{x}]$, we define $\phi_{\mathbf{a}}(f(\mathbf{x})) = f(\mathbf{a}) = f(a_1, a_2, \cdots, a_n)$.

† This section is used only in Section 38.

The proof that $\phi_{\mathbf{a}}$ is indeed a homomorphism follows from the associative, commutative, and distributive properties of the operations in $F[\mathbf{x}]$ and F. Just as for the one-indeterminate case, an element $\mathbf{a}$ of F^n is a **zero of** $f(\mathbf{x}) \in F[\mathbf{x}]$ if $f(\mathbf{a}) = 0$. In what follows, we further abbreviate a polynomial $f(\mathbf{x})$ by "f."

In this section and the following we discuss the problem of finding common zeros in F^n of a finite number of polynomials $f_1, f_2, \cdots, f_r$ in $F[\mathbf{x}]$. Finding and studying geometric properties of the set of all these common zeros is the subject of algebraic geometry.

37.1 Definition Let S be a finite subset of $F[\mathbf{x}]$. The **algebraic variety** $V(S)$ in F^n is the set of all common zeros in F^n of the polynomials in S. ■

In our illustrative examples, which usually involve at most three indeterminates, we use x, y, z in place of x_1, x_2, and x_3.

37.2 Example Let $S = \{2x + y - 2\} \subset \mathbb{R}[x, y]$. The algebraic variety $V(S)$ in $\mathbb{R}^2$ is the line with x-intercept 1 and y-intercept 2. ▲

We leave to Exercise 14 the straightforward proof that for r elements $f_1, f_2, \cdots, f_r$ in a commutative ring R with unity, the set

$$I = \{c_1 f_1 + c_2 f_2 + \cdots + c_r f_r \mid c_i \in R \text{ for } i = 1, \cdots, r\}$$

is an ideal of R. We denote this ideal by $\langle f_1, f_2, \cdots, f_r \rangle$. We are interested in the case $R = F[\mathbf{x}]$ where all the c_i and all the f_i are polynomials in $F[\mathbf{x}]$. We regard the c_i as "coefficient polynomials." By its construction, this ideal I is the smallest ideal containing the polynomials $f_1, f_2, \cdots, f_r$; it can also be described as the intersection of all ideals containing these r polynomials.

37.3 Definition Let I be an ideal in a commutative ring R with unity. A subset $\{b_1, b_2, \cdots, b_r\}$ of I is a **basis** for I if $I = \langle b_1, b_2, \cdots, b_r \rangle$. ■

Unlike the situation in linear algebra, there is no requirement of independence for elements of a basis, or of unique representation of an ideal member in terms of a basis.

37.4 Theorem Let $f_1, f_2, \cdots, f_r \in F[\mathbf{x}]$. The set of common zeros in F^n of the polynomials f_i for $i = 1, 2, \cdots, r$ is the same as the set of common zeros in F^n of all the polynomials in the entire ideal $I = \langle f_1, f_2, \cdots, f_r \rangle$.

Proof Let

$$f = c_1 f_1 + c_2 f_2 + \cdots + c_r f_r \qquad \textbf{(1)}$$

be any element of I, and let $\mathbf{a} \in F^n$ be a common zero of $f_1, f_2, \cdots$, and f_r. Applying the evaluation homomorphism $\phi_{\mathbf{a}}$ to Eq. (1), we obtain

$$\begin{aligned} f(\mathbf{a}) &= c_1(\mathbf{a}) f_1(\mathbf{a}) + c_2(\mathbf{a}) f_2(\mathbf{a}) + \cdots + c_r(\mathbf{a}) f_r(\mathbf{a}) \\ &= c_1(\mathbf{a}) 0 + c_2(\mathbf{a}) 0 + \cdots + c_r(\mathbf{a}) 0 = 0, \end{aligned}$$

showing that $\mathbf{a}$ is also a zero of every polynomial f in I. Of course, a zero of every polynomial in I will be a zero of each f_i because each $f_i \in I$. ◆

For an ideal I in $F[\mathbf{x}]$, we let $V(I)$ be the set of all common zeros of all elements of I. We can summarize Theorem 37.4 as

$$V(\{f_1, f_2, \cdots, f_r\}) = V(\langle f_1, f_2, \cdots, f_r \rangle).$$

Recall that a commutative ring with unity is Noetherian if for every chain $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$ of ideals in R, there is an integer r such that for $s \geq r$, $N_r = N_s$. Lemma 34.10

states that if R is a PID, then R is a Noetherian ring. Theorem 37.5 states that if R is a Noetherian ring, then polynomials with coefficients in R also form a Noetherian ring.

37.5 Example If R is a Noetherian ring, then $R[x]$ is also a Noetherian ring.

Proof Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be a chain of ideal in $R[x]$. As we saw in Lemma 34.9, $I = \bigcup_{n=1}^{\infty} I_n$ is an ideal in R.

We will show by contradiction that I has a finite basis. So we suppose that no finite set of polynomials is a basis for I. We let f_1 be a polynomial in I of minimal degree. We then let f_2 be a polynomial of minimum degree that is in I, but not in $\langle f_1 \rangle$. Continuing in this manner, we let f_n be a polynomial of minimal degree in I, but not in $\langle f_1, f_2, \ldots, f_{n-1} \rangle$. This defines an infinite sequence of polynomials since by our assumption no finite set of polynomials is a basis for I. It is clear that $\deg(f_1) \leq \deg(f_2)$ since otherwise we should have picked f_2 instead of f_1 as the first polynomial in the sequence. In general, $\deg(f_1) \leq \deg(f_2) \leq \deg(f_3) \leq \ldots$

We let a_j be the leading coefficient of f_j. Then in R, we have a chain of ideals

$$\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \langle a_1, a_2, a_3 \rangle \subseteq \ldots$$

By the ascending chain condition in R, there is some integer N so that for any $s \geq N$,

$$\langle a_1, a_2, \ldots, a_N \rangle = \langle a_1, a_2, \ldots, a_s \rangle.$$

In particular,

$$a_{N+1} = \sum_{j=1}^{N} c_j a_j$$

for some elements c_j in R. The polynomial

$$g(x) = \sum_{j=1}^{N} c_j x^{\deg(f_{N+1}) - \deg(f_j)} f_j$$

is in the ideal $\langle f_1, f_2, f_3, \ldots, f_N \rangle$. Thus $f_{N+1} - g \notin \langle f_1, f_2, \ldots, f_N = J \rangle$. The degrees of g and f_{N+1} are equal and they have the same leading coefficient a_{N+1}. Thus the degree of $f_{N+1} - g$ is less than the degree of f_{N+1}. But this contradicts the choice of f_{N+1} since $f_{N+1} - g \notin J$, $f_N - g$ has lower degree than f_{N+1}, and f_{N+1} has lowest degree among all the polynomials in I that are not in $\langle f_1(x), f_2(x), \ldots f_N(x) \rangle$. We conclude that there is a finite set of polynomials with $I = \langle f_1, f_2, \ldots, f_n \rangle$.

Since every polynomial f_j is in some I_{k_j} and $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$, it follows that there is an integer r such that f_j is in I_r for each j. Therefore, $I = \langle f_1, f_2, f_3, \ldots, f_n \rangle = I_r$. ◆

By repeated application of Theorem 37.5, it is immediate that $F[x_1, x_2, \ldots, x_n]$ is a Noetherian ring for any field F. Exercise 21 shows that if R is a commutative ring with unity, then R is a Noetherian ring if and only if every ideal I in R has a finite basis. These observations prove the following significant theorem.

37.6 Theorem **(Hilbert Basis Theorem)** Every ideal I in $F[x_1, x_2, \ldots, x_n]$ has a finite basis. ♦

Our objective: Given a basis for an ideal I in $F[\mathbf{x}]$, modify it if possible to become a basis that better exhibits the structure of I and the geometry of the associated algebraic variety $V(I)$.