Chapter 10

Rings

Bitte vergiß alles, was Du auf der Schule gelernt hast;
denn Du hast es nicht gelernt.

Edmund Landau

1. DEFINITION OF A RING

The integers form our basic model for the concept of a ring. They are closed under addition, subtraction, and multiplication, but not under division.

Before going to the abstract definition of a ring, we can get some examples by considering subrings of the complex numbers. A *subring* of $\mathbb{C}$ is a subset which is closed under addition, subtraction, and multiplication and which contains 1. Thus any subfield [Chapter 3 (2.1)] is a subring. Another example is the ring of *Gauss integers,* which are complex numbers of the form $a + bi$, where a and b are integers. This ring is denoted by

$$\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}. \tag{1.1}$$

The Gauss integers are the points of a square lattice in the complex plane.

We can form a subring $\mathbb{Z}[\alpha]$ analogous to the ring of Gauss integers, starting with any complex number α. We define $\mathbb{Z}[\alpha]$ to be the smallest subring of $\mathbb{C}$ containing α, and we call it the subring *generated by* α. It is not hard to describe this ring. If a ring contains α, then it contains all positive powers of α because it is closed under multiplication. Also, it contains sums and differences of such powers, and it contains 1. Therefore it contains every complex number β which can be expressed as a polynomial in α with integer coefficients:

$$\beta = a_n\alpha^n + \cdots + a_1\alpha + a_0, \quad \text{where } a_i \in \mathbb{Z}. \tag{1.2}$$

On the other hand, the set of all such numbers is closed under the operations of addition, subtraction, and multiplication, and it contains 1. So it is the subring generated

by α. But $\mathbb{Z}[\alpha]$ will not be represented as a lattice in the complex plane in most cases. For example, the ring $\mathbb{Z}[\frac{1}{2}]$ consists of the rational numbers which can be expressed as a polynomial in $\frac{1}{2}$ with integer coefficients. These rational numbers can be described simply as those whose denominator is a power of 2. They form a dense subset of the real line.

A complex number α is called *algebraic* if it is a root of a polynomial with integer coefficients, that is, if some expression of the form (1.2) is zero. For example, $i + 3, 1/7, 7 + \sqrt[3]{2}$, and $\sqrt{3} + \sqrt{-5}$ are algebraic numbers.

If there is *no* polynomial with integer coefficients having α as a root, then α is called a *transcendental* number. The numbers e and π are transcendental, though it is not easy to prove that they are. If α is transcendental, then two distinct polynomial expressions (1.2) must represent different complex numbers. In this case the elements of the ring $\mathbb{Z}[\alpha]$ correspond bijectively to polynomials $p(x)$ with integer coefficients, by the rule $p(x) \longleftrightarrow p(\alpha)$.

When α is algebraic there will be many polynomial expressions (1.2) which represent the same complex number. For example, when $\alpha = i$, the powers α^n take the four values $\pm 1, \pm i$. Using the relation $i^2 = -1$, every expression (1.2) can be reduced to one whose degree in i is ≤ 1. This agrees with the description given above for the ring of Gauss integers.

The two kinds of numbers, algebraic and transcendental, are somewhat analogous to the two possibilities, finite and infinite, for a cyclic group [Chapter 2 (2.7)].

The definition of abstract ring is similar to that of field [Chapter 3 (2.3)], except that multiplicative inverses are not required to exist:

(1.3) **Definition.** A *ring* R is a set with two laws of composition $+$ and $\times$, called addition and multiplication, which satisfy these axioms:

(a) With the law of composition $+$, R is an abelian group, with identity denoted by 0. This abelian group is denoted by R^+.

(b) Multiplication is associative and has an identity denoted by 1.

(c) *Distributive laws:* For all $a, b, c, \in R$,

$$(a + b)c = ac + bc \quad \text{and} \quad c(a + b) = ca + cb.$$

A *subring* of a ring is a subset which is closed under the operations of addition, subtraction, and multiplication and which contains the element 1.

The terminology used is not completely standardized. Some people do not require the existence of a multiplicative identity in a ring. We will study *commutative rings* in most of this book, that is, rings satisfying the commutative law $ab = ba$ for multiplication. So let us agree that the word *ring* will mean *commutative ring with identity,* unless we explicitly mention noncommutativity. The two distributive laws (c) are equivalent for commutative rings.

The ring $\mathbb{R}^{n \times n}$ of all $n \times n$ matrices with real entries is an important example of a ring which is not commutative.

Besides subrings of $\mathbb{C}$, the most important rings are polynomial rings. Given any ring R, a polynomial in x with coefficients in R is an expression of the form

$$a_n x^n + \cdots + a_1 x + a_0, \tag{1.4}$$

with $a_i \in R$. The set of these polynomials forms a ring which is usually denoted by $R[x]$. We will discuss polynomial rings in the next section.

Here are some more examples of rings:

(1.5) **Examples.**

(a) Any field is a ring.

(b) The set $\mathcal{R}$ of continuous real-valued functions of a real variable x forms a ring, with addition and multiplication of functions:

$$[f + g](x) = f(x) + g(x) \quad \text{and} \quad [fg](x) = f(x)g(x).$$

(c) The *zero ring* $R = \{0\}$ consists of a single element 0.

In the definition of a *field* [Chapter 3 (2.3)], the multiplicative identity 1 is required to lie in $F^\times = F - \{0\}$. Hence a field has at least two distinct elements, namely 1 and 0. The relation $1 = 0$ has not been ruled out in a ring, but it occurs only once:

(1.6) **Proposition.** Let R be a ring in which $1 = 0$. Then R is the zero ring.

Proof. We first note that $0a = 0$ for any element a of a ring R. The proof is the same as for vector spaces [Chapter 3 (1.6a)]. Assume that $1 = 0$ in R, and let a be any element of R. Then $a = 1a = 0a = 0$. So every element of R is 0, which means that R is the zero ring. □

Though multiplicative inverses are not required to exist in a ring, a particular element may have an inverse, and the inverse is unique if it exists. Elements which have multiplicative inverses are called *units*. For example, the units in the ring of integers are 1 and -1, and the units in the ring $\mathbb{R}[x]$ of real polynomials are the nonzero constant polynomials. Fields are rings which are not the zero ring and in which every nonzero element is a unit.

The identity element 1 of a ring is always a unit, and any reference to "the" unit element in R refers to the identity. This is ambiguous terminology, but it is too late to change it.

2. FORMAL CONSTRUCTION OF INTEGERS AND POLYNOMIALS

We learn that the ring axioms hold for the integers in elementary school. However, let us look again in order to see what is required in order to write down proofs of properties such as the associative and distributive laws. Complete proofs require a fair amount of writing, and we will only make a start here. It is customary to begin

by defining addition and multiplication for positive integers. Negative numbers are introduced later. This means that several cases have to be treated as one goes along, which is boring, or else a clever notation has to be found to avoid such a case analysis. We will content ourselves with a description of the operations on positive integers. Positive integers are also called *natural numbers*.

The set $\mathbb{N}$ of natural numbers is characterized by these properties, called *Peano's axioms:*

(2.1)

(a) The set $\mathbb{N}$ contains a particular element 1.

(b) *Successor function:* There is a map σ: $\mathbb{N} \longrightarrow \mathbb{N}$ that sends every integer $n \in \mathbb{N}$ to another integer, called the *next integer* or *successor*. This map is injective, and for every $n \in \mathbb{N}$, $\sigma(n) \neq 1$.

(c) *Induction axiom:* Suppose that a subset S of $\mathbb{N}$ has these properties:
(i) $1 \in S$;
(ii) if $n \in S$ then $\sigma(n) \in S$.
Then S contains every natural number: $S = \mathbb{N}$.

The next integer $\sigma(n)$ will turn into $n + 1$ when addition is defined. At this stage the notation $n + 1$ could be confusing. It is better to use a neutral notation, and we will often denote the successor by n' $[= \sigma(n)]$. Note that σ is assumed to be injective, so if m, n are distinct natural numbers, that is, if $m \neq n$, then m', n' are distinct too.

The successor function allows us to use the natural numbers for counting, which is the basis of arithmetic.

Property (c) is the induction property of the integers. Intuitively, it says that the natural numbers are obtained from 1 by repeatedly taking the next integer: $\mathbb{N} = \{1, 1', 1'', \ldots\}$ $(= \{1, 2, 3, \ldots\})$, that is, counting runs through all natural numbers. This property is the formal basis of induction proofs.

Suppose that a statement P_n is to be proved for every positive integer n, and let S be the set of integers n such that P_n is true. To say that P_n is true for every n is the same as saying that $S = \mathbb{N}$. For this set S, the Induction Axiom translates into the usual induction steps:

(2.2) (i) P_1 is true;
(ii) if P_n is true then $P_{n'}$ is true.

We can also use Peano's axioms to make recursive definitions. The phrase *recursive definition,* or *inductive definition,* refers to the definition of a sequence of objects C_n indexed by the natural numbers in which each object is defined in terms of the preceding one. The function $C_n = x^n$ is an example. A recursive definition of this function is

$$x^1 = x \quad \text{and} \quad x^{n'} = x^n x.$$

The important points are as follows:

(2.3) (i) C_1 is defined;
(ii) a rule is given for determining $C_{n'}$ $(= C_{n+1})$ from C_n.

It is intuitively clear that (2.3) determines the sequence C_n uniquely, though to prove this from Peano's axioms is tricky. A natural approach to proving it would be as follows: Let S be the set of integers n such that (2.3) determines C_k for every $k \leq n$. Then (2.3i) shows that $1 \in S$. Also, (2.3ii) shows that if $n \in S$ then $n' \in S$. The Induction Axiom shows that $S = \mathbb{N}$, hence that C_n is uniquely defined for each n. Unfortunately, the relation $\leq$ is not included in Peano's axioms, so it must be defined and its properties derived to start. A proof based on this approach is therefore lengthy, so we won't carry one out here.

Given the set of positive integers and the ability to make recursive definitions, we can define addition and multiplication of positive integers as follows:

(2.4) *Addition:* $m + 1 = m'$ and $m + n' = (m + n)'$.
Multiplication: $m \cdot 1 = m$ and $m \cdot n' = m \cdot n + m$.

In these definitions, we take an arbitrary integer m and then define addition and multiplication for that integer m and for every n recursively. In this way, $m + n$ and $m \cdot n$ are defined for all m and n.

The proofs of the associative, commutative, and distributive laws for the integers are exercises in induction which might be called "Peano playing." We will carry out two of the verifications here as samples.

Proof of the associative law for addition. We are to prove that $(a + b) + n = a + (b + n)$ for all $a, b, n \in \mathbb{N}$. We first check the case $n = 1$ for all a, b. Three applications of definition (2.4) give

$$(a + b) + 1 = (a + b)' = a + b' = a + (b + 1).$$

Next, assume the associative law true for a particular value of n and for all a, b. Then we verify it for n' as follows:

$$\begin{aligned}
(a + b) + n' &= (a + b) + (n + 1) && (\textit{definition}) \\
&= ((a + b) + n) + 1 && (\textit{case } n = 1) \\
&= (a + (b + n)) + 1 && (\textit{induction hypothesis}) \\
&= a + ((b + n) + 1) && (\textit{case } n = 1) \\
&= a + (b + (n + 1)) && (\textit{case } n = 1) \\
&= a + (b + n') && (\textit{definition}). \ \square
\end{aligned}$$

Proof of the commutative law for multiplication, assuming that the commutative law for addition has been proved. We first prove the following lemma:

(2.5) $$m' \cdot n = m \cdot n + n.$$

The case $n = 1$ is clear: $m' \cdot 1 = m' = m + 1 = m \cdot 1 + 1$. So assume that (2.5) is true for a particular n and for all values of m. We check it for n':

$$\begin{aligned} m' \cdot n' &= m' \cdot n + m' = m' \cdot n + (m + 1) && (\textit{definition}) \\ &= (m \cdot n + n) + (m + 1) && (\textit{induction}) \\ &= (m \cdot n + m) + (n + 1) && (\textit{various laws for addition}) \\ &= m \cdot n' + n' && (\textit{definition}). \end{aligned}$$

Next, we check that $1 \cdot n = n$ by induction on n. Finally, we show that $m \cdot n = n \cdot m$ by induction on n, knowing that $m \cdot 1 = m = 1 \cdot m$: Assume it true for n. Then $m \cdot n' = m \cdot n + m = n \cdot m + m = n' \cdot m$, as required. □

The proofs of other properties of addition and multiplication follow similar lines.

We now turn to the definition of polynomial rings. We can define the notion of a *polynomial* with coefficients in any ring R to mean a linear combination of powers of the variable:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \tag{2.6}$$

where $a_i \in R$. Such expressions are often called *formal polynomials,* to distinguish them from polynomial functions. Every formal polynomial with real coefficients determines a polynomial function on the real numbers.

The variable x appearing in (2.6) is an arbitrary symbol, and the monomials x^i are considered independent. This means that if

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

is another polynomial with coefficients in R, then $f(x)$ and $g(x)$ are equal if and only if $a_i = b_i$ for all $i = 0, 1, 2, \ldots$.

The *degree* of a nonzero polynomial is the largest integer k such that the coefficient a_k of x^k is not zero. (The degree of the zero polynomial is considered indeterminate.) The coefficient of highest degree of a polynomial which is not zero is called its *leading coefficient,* and a *monic* polynomial is one whose leading coefficient is 1.

The possibility that some of the coefficients of a polynomial may be zero creates a nuisance. We have to disregard terms with zero coefficient: $x^2 + 3 = 0x^3 + x^2 + 3$, for example. So the polynomial $f(x)$ has more than one representation (2.6). One way to standardize notation is to list the nonzero coefficients only, that is, to omit from (2.6) all terms $0x^i$. But zero coefficients may be produced in the course of computations, and they will have to be thrown out. Another possibility is to insist that the highest degree coefficient a_n of (2.6) be nonzero and to list all those of lower degree. The same problem arises. Such conventions therefore require a discussion of special cases in the description of the ring structure. This is irritating, because the ambiguity caused by zero coefficients is not an interesting point.

One way around the notational problem is to list the coefficients of *all* monomials, zero or not. This isn't good for computation, but it allows efficient

verification of the ring axioms. So for the purpose of defining the ring operations, we will write a polynomial in the standard form

$$f(x) = a_0 + a_1x + a_1x^2 + \cdots, \tag{2.7}$$

where the coefficients a_i are all in the ring R and *only finitely many of the coefficients are different from zero.* Formally, the polynomial (2.7) is determined by its vector (or sequence) of coefficients a_i:

$$a = (a_0, a_1, \ldots), \tag{2.8}$$

where $a_i \in R$ and all but a finite number of a_i are zero. Every such vector corresponds to a polynomial. In case R is a field, these infinite vectors form the vector space Z with the infinite basis e_i which was defined in Chapter 3 (5.2d). The vector e_i corresponds to the *monomial* x^i, and the monomials form a basis of the space of all polynomials.

Addition and multiplication of polynomials mimic the familiar operations on real polynomial functions. Let $f(x)$ be as above, and let

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots \tag{2.9}$$

be another polynomial with coefficients in the same ring R, determined by the vector $b = (b_0, b_1, \ldots)$. The *sum* of f and g is

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots \\ &= \sum_k (a_k + b_k)x^k, \end{aligned} \tag{2.10}$$

which corresponds to vector addition: $a + b = (a_0 + b_0, a_1 + b_1, \ldots)$.

The *product* of two polynomials f, g is computed by multiplying term by term and collecting coefficients of the same degree in x. If we expand the product using the distributive law, but without collecting terms, we obtain

$$f(x)g(x) = \sum_{i,j} a_ib_jx^{i+j}. \tag{2.11}$$

Note that there are finitely many nonzero coefficients a_ib_j. This is a correct formula, but the right side is not in the standard form (2.7) because the same monomial x^n appears many times—once for each pair i, j of indices such that $i + j = n$. So terms have to be collected to put the right side back into standard form. This leads to the definition

$$f(x)g(x) = p_0 + p_1x + p_2x^2 + \cdots,$$

where

$$p_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 = \sum_{i+j=k} a_ib_j. \tag{2.12}$$

However, it may be desirable to defer the collection of terms for a while when making computations.

(2.13) **Proposition.** There is a unique commutative ring structure on the set of polynomials $R[x]$ having these properties:

(a) Addition of polynomials is vector addition (2.10).
(b) Multiplication of monomials is given by the rule (2.12).
(c) The ring R is a subring of $R[x]$, when the elements of R are identified with the constant polynomials.

The proof of this proposition is notationally unpleasant without having any interesting features, so we omit it. □

Polynomials are fundamental to the theory of rings, and we must also consider polynomials, such as $x^2y^2 + 4x^3 - 3x^2y - 4y^2 + 2$, in several variables. There is no major change in the definitions.

Let $x_1,\dots,x_n$ be variables. A *monomial* is a formal product of these variables, of the form

$$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n},$$

where the exponents i_ν are nonnegative integers. The n-tuple $(i_1,\dots i_n)$ of exponents determines the monomial. Such an n-tuple is called a *multi-index*, and vector notation $i = (i_1,\dots,i_n)$ for multi-indices is very convenient. Using it, we may write the monomial symbolically as

$$x^i = x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}. \tag{2.14}$$

The monomial x^0, where $0 = (0,\dots,0)$, is denoted by 1.

A *polynomial* with coefficients in a ring R is a finite linear combination of monomials, with coefficients in R. Using the shorthand notation (2.14), any polynomial $f(x) = f(x_1,\dots,x_n)$ can be written in exactly one way in the form

$$f(x) = \sum_i a_i x^i, \tag{2.15}$$

where i runs through all multi-indices $(i_1,\dots,i_n)$, the coefficients a_i are in R, and only finitely many of these coefficients are different from zero.

A polynomial which is the product of a monomial by a nonzero element of R is also called a *monomial*. Thus

$$m = rx^i \tag{2.17}$$

is a monomial if $r \in R$ is not zero and if x^i is as above (2.14). A monomial can be thought of as a polynomial which has exactly one nonzero coefficient.

Using multi-index notation, formulas (2.10) and (2.12) define addition and multiplication of polynomials in several variables, and the analogue of Proposition (2.13) is true.

The ring of polynomials with coefficients in R is denoted by one of the symbols

$$R[x_1,\dots,x_n] \quad \text{or} \quad R[x], \tag{2.16}$$

where the symbol x is understood to refer to the set of variables $(x_1,\dots,x_n)$. When no set of variables has been introduced, $R[x]$ refers to the polynomial ring in one variable x.

3. HOMOMORPHISMS AND IDEALS

A *homomorphism* $\varphi\colon R \longrightarrow R'$ from one ring to another is a map which is compatible with the laws of composition and which carries 1 to 1, that is, a map such that

$$(3.1)\qquad \varphi(a+b) = \varphi(a) + \varphi(b),\quad \varphi(ab) = \varphi(a)\varphi(b),\quad \varphi(1_R) = 1_{R'},$$

for all $a, b \in R$. An *isomorphism* of rings is a bijective homomorphism. If there is an isomorphism $R \longrightarrow R'$, the two rings are said to be *isomorphic*.

A word about the third part of (3.1) is in order. The assumption that a homomorphism φ is compatible with addition implies that it is a group homomorphism $R^+ \longrightarrow R'^+$. We know that a group homomorphism carries the identity to the identity, so $f(0) = 0$. But R is not a group with respect to $\times$, and we can't conclude that $\varphi(1) = 1$ from compatibility with multiplication. So the condition $\varphi(1) = 1$ must be listed separately. For example, the *zero map* $R \longrightarrow R'$ sending all elements of R to zero is compatible with $+$ and $\times$, but it doesn't send 1 to 1 unless $1 = 0$ in R'. The zero map isn't a ring homomorphism unless R' is the zero ring [see (1.6)].

The most important ring homomorphisms are those obtained by evaluating polynomials. Evaluation of real polynomials at a real number a defines a homomorphism

$$(3.2)\qquad \mathbb{R}[x] \longrightarrow \mathbb{R},\quad \text{sending } p(x) \rightsquigarrow p(a).$$

We can also evaluate real polynomials at a complex number such as i, to obtain a homomorphism

$$(3.3)\qquad \mathbb{R}[x] \longrightarrow \mathbb{C},\quad \text{sending } p(x) \rightsquigarrow p(i).$$

The general formulation of the principle of evaluation of polynomials is this:

(3.4) **Proposition.** *Substitution Principle:* Let $\varphi\colon R \longrightarrow R'$ be a ring homomorphism.

(a) Given an element $\alpha \in R'$, there is a unique homomorphism $\Phi\colon R[x] \longrightarrow R'$ which agrees with the map φ on constant polynomials and which sends $x \rightsquigarrow \alpha$.

(b) More generally, given elements $\alpha_1,\dots,\alpha_n \in R'$, there is a unique homomorphism $\Phi\colon R[x_1,\dots,x_n] \longrightarrow R'$ from the polynomial ring in n variables to R', which agrees with φ on constant polynomials and which sends $x_\nu \rightsquigarrow \alpha_\nu$, for $\nu = 1,\dots,n$.

Proof. With vector notation for indices, the proof of (b) is the same as that of (a). Let us denote the image of an element $r \in R$ in R' by r'. Using the fact that Φ

is a homomorphism which restricts to φ on R and sends x_ν to α_ν, we find that it acts on a polynomial $f(x) = \sum r_i x^i$ by sending

$$\sum r_i x^i \rightsquigarrow \sum \varphi(r_i)\alpha^i = \sum r_i'\alpha^i. \tag{3.5}$$

In other words, Φ acts on the coefficients of a polynomial as φ, and it substitutes α for x. Since this formula describes Φ for us, we have proved the uniqueness of the substitution homomorphism. To prove its existence, we take this formula as the definition of Φ, and we show that this map is a homomorphism $R[x] \longrightarrow R'$. It is easy to show that Φ sends 1 to 1 and that it is compatible with addition of polynomials. Compatibility with multiplication can be checked using formula (2.11):

$$\Phi(fg) = \Phi(\sum a_i b_j x^{i+j}) = \sum \Phi(a_i b_j x^{i+j}) = \sum_{i,j} a_i' b_j' \alpha^{i+j}$$

$$= (\sum_i a_i'\alpha^i)(\sum_j b_j'\alpha^j) = \Phi(f)\Phi(g). \square$$

Here is an example of the Substitution Principle in which the coefficient ring R changes: Let $\psi\colon R \longrightarrow R_1$ be a ring homomorphism. Composing ψ with the inclusion of R_1 as a subring of $R_1[x]$, we obtain a homomorphism $\varphi\colon R \longrightarrow R_1[x]$. The Substitution Principle asserts that there is a unique extension of φ to a homomorphism $\Phi\colon R[x] \longrightarrow R_1[x]$ which sends $x \rightsquigarrow x$. This is the map which operates on the coefficients of a polynomial, leaving the variable x fixed. If we denote $\psi(a)$ by a', then it sends a polynomial $a_n x^n + \cdots + a_1 x + a_0$ to $a_n' x^n + \cdots + a_1' x + a_0'$.

An important case is the homomorphism $\mathbb{Z} \longrightarrow \mathbb{F}_p$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements. This map extends to a homomorphism

$$\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x], \text{ sending} \tag{3.6}$$

$$f(x) = a_n x^n + \cdots + a_0 \rightsquigarrow \bar{a}_n x^n + \cdots + \bar{a}_0 = \bar{f}(x),$$

where $\bar{a}_i$ denotes the residue class of a_i modulo p. It is natural to call the polynomial $\bar{f}(x)$ the *residue of* $f(x)$ *modulo* p.

The Substitution Principle is also an efficient way to prove that various constructions of polynomial rings are equivalent; the isomorphism

$$R[x, y] \approx R[x][y]$$

is a typical example. Here the right side stands for the ring of polynomials in y whose coefficients are polynomials in x. The statement that these rings are isomorphic is a formalization of the procedure of collecting terms of like degree in y in a polynomial $f(x, y)$, to write it as a polynomial in y. For example,

$$x^2y^2 + 4x^3 - 3x^2y - 4y^2 + 2 = (x^2 - 4)y^2 - (3x^2)y + (4x^3 + 2).$$

(3.7) **Corollary.** Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_n)$ denote sets of variables. There is a unique isomorphism $R[x, y] \longrightarrow R[x][y]$ which is the identity on R and which sends the variables to themselves.

Proof. Note that R is a subring of $R[x]$, and that $R[x]$ is a subring of $R[x][y]$. So R is also a subring of $R[x][y]$. Consider the inclusion map $\varphi\colon R \longrightarrow R[x][y]$. The Substitution Principle (3.4) tells us that there is a unique homomorphism $\Phi\colon R[x,y] \longrightarrow R[x][y]$ which extends this map and sends the variables x_μ, y_ν wherever we like. So we can send the variables to themselves. The map Φ thus constructed is the required isomorphism. We can show that it has an inverse by using the Substitution Principle once more: We note that $R[x]$ is a subring of $R[x,y]$, so we can extend the inclusion map $\psi\colon R[x] \longrightarrow R[x,y]$ to a map $\Psi\colon R[x][y] \longrightarrow R[x,y]$ by sending y_j to itself. The composed homomorphism $\Psi\Phi\colon R[x,y] \longrightarrow R[x,y]$ is the identity on R and on $\{x_\mu, y_\nu\}$. By the uniqueness of the substitution homomorphism, $\Psi\Phi$ is the identity map. Similarly, $\Phi\Psi$ is the identity. This proves that Φ is an isomorphism. □

Since a real polynomial $f(x)$ can be evaluated at a real number, it defines a polynomial function on the real line. The term *polynomial* is often used to refer to a function obtained in this way, and not much danger is involved in doing this, because we can recover the polynomial from its function:

(3.8) **Proposition.** Let $\mathcal{R}$ denote the ring of continuous real-valued functions on $\mathbb{R}^n$. The map $\varphi\colon \mathbb{R}[x_1,\dots,x_n] \longrightarrow \mathcal{R}$ sending a polynomial to its associated polynomial function is an injective homomorphism.

Proof. The existence of this homomorphism follows from the Substitution Principle. Let us prove injectivity. It is enough to show that if the function associated to a polynomial $f(x)$ is the zero function, then $f(x)$ is the zero polynomial. Let the associated function be $\tilde{f}(x)$. If $\tilde{f}(x)$ is identically zero, then all its derivatives are zero too. On the other hand, we can differentiate a formal polynomial by using the rule for differentiating polynomial functions. If some coefficient of our polynomial f is not zero, then the constant term of a suitable derivative will be nonzero too. So that derivative will not vanish at the origin. Therefore $\tilde{f}(x)$ can't be the zero function. □

Another important example of a ring homomorphism is the map from the integers to an arbitrary ring:

(3.9) **Proposition.** There is exactly one homomorphism

$$\varphi\colon \mathbb{Z} \longrightarrow R$$

from the ring of integers to an arbitrary ring R. It is the map defined by $\varphi(n) =$ "n times 1_R" $= 1_R + \cdots + 1_R$ (n times) if $n > 0$, and $\varphi(-n) = -\varphi(n)$.

Sketch of Proof. Let $\varphi\colon \mathbb{Z} \longrightarrow R$ be a homomorphism. By the definition of homomorphism, $\varphi(1) = 1_R$, and $\varphi(n+1) = \varphi(n) + \varphi(1)$. So φ is determined on the natural numbers by the recursive definition

$$\varphi(1) = 1 \quad \text{and} \quad \varphi(n') = \varphi(n) + 1,$$

where $'$ denotes the successor function (2.1b). This formula, together with $\varphi(-n) = -\varphi(n)$ if $n > 0$ and $\varphi(0) = 0$, determines φ uniquely. So the above map is the only possible one. To give a formal proof that this map is a homomorphism, we must go back to Peano's axioms. Let us verify that φ is compatible with addition of positive integers. To prove that $\varphi(m + n) = \varphi(m) + \varphi(n)$, we note that this is true when $n = 1$, by the definition of φ. Assume it true for all m and some particular n. Then we prove it for all m and for n':

$$\begin{aligned}
\varphi(m + n') &= \varphi((m + n) + 1) && \textit{(properties of addition of integers)} \\
&= \varphi(m + n) + 1 && \textit{(definition of } \varphi\textit{)} \\
&= \varphi(m) + \varphi(n) + 1 && \textit{(induction hypothesis)} \\
&= \varphi(m) + \varphi(n') && \textit{(definition of } \varphi\textit{)}.
\end{aligned}$$

By induction, $\varphi(m + n) = \varphi(m) + \varphi(n)$ for all m and n. We leave the proof of compatibility with multiplication of positive integers as an exercise. □

This proposition allows us to identify the images of the integers in an arbitrary ring R. Thus we can interpret the symbol 3 as the element $1 + 1 + 1$ in R, and we can interpret an integer polynomial such as $3x^2 + 2x$ as an element of the polynomial ring $R[x]$.

We now go back to an arbitrary ring homomorphism $\varphi\colon R \longrightarrow R'$. The *kernel* of φ is defined in the same way as the kernel of a group homomorphism:

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0\}.$$

As you will recall, the kernel of a group homomorphism is a subgroup, and in addition it is normal [Chapter 2 (4.9)]. Similarly, the kernel of a ring homomorphism is closed under the ring operations of addition and multiplication, and it also has a stronger property than closure under multiplication:

(3.10) *If $a \in \ker \varphi$ and $r \in R$, then $ra \in \ker \varphi$.*

For if $\varphi(a) = 0$, then $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$. On the other hand, $\ker \varphi$ does not contain the unit element 1 of R, and so *the kernel is not a subring*, unless it is the whole ring R. (If $1 \in \ker \varphi$, then $r = r1 \in \ker \varphi$ for all $r \in R$.) Moreover, if $\ker \varphi = R$, then φ is the zero map, and by what was said above, R' is the zero ring.

For example, let φ be the homomorphism $\mathbb{R}[x] \longrightarrow \mathbb{R}$ defined by evaluation at the real number 2. Then $\ker \varphi$ is the set of polynomials which have 2 as a root. It can also be described as the set of polynomials divisible by $x - 2$.

The property of the kernel of a ring homomorphism—that it is closed under multiplication by arbitrary elements of the ring—is abstracted in the concept of an *ideal*. An ideal I of a ring R is, by definition, a subset of R with these properties:

(3.11)

(i) I is a subgroup of R^+;

(ii) If $a \in I$ and $r \in R$, then $ra \in I$.

This peculiar term "ideal" is an abbreviation of "ideal element," which was formerly used in number theory. We will see in Chapter 11 how the term arose. Property (ii) implies that an ideal is closed under multiplication, but it is stronger. A good way to think of properties (i) and (ii) together is this equivalent formulation:

(3.12) *I is not empty, and a linear combination $r_1a_1 + \cdots + r_ka_k$ of elements $a_i \in I$ with coefficients $r_i \in R$ is in I.*

In any ring R, the set of multiples of a particular element a, or equivalently, the set of elements divisible by a, forms an ideal called the *principal ideal* generated by a. This ideal will be denoted in one of the following ways:

$$(a) = aR = Ra = \{ra \mid r \in R\}. \tag{3.13}$$

Thus the kernel of the homomorphism $\mathbb{R}[x] \longrightarrow \mathbb{R}$ defined by evaluation at 2 may be denoted by $(x - 2)$ or by $(x - 2)\mathbb{R}[x]$. Actually the notation (a) for a principal ideal, though convenient, is ambiguous because the ring is not mentioned. For instance, $(x - 2)$ may stand for an ideal in $\mathbb{R}[x]$ or in $\mathbb{Z}[x]$, depending on the circumstances. When there are several rings around, a different notation may be preferable.

We may also consider the ideal I *generated by* a set of elements $a_1, \ldots, a_n$ of R, which is defined to be the smallest ideal containing the elements. It can be described as the set of all linear combinations

$$r_1a_1 + \cdots + r_na_n, \tag{3.14}$$

with coefficients r_i in the ring. For if an ideal contains $a_1, \ldots, a_n$, then (3.12) tells us that it contains every linear combination of these elements. On the other hand, the set of linear combinations is closed under addition, subtraction, and multiplication by elements of R. Hence it is the ideal I. This ideal is often denoted by

$$(a_1, \ldots, a_n) = \{r_1a_1 + \cdots + r_na_n \mid r_i \in R\}. \tag{3.15}$$

For example, if R is the ring $\mathbb{Z}[x]$ of integer polynomials, the notation $(2, x)$ stands for the ideal of linear combinations of 2 and x with integer polynomial coefficients. This ideal can also be described as the set of all integer polynomials $f(x)$ whose constant term is divisible by 2. It is the kernel of the homomorphism $\mathbb{Z}[x] \longrightarrow \mathbb{Z}/2\mathbb{Z}$ defined by $f(x) \rightsquigarrow$ (*residue of* $f(0)$ (modulo 2)).

For the rest of this section, we will describe ideals in some simple cases. In any ring R, the set consisting of zero alone is an ideal, called the *zero ideal*. It is obviously a principal ideal, as is the whole ring. Being generated as an ideal by the element 1, R is called the *unit ideal*, often denoted by (1). The unit ideal is the only ideal which contains a unit. An ideal I is said to be *proper* if it is not (0) or (1).

Fields can be characterized by the fact that they have no proper ideals:

(3.16) **Proposition.**

(a) Let F be a field. The only ideals of F are the zero ideal and the unit ideal.

(b) Conversely, if a ring R has exactly two ideals, then R is a field.

Let us prove (b). Assume that R has exactly two ideals. The properties that distinguish fields among rings are that $1 \neq 0$ and that every nonzero element $a \in R$ has a multiplicative inverse. As we saw above, $1 = 0$ occurs only in the zero ring, which has one element. This ring has only one ideal. Since our ring has two ideals, $1 \neq 0$ in R. The two ideals (1) and (0) are different, so they are the only two ideals of R.

We now show that every nonzero element of R has an inverse. Let $a \in R$ be a nonzero element, and consider the principal ideal (a). Then $(a) \neq (0)$ because $a \in (a)$. Therefore $(a) = (1)$. This implies that 1 is a multiple, say ra, of a. The equation $ar = 1$ shows that a has an inverse. □

(3.17) **Corollary.** Let F be a field and let R' be a nonzero ring. Every homomorphism $\varphi: F \longrightarrow R'$ is injective.

Proof. We apply (3.16). If $\ker \varphi = (1)$, then φ is the zero map. But the zero map isn't a homomorphism because R' isn't the zero ring. Therefore $\ker \varphi = (0)$. □

It is also easy to determine the ideals in the ring of integers.

(3.18) **Proposition.** Every ideal in the ring $\mathbb{Z}$ of integers is a principal ideal.

This is because every subgroup of the additive group $\mathbb{Z}^+$ of integers is of the form $n\mathbb{Z}$ [Chapter 2 (2.3)], and these subgroups are precisely the principal ideals. □

The *characteristic* of a ring R is the nonnegative integer n which generates the kernel of the homomorphism $\varphi: \mathbb{Z} \longrightarrow R$ (3.9). This means that n is the smallest positive integer such that "n times 1_R" $= 0$ or, if the kernel is (0), the characteristic is zero (see Chapter 3, Section 2). Thus $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}$ have characteristic zero, while the field $\mathbb{F}_p$ with p elements has characteristic p.

The proof that every ideal of the ring of integers is principal can be adapted to show that every ideal in the polynomial ring $F[x]$ is principal. To prove this, we need division with remainder for polyomials.

(3.19) **Proposition.** Let R be a ring and let f, g be polynomials in $R[x]$. Assume that the leading coefficient of f is a unit in R. (This is true, for instance, if f is a monic polynomial.) Then there are polynomials $q, r \in R[x]$ such that

$$g(x) = f(x)q(x) + r(x),$$

and such that the degree of the remainder r is less than the degree of f or else $r = 0$.

This division with remainder can be proved by induction on the degree of g. □

Note that when the coefficient ring is a field, the assumption that the leading coefficient of f is a unit is satisfied, provided only that there is a leading coefficient, that is, that $f \neq 0$.

(3.20) **Corollary.** Let $g(x)$ be a monic polynomial in $R[x]$, and let α be an element of R such that $g(\alpha) = 0$. Then $x - \alpha$ divides g in $R[x]$. □

(3.21) **Proposition.** Let F be a field. Every ideal in the ring $F[x]$ of polynomials in a single variable x is a principal ideal.

Proof. Let I be an ideal of $F[x]$. Since the zero ideal is principal, we may assume that $I \neq (0)$. The first step in finding a generator for a nonzero subgroup of $\mathbb{Z}$ is to choose its smallest positive element. Our substitute here is to choose a nonzero polynomial f in I of minimal degree. We claim that I is the principal ideal generated by f. It follows from the definition of an ideal that the principal ideal (f) is contained in I. To prove that $I \subset (f)$, we use division with remainder to write $g = fq + r$, where r has lower degree than f, unless it is zero. Now if g is in the ideal I, then since $f \in I$ the definition of an ideal shows that $r = g - fq$ is in I too. Since f has minimal degree among nonzero elements, the only possibility is that $r = 0$. Thus f divides g, as required. □

The proof of the following corollary is similar to that of (2.6) in Chapter 2.

(3.22) **Corollary.** Let F be a field, and let f,g be polynomials in $F[x]$ which are not both zero. There is a unique monic polymomial $d(x)$ called the *greatest common divisor* of f and g, with the following properties:

(a) d generates the ideal (f, g) of $F[x]$ generated by the two polynomials f, g.
(b) d divides f and g.
(c) If h is any divisor of f and g, then h divides d.
(d) There are polynomials $p,q \in F[x]$ such that $d = pf + qg$. □

4. QUOTIENT RINGS AND RELATIONS IN A RING

Let I be an ideal of a ring R. The cosets of the additive subgroup I^+ of R^+ are the subsets

$$a + I, \quad a \in R.$$

It follows from what has been proved for groups that the set of cosets $R/I = \bar{R}$ is a group under addition. It is also a ring:

(4.1) **Theorem.** Let I be an ideal of a ring R.

(a) There is a unique ring structure on the set of cosets $\bar{R} = R/I$ such that the canonical map $\pi: R \longrightarrow \bar{R}$ sending $a \rightsquigarrow \bar{a} = a + I$ is a homomorphism.
(b) The kernel of π is I.

Proof. This proof has already been carried out in the special case that R is the ring of integers (Chapter 2, Section 9). We want to put a ring structure on $\bar{R}$ with the required properties, and if we forget about multiplication and consider only the addition law, the proof has already been given [Chapter 2 (10.5)]. What is left to do is to define multiplication. Let $x,y \in \bar{R}$, and say that $x = \bar{a} = a + I$ and $y = \bar{b} =$

$b + I$. We would like to define the product to be $xy = \overline{ab} = ab + I$. In contrast with coset multiplication in a group [Chapter 2 (10.1)], the set of products

$$P = \{rs \mid r \in a + I, s \in b + I\}$$

is not always a coset of I. However, as in the case of the ring of integers, the set P is always contained in the single coset $ab + I$: If we write $r = a + u$ and $s = b + v$ with $u, v \in I$, then

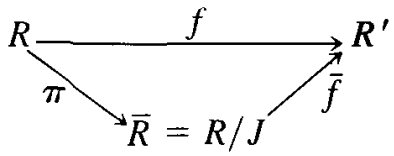
$$(a + u)(b + v) = ab + (av + bu + uv),$$

and since I is an ideal, $av + bu + uv \in I$. This is all that is needed to define the product coset: It is the coset which contains the set P. This coset is unique because the cosets partition R. The proof of the remaining assertions closely follows the pattern of Chapter 2, Section 9. □

As in Chapter 6 (8.4) and Chapter 2 (10.9), one can show the following:

(4.2) **Proposition.** *Mapping property of quotient rings:* Let $f\colon R \longrightarrow R'$ be a ring homomorphism with kernel I and let J be an ideal which is contained in I. Denote the residue ring R/J by $\bar{R}$.

(a) There is a unique homomorphism $\bar{f}\colon \bar{R} \longrightarrow R'$ such that $\bar{f}\pi = f$:



(b) *First Isomorphism Theorem:* If $J = I$, then $\bar{f}$ maps $\bar{R}$ isomorphically to the image of f. □

We will now describe the fundamental relationship between ideals in a quotient ring R/J and ideals in the original ring R.

(4.3) **Proposition.** *Correspondence Theorem:* Let $\bar{R} = R/J$, and let π denote the canonical map $R \longrightarrow \bar{R}$.

(a) There is a bijective correspondence between the set of ideals of R which contain J and the set of all ideals of $\bar{R}$, given by

$$I \rightsquigarrow \pi(I) \quad \text{and} \quad \pi^{-1}(\bar{I}) \leftsquigarrow \bar{I}.$$

(b) If $I \subset R$ corresponds to $\bar{I} \subset \bar{R}$, then R/I and $\bar{R}/\bar{I}$ are isomorphic rings.

The second part of this proposition is often called the *Third Isomorphism Theorem.* [There is also a *Second Isomorphism Theorem* (see Chapter 6, miscellaneous exercise 7)].

Proof. To prove (a), we must check the following points:

(i) If I is an ideal of R which contains J, then $\pi(I)$ is an ideal of $\bar{R}$.
(ii) If $\bar{I}$ is an ideal of $\bar{R}$, then $\pi^{-1}(\bar{I})$ is an ideal of R.
(iii) $\pi^{-1}(\pi(\bar{I})) = I$ and $\pi(\pi^{-1}(\bar{I})) = \bar{I}$.

We know that the image of a subgroup is a subgroup [Chapter 2 (4.4)]. So to show that $\pi(I)$ is an ideal of $\bar{R}$, we need only prove that it is closed under multiplication by elements of $\bar{R}$. Let $\bar{r} \in \bar{R}$, and let $\bar{x} \in \pi(I)$. We write $\bar{r} = \pi(r)$ for some $r \in R$, and $\bar{x} = \pi(x)$ for some $x \in I$. Then $\bar{r}\bar{x} = \pi(rx)$ and $rx \in I$. So $\bar{r}\bar{x} \in \pi(I)$. Note that this proof works for all ideals I of R. We do not need the assumption that $I \supset J$ at this point. However, the fact that π is surjective is essential.

Next, we denote the homomorphism $\bar{R} \longrightarrow \bar{R}/\bar{I}$ by φ, and we consider the composed homomorphism $R \xrightarrow{\pi} \bar{R} \xrightarrow{\varphi} \bar{R}/\bar{I}$. Since π and φ are surjective, so is $\varphi \circ \pi$. Moreover, the kernel of $\varphi \circ \pi$ is the set of elements $r \in R$ such that $\pi(r) \in \bar{I} = \ker \varphi$. By definition, this is $\pi^{-1}(\bar{I})$. Therefore $\pi^{-1}(\bar{I})$, being the kernel of a homomorphism, is an ideal of R. This proves (ii). Also, the First Isomorphism Theorem applies to the homomorphism $\varphi \circ \pi$ and shows that $R/\pi^{-1}(\bar{I})$ is isomorphic to $\bar{R}/\bar{I}$. This proves part (b) of the proposition.

It remains to prove (iii); remember that π^{-1} isn't usually a map. The inclusions $\pi^{-1}(\pi(I)) \supset I$ and $\pi(\pi^{-1}(\bar{I})) \subset \bar{I}$ are general properties of any map of sets and for arbitrary subsets. Moreover, the equality $\pi(\pi^{-1}(\bar{I})) = \bar{I}$ holds for any surjective map of sets. We omit the verification of these facts. The final point, that $\pi^{-1}(\pi(I)) \subset I$, is the one which requires that $I \supset J$. Let $x \in \pi^{-1}(\pi(I))$. Then $\pi(x) \in \pi(I)$, so there is an element $y \in I$ such that $\pi(y) = \pi(x)$. Since π is a homomorphism, $\pi(x - y) = 0$ and $x - y \in J = \ker \pi$. Since $y \in I$ and $J \subset I$, this implies that $x \in I$, as required. □

The quotient construction has an important interpretation in terms of *relations* among elements in a ring R. Let us imagine performing a sequence of operations $+, -, \times$ on some elements of R to get a new element a. If the resulting element a is zero, we say that the given elements are related by the equation

$$a = 0. \tag{4.4}$$

For instance, the elements 2, 3, 6 of the ring $\mathbb{Z}$ are related by the equation $2 \times 3 - 6 = 0$.

Now if the element a is not zero, we may ask whether it is possible to modify R in such a way that (4.4) becomes true. We can think of this process as adding a new relation, which will collapse the ring. For example, the relation $3 \times 4 - 5 = 0$ does not hold in $\mathbb{Z}$, because $3 \times 4 - 5 = 7$. But we can impose the relation $7 = 0$ on the integers. Doing so amounts to working modulo 7.

At this point we can forget about the procedure which led us to the particular element a; let it be an arbitrary element of R. Now when we modify R to impose the relation $a = 0$, we want to keep the operations $+$ and $\times$, so we will have to accept some consequences of this relation. For example, $ra = 0$ and $b + a = b$ are the

consequences of multiplying and adding given elements to both sides of $a = 0$. Performing these operations in succession gives us the consequence

$$b + ra = b. \tag{4.5}$$

If we want to set $a = 0$, we must also set $b + ra = b$ for all $b, r \in R$. Theorem (4.1) tells us that this is enough: There are no other consequences of (4.4). To see this, note that if we fix an element b but let r vary, the set $\{b + ra\}$ is the coset $b + (a)$, where $(a) = aR$ is the principal ideal generated by a. Setting $b + ra = b$ for all r is the same as equating the elements of this coset. This is precisely what happens when we pass from R to the quotient ring $\bar{R} = R/(a)$. The elements of $\bar{R}$ are the cosets $\bar{b} = b + (a)$, and the canonical map $\pi\colon R \longrightarrow \bar{R}$ carries all the elements $b + ra$ in one coset to the same element $\bar{b} = \pi(b)$. So exactly the right amount of collapsing has taken place in $\bar{R}$. Also, $\bar{a} = 0$, because a is an element of the ideal (a), which is the kernel of π. So it is reasonable to view $\bar{R} = R/(a)$ as the ring obtained by introducing the relation $a = 0$ into R.

If our element a was obtained from some other elements by a sequence of ring operations, as we supposed in (4.4), then the fact that π is a homomorphism implies that the same sequence of operations gives 0 in $\bar{R}$. Thus if $uv + w = a$ for some $u, v, w \in R$, then the relation

$$\bar{u}\,\bar{v} + \bar{w} = 0 \tag{4.6}$$

holds in $\bar{R}$. For, since π is a homomorphism, $\bar{u}\,\bar{v} + \bar{w} = \overline{uv + w} = \bar{a} = 0$.

A good example of this construction is the relation $n = 0$ in the ring of integers $\mathbb{Z}$. The resulting ring is $\mathbb{Z}/n\mathbb{Z}$.

More generally, we can introduce any number of relations $a_1 = \ldots = a_n = 0$, by taking the ideal I generated by $a_1, \ldots, a_n$ (3.15), which is the set of linear combinations $\{r_1a_1 + \cdots + r_na_n \mid r_i \in R\}$. The quotient ring $\bar{R} = R/I$ should be viewed as the ring obtained by introducing the n relations $a_1 = 0, \ldots, a_n = 0$ into R. Since $a_i \in I$, the residues $\bar{a}_i$ are zero. Two elements b, b' of R have the same image in $\bar{R}$ if and only if $b' - b \in I$, or $b' = b + r_1a_1 + \cdots + r_na_n$, for some $r_i \in R$. Thus the relations

$$b + r_1a_1 + \cdots + r_na_n = b \tag{4.7}$$

are the only consequences of $a_1 = \cdots = a_n = 0$.

It follows from the Third Isomorphism Theorem (4.3b) that introducing relations one at a time or all together leads to isomorphic results. To be precise, let a, b be elements of a ring R, and let $\bar{R} = R/(a)$ be the result of killing a. Introducing the relation $\bar{b} = 0$ into the ring $\bar{R}$ leads to the quotient ring $\bar{R}/(\bar{b})$, and this ring is isomorphic to the quotient $R/(a, b)$ obtained by killing a and b at the same time, because (a, b) and $(\bar{b})$ are corresponding ideals [see (4.3)].

Note that the more relations we add, the more collapsing takes place in the map $R \longrightarrow \bar{R}$. If we add them carelessly, the worst that can happen is that we may end up with $I = R$ and $\bar{R} = 0$. All relations $a = 0$ become true when we collapse R to the zero ring.

The procedure of introducing relations will lead to a new ring in most cases. That is why it is so important. But in some simple cases the First Isomorphism Theorem can be used to relate the ring obtained to a more familiar one. We will work out two examples to illustrate this.

Let $R = \mathbb{Z}[i]$ be the ring of Gauss integers, and let $\bar{R}$ be obtained by introducing the relation $1 + 3i = 0$. So $\bar{R} = R/I$ where I is the principal ideal generated by $1 + 3i$. We begin by experimenting with the relation, looking for recognizable consequences. Multiplying $-1 = 3i$ on both sides by $-i$, we obtain $i = 3$. So $i = 3$ in $\bar{R}$. On the other hand, $i^2 = -1$ in R, and hence in $\bar{R}$ too. Therefore $3^2 = -1$, or $10 = 0$, in $\bar{R}$. Since $i = 3$ and $10 = 0$ in $\bar{R}$, it is reasonable to guess that $\bar{R}$ is isomorphic to $\mathbb{Z}/(10) = \mathbb{Z}/10\mathbb{Z}$.

(4.8) **Proposition.** The ring $\mathbb{Z}[i]/(1 + 3i)$ is isomorphic to the ring $\mathbb{Z}/10\mathbb{Z}$ of integers modulo 10.

Proof. Having made this guess, we can prove it by analyzing the homomorphism $\varphi\colon \mathbb{Z} \longrightarrow \bar{R}$ (3.9). By the First Isomorphism Theorem, $\text{im } \varphi \approx \mathbb{Z}/(\ker \varphi)$. So if we show that φ is surjective and that $\ker \varphi = 10\mathbb{Z}$, we will have succeeded. Now every element of $\bar{R}$ is the residue of a Gauss integer $a + bi$. Since $i = 3$ in $\bar{R}$, the residue of $a + bi$ is the same as that of the integer $a + 3b$. This shows that φ is surjective. Next, let n be an element of $\ker \varphi$. Using the fact that $\bar{R} = R/I$, we see that n must be in the ideal I, that is, that n is divisible by $1 + 3i$ in the ring of Gauss integers. So we may write $n = (a + bi)(1 + 3i) = (a - 3b) + (3a + b)i$ for some integers a, b. Since n is an integer, $3a + b = 0$, or $b = -3a$. Thus $n = a(1 - 3i)(1 + 3i) = 10a$, and this shows that $\ker \varphi \subset 10\mathbb{Z}$. On the other hand, we already saw that $10 \in \ker \varphi$. So $\ker \varphi = 10\mathbb{Z}$, as required. □

Another possible way to identify the quotient R/I is to find a ring R' and a homomorphism $\varphi\colon R \longrightarrow R'$ whose kernel is I. To illustrate this, let $\bar{R} = \mathbb{C}[x, y]/(xy)$. Here the fact that xy is a product can be used to find such a map φ.

(4.10) **Proposition.** The ring $\mathbb{C}[x, y]/(xy)$ is isomorphic to the subring of the product ring $\mathbb{C}[x] \times \mathbb{C}[y]$ consisting of the pairs $(p(x), q(y))$ such that $p(0) = q(0)$.

Proof. We can identify the ring $\mathbb{C}[x, y]/(y)$ easily, because the principal ideal (y) is the kernel of the substitution homomorphism $\varphi\colon \mathbb{C}[x, y] \longrightarrow \mathbb{C}[x]$ sending $y \rightsquigarrow 0$. By the First Isomorphism Theorem, $\mathbb{C}[x, y]/(y) \approx \mathbb{C}[x]$. Similarly, $\mathbb{C}[x, y]/(x) \approx \mathbb{C}[y]$. So it is natural to look at the homomorphism to the product ring $\varphi\colon \mathbb{C}[x, y] \longrightarrow \mathbb{C}[x] \times \mathbb{C}[y]$, which is defined by $f(x, y) \rightsquigarrow (f(x, 0), f(0, y))$. The kernel of φ is the intersection of the kernels: $\ker \varphi = (y) \cap (x)$. To be in this intersection, a polynomial must be divisible by both y and x. This just means that it is divisible by xy. So $\ker \varphi = (xy)$. By the First Isomorphism Theorem, $\bar{R} = \mathbb{C}[x, y]/(xy)$ is isomorphic to the image of the homomorphism φ. That image is the subring described in the statement of the proposition. □

Aside from the First Isomorphism Theorem, there are no general methods for identifying a quotient ring, because it will usually not be a familiar ring. The ring $\mathbb{C}[x,y]/(y^2 - x^3 + x)$, for example, is fundamentally different from any ring we have seen up to now.

5. ADJUNCTION OF ELEMENTS

In this section we discuss a procedure which is closely related to the introduction of relations, that of adding new elements to a ring. Our model for this procedure is the construction of the complex field, starting from the real numbers. One obtains $\mathbb{C}$ from $\mathbb{R}$ by adjoining i, and the construction is completely formal. That is, the imaginary number i has no properties other than those forced by the relation

$$i^2 = -1. \tag{5.1}$$

We are now ready to understand the general principle behind this construction. Let us start with an arbitrary ring R, and consider the problem of building a bigger ring containing the elements of R and also containing a new element, which we denote by α. We will probably want α to satisfy some relations such as (5.1), for instance. A ring R' containing R as a subring is called a *ring extension* of R. So we are looking for a suitable extension.

Sometimes the element α may be available in a ring extension R' that we already know. In that case, our solution is the subring of R' generated by R and α. This subring is denoted by $R[\alpha]$. We have already described this ring in Section 1, in the case $R = \mathbb{Z}$ and $R' = \mathbb{C}$. The description is no different in general: $R[\alpha]$ consists of the elements of R' which have polynomial expressions

$$r_n\alpha^n + \cdots + r_1\alpha + r_0$$

with coefficients r_i in R. But as happens when we first construct $\mathbb{C}$ from $\mathbb{R}$, we may not yet know an extension containing α. Then we must construct it abstractly. Actually, we already did this when we constructed the polynomial ring $R[x]$.

Note that the polynomial ring $R[x]$ is an extension of R and that it is generated by R and x. So the notation $R[x]$ agrees with the one introduced above. Moreover, the Substitution Principle (3.4) tells us that the polynomial ring is the *universal solution* to our problem of adjoining a new element, in the following sense: If α is an element of any ring extension R' of R, then there is a unique map $R[x] \longrightarrow R'$ which is the identity on R and which carries x to α. The image of this map will be the subring $R[\alpha]$.

Let us now consider the question of the relations which we want our new element to satisfy. The variable x in the polynomial ring $R[x]$ satisfies no relations except those, such as $0x = 0$, implied by the ring axioms. This is another way to state the universal property of the polynomial ring. We may want some nontrivial relations. But now that we have the ring $R[x]$ in hand we can add relations to it as we like, using the procedure given in Section 4. We introduce relations by using the quotient construction *on the polynomial ring* $R[x]$. The fact that R gets replaced by

$R[x]$ in the construction complicates things notationally, but aside from this notational complication, nothing is different.

For example, we can construct the complex numbers formally by introducing the relation $x^2 + 1 = 0$ into the ring of real polynomials $\mathbb{R}[x] = P$. To do so, we form the quotient ring $\bar{P} = P/(x^2 + 1)$. The residue of x becomes our element i. Note that the relation $\overline{x^2+1} = \bar{x}^2 + \bar{1} = 0$ holds in $\bar{P}$, because the map $\pi: P \longrightarrow \bar{P}$ is a homomorphism and because $x^2 + 1 \in \ker \pi$. And since $\bar{1}$ is the unit element in $\bar{P}$, our standard notation for the unit element drops the bar. So $\bar{P}$ is obtained from $\mathbb{R}$ by adjoining an element $\bar{x}$ satisfying $\bar{x}^2 + 1 = 0$. In other words, $P \approx \mathbb{C}$ as required.

The fact that the quotient $\mathbb{R}[x]/(x^2 + 1)$ is isomorphic to $\mathbb{C}$ also follows from the First Isomorphism Theorem (4.2b): Substitution (3.4) of i for x defines a surjective homomorphism φ: $\mathbb{R}[x] \longrightarrow \mathbb{C}$, whose kernel is the set of real polynomials with i as a root. Now if i is a root of a real polynomial $p(x)$, then $-i$ is also a root. Therefore $x - i$ and $x + i$ both divide $p(x)$. The kernel is the set of real polynomials divisible by $(x - i)(x + i) = x^2 + 1$, which is the principal ideal $(x^2 + 1)$. By the First Isomorphism Theorem, $\mathbb{C}$ is isomorphic to $\mathbb{R}[x]/(x^2 + 1)$.

Another simple example of adjunction of an element was used in Section 6 of Chapter 8, where a formal infinitesimal element satisfying

$$\epsilon^2 = 0 \tag{5.2}$$

was introduced to compute tangent vectors. An element of a ring R is called *infinitesimal* or *nilpotent* if some power is zero, and our procedure allows us to adjoin infinitesimals to a ring. Thus the result of adjoining an element ϵ satisfying (5.2) to a ring R is the quotient ring $R' = R[x]/(x^2)$. The residue of x is the infinitesimal element ϵ. In this ring, the relation $\epsilon^2 = 0$ reduces all polynomial expressions in ϵ to degree < 2, so the elements of R' have the form $a + b\epsilon$, with $a, b \in R$. But the multiplication rule [Chapter 8 (6.5)] is different from the rule for multiplying complex numbers.

In general, if we want to adjoin an element α satisfying one or more polynomial relations of the form

$$f(\alpha) = c_n\alpha^n + \cdots + c_1\alpha + c_0 = 0 \tag{5.3}$$

to a ring R, the solution is $R' = R[x]/I$, where I is the ideal in $R[x]$ generated by the polynomials $f(x)$. If α denotes the residue $\bar{x}$ of x in R', then

$$0 = \overline{f(x)} = \bar{c}_n\bar{x}^n + \cdots + \bar{c}_0 = \bar{c}_n\alpha^n + \cdots + \bar{c}_0. \tag{5.4}$$

Here $\bar{c}_i$ is the image in R' of the constant polynomial c_i. So α satisfies the relation in R' which corresponds to the relation (5.3) in R. The ring obtained in this way will often be denoted by

$$R[\alpha] = \textit{ring obtained by adjoining } \alpha \textit{ to } R. \tag{5.5}$$

Several elements $\alpha_1, \ldots, \alpha_m$ can be adjoined by repeating this procedure, or by introducing the appropriate relations in the polynomial ring $R[x_1, \ldots, x_m]$ in m variables all at once.

One of the most important cases is that the new element α is required to satisfy a single *monic* equation of degree $n > 0$. Suppose we want the relation $f(x) = 0$, where f is the monic polynomial

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0. \tag{5.6}$$

It isn't difficult to describe the ring $R[\alpha]$ precisely in this special case.

(5.7) **Proposition.** Let R be a ring, and let $f(x)$ be a monic polynomial of positive degree n, with coefficients in R. Let $R[\alpha]$ denote the ring obtained by adjoining an element satisfying the relation $f(\alpha) = 0$. The elements of $R[\alpha]$ are in bijective correspondence with vectors $(r_0,\dots,r_{n-1}) \in R^n$. Such a vector corresponds to the linear combination

$$r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{n-1}\alpha^{n-1}, \quad \text{with } r_i \in R.$$

This proposition says that the powers $1,\alpha,\alpha^2,\dots,\alpha^{n-1}$ form a *basis* for $R[\alpha]$ over R. To multiply two such linear combinations in $R[\alpha]$, we use polynomial multiplication and then divide the product by f. The remainder is the linear combination of $1,\alpha,\dots,\alpha^{n-1}$ which represents the product. So although addition in R' depends only on the degree, multiplication depends strongly on the particular polynomial f.

For example, let R' be the result of adjoining an element α to $\mathbb{Z}$ satisfying the relation $\alpha^3+3\alpha+1 = 0$. So $R' = \mathbb{Z}[x]/(x^3 + 3x + 1)$. The elements of R' are linear combinations $r_0+r_1\alpha+r_2\alpha^2$, where r_i are integers. Addition of two linear combinations is polynomial addition: $(2+\alpha-\alpha^2) + (1+\alpha) = 3+2\alpha-\alpha^2$, for instance. To multiply, we compute the product using polynomial multiplication: $(2+\alpha-\alpha^2)(1+\alpha) = 2+3\alpha-\alpha^3$. Then we divide by $1+3\alpha+\alpha^3$: $2+3\alpha-\alpha^3 = (1+3\alpha+\alpha^3)(-1) + (3+6\alpha)$. Since $1+3\alpha+\alpha^3 = 0$ in R', the remainder $3 + 6\alpha$ is the linear combination which represents the product.

Or let R' be obtained by adjoining an element α to $\mathbb{F}_5$ with the relation $\alpha^2 - 3 = 0$, that is, $R' = \mathbb{F}_5[x]/(x^2 - 3)$. Here α represents a formal square root of 3. The elements of R' are the 25 linear expressions $a + b\alpha$ in α with coefficients $a, b \in \mathbb{F}_5$. This ring is a field. To prove this, we verify that every nonzero element $a + b\alpha$ of R' is invertible. Note that $(a + b\alpha)(a - b\alpha) = a^2 - 3b^2 \in \mathbb{F}_5$. Moreover, the equation $x^2 = 3$ has no solution in $\mathbb{F}_5$, and this implies that $a^2 - 3b^2 \neq 0$. Therefore $a^2 - 3b^2$ is invertible in $\mathbb{F}_5$ and in R'. This shows that $a + b\alpha$ is invertible too. Its inverse is $(a^2 - 3b^2)^{-1}(a - b\alpha)$.

On the other hand, the same procedure applied to $\mathbb{F}_{11}$ does not yield a field. The reason is that $x^2 - 3 = (x + 5)(x - 5)$ in $\mathbb{F}_{11}[x]$. So if α denotes the residue of x in $R' = \mathbb{F}_{11}[x]/(x^2 - 3)$, then $(\alpha + 5)(\alpha - 5) = 0$. This can be explained intuitively by noting that we constructed R' by adjoining a square root of 3 to $\mathbb{F}_{11}$ when that field already contains the two square roots ± 5. At first glance, one might expect to get $\mathbb{F}_{11}$ back by this procedure. But we haven't told α whether to be equal to 5 or to -5. We've only told it that its square is 3. The relation $(\alpha + 5)(\alpha - 5) = 0$ reflects this ambiguity. □

Proof of Proposition (5.7). Since $R[\alpha]$ is a quotient of the polynomial ring $R[x]$, every element in $R[\alpha]$ is the residue of a polynomial. This means that it can be written in the form $g(\alpha)$ for some polynomial $g(x) \in R[x]$. The relation $f(\alpha) = 0$ can be used to replace any polynomial $g(\alpha)$ of degree $\geq n$ by one of lower degree: We perform division with remainder by $f(x)$ on the polynomial $g(x)$, obtaining an expression of the form $g(x) = f(x)q(x) + r(x)$ (3.19). Since $f(\alpha) = 0$, $g(\alpha) = r(\alpha)$. Thus every element β of $R[\alpha]$ can be written as a polynomial in α, of degree $< n$.

We now show that the principal ideal generated by $f(x)$ contains no element of degree $< n$, and therefore that $g(\alpha) \neq 0$ for every nonzero polynomial $g(x)$ of degree $< n$. This will imply that the expression of degree $< n$ for an element β is unique. The principal ideal generated by $f(x)$ is the set of all multiples hf of f. Suppose $h(x) = b_m x^m + \cdots + b_0$, with $b_m \neq 0$. Then the highest-degree term of $h(x)f(x)$ is $b_m x^{m+n}$, and hence hf has degree $m + n \geq n$. This completes the proof of the proposition. □

It is harder to analyze the structure of the ring obtained by adjoining an element which satisfies a nonmonic polynomial relation. One of the simplest and most important cases is obtained by adjoining a multiplicative inverse of an element to a ring. If an element $a \in R$ has an inverse α, then α satisfies the relation

$$a\alpha - 1 = 0. \tag{5.8}$$

So we can adjoin an inverse by forming the quotient ring $R' = R[x]/(ax - 1)$. The residue of x becomes the inverse α of a. This ring has no basis of the type described in Proposition (5.7), but we can compute in it fairly easily because every element of R' has the form $\alpha^k r$, where $r \in R$ and k is a nonnegative integer: Say that $\beta = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}$, with $r_i \in R$. Then since $a\alpha = 1$, we can also write $\beta = \alpha^{n-1}(r_0 a^{n-1} + r_1 a^{n-2} + \cdots + r_{n-1})$.

One interesting example is that R is a polynomial ring itself, say $R = F[t]$, and that we adjoin an inverse to the variable t. Then $R' = F[t, x]/(xt - 1)$. This ring identifies naturally with the ring $F[t, t^{-1}]$ of *Laurent polynomials* in t. A Laurent polynomial is a polynomial in t and t^{-1} of the form

$$f(t) = \sum_{-n}^{n} a_i t^i = a_{-n}t^{-n} + \cdots + a_{-1}t^{-1} + a_0 + a_1 t + \cdots + a_n t^n. \tag{5.9}$$

We leave the construction of this isomorphism as an exercise.

We must now consider a point which we have suppressed in our discussion of adjunction of elements: When we adjoin an element α to a ring R and impose some relations, will our original R be a subring of the ring $R[\alpha]$ which we obtain? We know that R is contained in the polynomial ring $R[x]$, as the subring of constant polynomials. So the restriction of the canonical map $\pi\colon R[x] \longrightarrow R[x]/I = R[\alpha]$ to constant polynomials gives us a homomorphism $\psi\colon R \longrightarrow R[\alpha]$, which is the map $r \rightsquigarrow \bar{r}$ considered above. The kernel of the map $\psi\colon R \longrightarrow R[\alpha] = R[x]/I$ is easy

to determine in principle. It is the set of constant polynomials in the ideal I:

$$\ker \psi = R \cap I. \tag{5.10}$$

It follows from Proposition (5.7) that ψ is injective, and hence that $\ker \psi = 0$, when α is required to satisfy one monic equation. But ψ is not always injective.

For example, we had better not adjoin an inverse of 0 to a ring. From the equation $0\alpha = 1$ we can conclude that $0 = 1$. The zero element is invertible only in the zero ring, so if we insist on adjoining an inverse of 0, we must end up with the zero ring.

More generally, let a, b be two elements of a ring R whose product ab is zero. Then a is not invertible unless $b = 0$. For, if a^{-1} exists in R, then $b = a^{-1}ab = a^{-1}0 = 0$. It follows that if a product ab of two elements of a ring R is zero, then the procedure of adjoining an inverse of a to R must kill b. This can also be seen directly: The ideal of $R[x]$ generated by $ax - 1$ contains $-b(ax - 1) = b$, which shows that the residue of b in the ring $R[x]/(ax - 1)$ is zero.

For example, $\bar{2}\cdot\bar{3} = 0$ in the ring $\mathbb{Z}/(6)$. If we adjoin $\bar{3}^{-1}$ to this ring, we must kill $\bar{2}$. Killing $\bar{2}$ collapses $\mathbb{Z}/(6)$ to $\mathbb{Z}/(2) = \mathbb{F}_2$. Since $\bar{3} = \bar{1}$ is invertible in $\mathbb{F}_2$, no further action is necessary, and $R' = (\mathbb{Z}/(6))[x]/(\bar{3}x - \bar{1}) \approx \mathbb{F}_2$. Again, this can be checked directly. To do so, we note that the ring R' is isomorphic to $\mathbb{Z}[x]/(6, 3x - 1)$, and we analyze the two relations $6 = 0$ and $3x - 1 = 0$. They imply $6x = 0$ and $6x - 2 = 0$; hence $2 = 0$. Then $2x = 0$ too, and combined with $3x - 1 = 0$, this implies $x - 1 = 0$. Hence the ideal $(6, 3x - 1)$ of $\mathbb{Z}[x]$ contains the elements $(2, x - 1)$. On the other hand, 6 and $3x - 1$ are in the ideal $(2, x - 1)$. So the two ideals are equal, and R' is isomorphic to $\mathbb{Z}[x]/(2, x - 1) \approx \mathbb{F}_2$.

An element a of a ring is called a *zero divisor* if there is a nonzero element b such that $ab = 0$. For example, the residue of 3 is a zero divisor in the ring $\mathbb{Z}/(6)$. The term "zero divisor" is traditional, but it has been poorly chosen, because actually every $a \in R$ divides zero: $0 = a0$.

6. INTEGRAL DOMAINS AND FRACTION FIELDS

The difference between rings and fields is that nonzero elements of a ring R do not necessarily have inverses. In this section we discuss the problem of embedding a given ring R as a subring into a field. We saw in the last section that we can not adjoin the inverse of a zero divisor without killing some elements. So a ring which contains zero divisors can not be embedded into a field.

(6.1) **Definition.** An *integral domain* R is a nonzero ring having no zero divisors. In other words, it has the property that if $ab = 0$, then $a = 0$ or $b = 0$, and also $1 \neq 0$ in R.

For example, any subring of a field is an integral domain.

An integral domain satisfies the *cancellation law:*

(6.2) *If* $ab = ac$ *and* $a \neq 0$, *then* $b = c$.

For, from $ab = ac$ we can deduce $a(b - c) = 0$. Then since $a \neq 0$, it follows that $b - c = 0$. □

(6.3) **Proposition.** Let R be an integral domain. Then the polynomial ring $R[x]$ is an integral domain.

(6.4) **Proposition.** An integral domain with finitely many elements is a field.

We leave the proofs of these propositions as exercises. □

(6.5) **Theorem.** Let R be an integral domain. There exists an embedding of R into a field, meaning an injective homomorphism $R \longrightarrow F$, where F is a field.

We could construct the field by adjoining inverses of all nonzero elements of R, using the procedure described in the last section. But in this case it is somewhat simpler to construct F with fractions. Our model is the construction of the rational numbers as fractions of integers, and once the idea of using fractions is put forward, the construction follows the construction of the rational numbers very closely.

Let R be an integral domain. A *fraction* will be a symbol a/b where $a, b \in R$ and $b \neq 0$. Two fractions $a_1/b_1, a_2/b_2$ are called *equivalent*, $a_1/b_1 \approx a_2/b_2$, if

$$a_1b_2 = a_2b_1.$$

Let us check transitivity of this relation—the reflexive and symmetric properties are clear (see Chapter 2, Section 5). Suppose that $a_1/b_1 \approx a_2/b_2$ and also that $a_2/b_2 \approx a_3/b_3$. Then $a_1b_2 = a_2b_1$ and $a_2b_3 = a_3b_2$. Multiply by b_3 and b_1 to obtain

$$a_1b_2b_3 = a_2b_1b_3 = a_3b_2b_1.$$

Cancel b_2 to get $a_3b_1 = a_1b_3$. Thus $a_1/b_1 \approx a_3/b_3$.

The *field of fractions* F of R is the set of equivalence classes of fractions. As we do with rational numbers, we will speak of fractions $a_1/b_1, a_2/b_2$ as equal elements of F if they are equivalent fractions: $a_1/b_1 = a_2/b_2$ in F means $a_1b_2 = a_2b_1$. Addition and multiplication of fractions is defined as in arithmetic:

$$(a/b)(c/d) = ac/bd, \quad a/b + c/d = \frac{ad + bc}{bd}.$$

Here it must be verified that these rules lead to equivalent answers if a/b and c/d are replaced by equivalent fractions. Then the axioms for a field must be verified. All of these verifications are straightforward exercises. □

Notice that R is contained in F, provided that we identify $a \in R$ with the fraction $a/1$ because $a/1 \approx b/1$ only if $a = b$. The map $a \rightsquigarrow a/1$ is the injective homomorphism referred to in the theorem.

As an example, consider the polynomial ring $K[x]$, where K is any field. This is an integral domain, and its fraction field is called the field of *rational functions* in x, with coefficients in K. This field is usually denoted by

$$K(x) = \left\{\begin{array}{l}\textit{equivalence classes of fractions } f/g, \textit{ where } f, g \\ \textit{are polynomials and } g \textit{ is not the zero polynomial}\end{array}\right\}. \tag{6.6}$$

If $K = \mathbb{R}$, then evaluation of a rational function $f(x)/g(x)$ defines an actual function on the real line, wherever $g(x) \neq 0$. But as with polynomials, we should distinguish between the formally defined rational functions, which are fractions of polynomials, and the actual functions which they define by evaluation.

The fraction field is a universal solution to the problem of embedding an integral domain into a field. This is shown by the following proposition:

(6.7) **Proposition.** Let R be an integral domain, with field of fractions F, and let $\varphi\colon R \longrightarrow K$ be any injective homomorphism of R to a field K. Then the rule

$$\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$$

defines the unique extension of φ to a homomorphism $\Phi\colon F \longrightarrow K$.

Proof. We must check that this extension is well defined. First, since the denominator of a fraction is not allowed to be zero and since φ is injective, $\varphi(b) \neq 0$ for any fraction a/b. Therefore $\varphi(b)$ is invertible in K, and $\varphi(a)\varphi(b)^{-1}$ is an element of K. Next, we check that equivalent fractions have the same image: If $a_2/b_2 \approx a_1/b_1$, then $a_2b_1 = a_1b_2$; hence $\varphi(a_2)\varphi(b_1) = \varphi(a_1)\varphi(b_2)$, and $\Phi(a_2/b_2) = \varphi(a_2)\varphi(b_2)^{-1} = \varphi(a_1)\varphi(b_1)^{-1} = \Phi(a_1/b_1)$, as required. The facts that Φ is a homomorphism and that it is the unique extension of φ follow easily. □

7. MAXIMAL IDEALS

In this section we investigate surjective homomorphisms

$$\varphi\colon R \longrightarrow F \tag{7.1}$$

from a ring R to a field F. Given such a homomorphism, the First Isomorphism Theorem tells us that F is isomorphic to $R/\ker \varphi$. Therefore we can recover F and φ, up to isomorphism, from the kernel. To classify such homomorphisms, we must determine the ideals M such that R/M is a field.

By the Correspondence Theorem (4.3), the ideals of $\bar{R} = R/M$ correspond to ideals of R which contain M. Also, fields are characterized by the property of having exactly two ideals (3.16). So if $\bar{R}$ is a field, there are exactly two ideals containing M, namely M and R. Such an ideal is called maximal.

(7.2) **Definition.** An ideal M is *maximal* if $M \neq R$ but M is not contained in any ideals other than M and R.

(7.3) **Corollary.**

(a) An ideal M of a ring R is maximal if and only if $\bar{R} = R/M$ is a field.

(b) The zero ideal of R is maximal if and only if R is a field. □

The next proposition follows from the fact that all ideals of $\mathbb{Z}$ are principal:

(7.4) **Proposition.** The maximal ideals of the ring $\mathbb{Z}$ of integers are the principal ideals generated by prime integers. □

The maximal ideals of the ring $\mathbb{C}[x]$ of complex polynomials in one variable can also be described very simply:

(7.5) **Proposition.** The maximal ideals of the polynomial ring $\mathbb{C}[x]$ are the principal ideals generated by the linear polynomials $x - a$. The ideal M_a generated by $x - a$ is the kernel of the substitution homomorphism s_a: $\mathbb{C}[x] \longrightarrow \mathbb{C}$ which sends $f(x) \rightsquigarrow f(a)$. Thus there is a bijective correspondence between maximal ideals M_a and complex numbers a.

Proof. We first show that every maximal ideal is generated by a linear polynomial $x - a$. Let M be maximal. By Proposition (3.21), M is a principal ideal, generated by the monic polynomial $f \in M$ of least degree. Since every complex polynomial of positive degree has a root, f is divisible by some linear polynomial $x - a$. Then f is in the principal ideal $(x - a)$, and hence $M \subset (x - a)$. Since M is maximal, $M = (x - a)$.

Next, we show that the kernel of the substitution homomorphism s_a is generated by $x - a$: To say that a polynomial g is in the kernel of s_a means that a is a root of g, or that $x - a$ divides g. Thus $x - a$ generates $\ker s_a$. Since the image of s_a is a field, this also shows that $(x - a)$ is a maximal ideal. □

The extension of Proposition (7.5) to several variables is one of the most important theorems about polynomial rings.

(7.6) **Theorem.** *Hilbert's Nullstellensatz:* The maximal ideals of the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ are in bijective correspondence with points of complex n-dimensional space. A point $a = (a_1, \ldots, a_n)$ in $\mathbb{C}^n$ corresponds to the kernel of the substitution map s_a: $\mathbb{C}[x_1, \ldots, x_n] \longrightarrow \mathbb{C}$, which sends $f(x) \rightsquigarrow f(a)$. The kernel M_a of this map is the ideal generated by the linear polynomials

$$x_1 - a_1, \ldots, x_n - a_n.$$

Proof. Let $a \in \mathbb{C}^n$, and let M_a be the kernel of the substitution map s_a. Since s_a is surjective and $\mathbb{C}$ is a field, M_a is a maximal ideal. Next, let us verify that M_a is generated by the linear polynomials, as asserted. To do so, we expand $f(x)$ in powers of $x_1 - a_1, \ldots, x_n - a_n$, writing

$$f(x) = f(a) + \sum_i c_i(x_i - a_i) + \sum_{i,j} c_{ij}(x_i - a_i)(x_j - a_j) + \cdots.$$

You may recognize this as Taylor's expansion: $c_i = \partial f/\partial x_i$, and so on. The existence of such an expansion can be derived algebraically by substituting $x = a + u$ into f, expanding in powers of the variables u, and then substituting $u = x - a$ back into the result. Note that every term on the right side except $f(a)$ is divisible by at least one of the polynomials $(x_i - a_i)$. So if f is in the kernel of s_a, that is, if $f(a) = 0$, then $f(x)$ is in the ideal which these elements generate. This shows that the polynomials $x_i - a_i$ generate M_a.

It is harder to prove that every maximal ideal is of the form M_a for some point $a \in \mathbb{C}^n$. To do so, let M be any maximal ideal, and let K denote the field $\mathbb{C}[x_1,\dots,x_n]/M$. We consider the restriction of the canonical map (4.1) $\pi\colon \mathbb{C}[x_1,\dots,x_n] \longrightarrow K$ to the subring $\mathbb{C}[x_1]$ of polynomials in one variable:

$$\pi_1\colon \mathbb{C}[x_1] \longrightarrow K.$$

(7.7) **Lemma.** The kernel of π_1 is either zero or else it is a maximal ideal.

Proof. Assume that the kernel is not zero, and let f be a nonzero element in $\ker \pi_1$. Since K is not the zero ring, $\ker \pi_1$ is not the whole ring. So f is not constant, which implies that it is divisible by a linear polynomial, say $f = (x_1 - a_1)g$. Then $\pi_1(x_1 - a_1)\pi_1(g) = \pi_1(f) = 0$ in K. Since K is a field, $\pi_1(x_1 - a_1) = 0$ or $\pi_1(g) = 0$. So one of the two elements $x_1 - a_1$ or g is in $\ker \pi_1$. By induction on the degree of f, $\ker \pi_1$ contains a linear polynomial. Hence it is a maximal ideal (7.5). □

We are going to show that $\ker \pi_1$ is not the zero ideal. It will follow that M contains a linear polynomial of the form $x_1 - a_1$. Since the index 1 can be replaced by any other index, M contains polynomials of the form $x_\nu - a_\nu$ for every $\nu = 1,\dots,n$. This will show that M is contained in, and hence equal to, the kernel of a substitution map $f(x) \rightsquigarrow f(a)$, as claimed.

So, suppose $\ker \pi_1 = (0)$. Then π_1 maps $\mathbb{C}[x_1]$ isomorphically to its image, which is a subring of K. According to Proposition (6.7), this map can be extended to the field of fractions of $\mathbb{C}[x]$. Hence K contains a field isomorphic to the field of rational functions $\mathbb{C}(x)$ [see (3.17)].

Now the monomials $x^i = x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ form a basis of $\mathbb{C}[x_1,\dots,x_n]$ as a vector space over $\mathbb{C}$ (see Section 2). Thus $\mathbb{C}[x_1,\dots,x_n]$ has a *countable* basis (Appendix, Section 1). Since K is a quotient of $\mathbb{C}[x_1,\dots,x_n]$, there is a countable family which spans K as vector space over $\mathbb{C}$, namely the residues of the monomials span this field. We will show that there are *uncountably many linearly independent elements* in $\mathbb{C}(x)$. It will follow [Lemma (7.9)] that $\mathbb{C}(x)$ can not be isomorphic to a subspace of K. This contradiction will show $\ker \pi_1 \neq (0)$.

The fact we need is that the elements of the complex field $\mathbb{C}$ do not form a countable set [Appendix (1.7)]. Using this fact, the following two lemmas will finish the proof:

(7.8) **Lemma.** The uncountably many rational functions $(x - \alpha)^{-1}$, $\alpha \in \mathbb{C}$, are linearly independent.

Proof. A rational function f/g defines an actual function by evaluation, at all points of the complex plane at which $g \neq 0$. The rational function $(x - \alpha)^{-1}$ has a *pole* at α, which means that it takes on arbitrarily large values near α. It is bounded near any other point. Consider a linear combination

$$\sum_{i=1}^{n} \frac{c_i}{x - \alpha_i},$$

where $\alpha_1, \ldots, \alpha_n$ are distinct complex numbers and where some coefficient, say c_1, is not zero. The first term of this sum is unbounded near α_1, but the others are bounded there. It follows that the linear combination does not define the zero function; hence it is not zero. □

(7.9) **Lemma.** Let V be a vector space which is spanned by a countable family $\{v_1, v_2, \ldots\}$ of vectors. Then every set L of linearly independent vectors in V is finite or countably infinite.

Proof. Let L be a linearly independent subset of V, let V_n be the span of the first n vectors $v_1, \ldots, v_n$ and let $L_n = L \cap V_n$. Then L_n is a linearly independent set in a finite-dimensional space V_n, hence it is a finite set [Chapter 3 (3.16)]. Moreover, L is the union of all the L_n's. The union of countably many finite sets is finite or countably infinite. □

8. ALGEBRAIC GEOMETRY

To me algebraic geometry is algebra with a kick.

Solomon Lefschetz

Let V be a subset of complex n-space $\mathbb{C}^n$. If V can be defined as the set of common zeros of a finite number of polynomials in n variables, then it is called an *algebraic variety,* or just a *variety* for short. (I don't know the origin of this unattractive term.) For instance, a complex line in $\mathbb{C}^2$ is, by definition, the set of solutions of a linear equation $ax + by + c = 0$. This is a variety. So is a point. The point (a, b) is the set of common zeros of the two polynomials $x - a$ and $y - b$. We have seen a number of other interesting varieties already. The group $SL_2(\mathbb{C})$, for example, being the locus of solutions of the polynomial equation $x_{11}x_{22} - x_{12}x_{21} - 1 = 0$, is a variety in $\mathbb{C}^4$.

Hilbert's Nullstellensatz provides us with an important link between algebra and geometry. It tells us that the maximal ideals in the polynomial ring $\mathbb{C}[x] = \mathbb{C}[x_1, \ldots, x_n]$ correspond to points in $\mathbb{C}^n$. This correspondence can also be used to relate algebraic varieties to quotient rings of the polynomial ring.

(8.1) **Theorem.** Let $f_1, \ldots, f_r$ be polynomials in $\mathbb{C}[x_1, \ldots, x_n]$, and let V be the variety defined by the system of equations $f_1(x) = 0, \ldots, f_r(x) = 0$. Let I be the ideal

$(f_1,\ldots,f_r)$ generated by the given polynomials. The maximal ideals of the quotient ring $R = \mathbb{C}[x]/I$ are in bijective correspondence with points of V.

Proof. The maximal ideals of R correspond to those maximal ideals of $\mathbb{C}[x]$ which contain I [Correspondence Theorem (4.3)]. And an ideal will contain I if and only if it contains the generators $f_1,\ldots,f_r$ of I. On the other hand, the maximal ideal M_a which corresponds to a point $a \in C^n$ is the kernel of the substitution map $f(x) \rightsquigarrow f(a)$. So $f_i \in M_a$ if and only if $f_i(a) = 0$, which means that $a \in V$. □

This theorem shows that the algebraic properties of the ring R are closely connected with the geometry of V. In principle, all properties of the system of polynomial equations

$$f_1(x) = \ldots = f_r(x) = 0 \tag{8.2}$$

are reflected in the structure of the ring $R = \mathbb{C}[x]/(f_1,\ldots,f_r)$. The theory of this relationship is the field of mathematics called algebraic geometry. We won't take the time to go very far into it here. The important thing for us to learn is that geometric properties of the variety provide information about the ring, and conversely.

The simplest question about a set is whether or not it is empty. So we might ask whether it is possible for a ring to have no maximal ideals at all. It turns out that this happens only for the zero ring:

(8.3) **Theorem.** Let R be a ring. Every ideal I of R which is not the unit ideal is contained in a maximal ideal.

(8.4) **Corollary.** The only ring R having no maximal ideals is the zero ring. □

Theorem (8.3) can be proved using the *Axiom of Choice*, or *Zorn's Lemma*. However, for quotients of polynomial rings it is a consequence of the Hilbert Basis Theorem, which we will prove later [Chapter 12 (5.18)]. Rather than enter into a discussion of the Axiom of Choice, we will defer further discussion of the proof to Chapter 12.

If we put Theorems (8.1) and (8.3) together, we obtain another important corollary:

(8.5) **Corollary.** Let $f_1,\ldots,f_r$ be polynomials in $\mathbb{C}[x_1,\ldots,x_n]$. If the system of equations $f_1 = \ldots = f_r = 0$ has no solution in $\mathbb{C}^n$, then 1 is a linear combination

$$1 = \sum g_i f_i$$

of the f_i, with polynomial coefficients.

For, if the system has no solution, then Theorem (8.1) tells us that there is no maximal ideal containing the ideal $I = (f_1,\ldots,f_r)$. By Theorem (8.3), I is the unit ideal. □

Most choices of three polynomials f_1, f_2, f_3 in two variables x, y have no common solutions. If follows that we can usually express 1 as a linear combination $1 = p_1f_1 + p_2f_2 + p_3f_3$, where p_i are polynomials. This is not obvious. For instance, the ideal generated by

$$f_1 = x^2 + y^2 - 1, \quad f_2 = x^2 - y + 1, \quad f_3 = xy - 1 \tag{8.6}$$

is the unit ideal. This can be proved by showing that the set of equations $f_1 = f_2 = f_3 = 0$ has no solution in $\mathbb{C}^2$. If we didn't have the Nullstellensatz, it might take us some time to discover that we could write 1 as a linear combination, with polynomial coefficients, of these three polynomials.

The Nullstellensatz has been reformulated in many ways, and actually the one we gave in the last section is not its original form. Here is the original:

(8.7) **Theorem.** *Classical form of the Nullstellensatz:* Let $f_1,\dots, f_r$ and g be polynomials in $\mathbb{C}[x_1,\dots, x_n]$. Let V be the variety of zeros of $f_1,\dots, f_r$, and let I be the ideal generated by these polynomials. If $g = 0$ identically on V, then some power of g is in the ideal I.

Proof. To prove this we study the ring obtained by inverting the polynomial g, by means of the equation $gy = 1$. Assume that g vanishes identically on V. Consider the $r + 1$ polynomials $f_1(x),\dots, f_r(x), g(x)y - 1$ in the variables $x_1,\dots, x_n, y$. The last is the only polynomial which involves the variable y. Notice that these polynomials have no common zero in C^{n+1}. For, if $f_1,\dots, f_r$ vanish at a point $(a_1,\dots, a_n, b) \in C^{n+1}$, then by hypothesis g vanishes too, and hence $gy - 1$ takes the value -1. Corollary (8.5) applies and tells us that the polynomials $f_1,\dots, f_r, gy - 1$ generate the unit ideal in $\mathbb{C}[x, y]$. So we may write

$$1 = \sum_i p_i(x, y)f_i(x, y) + q(x, y)(g(x)y - 1).$$

We substitute $y = 1/g$ into this equation, obtaining

$$1 = \sum_i p_i(x, g^{-1})f_i(x).$$

We now clear denominators in $p_i(x, g^{-1})$, multiplying both sides of the equation by a sufficiently large power of g. This yields the required polynomial expression

$$g(x)^N = \sum_i h_i(x)f_i(x),$$

where $h_i(x) = g(x)^N p_i(x, g^{-1})$. □

It is not easy to get a good feeling for a general algebraic variety in $\mathbb{C}^n$, but the general shape of a variety in $\mathbb{C}^2$ can be described fairly simply.

(8.8) **Proposition.** Two nonzero polynomials $f(x, y), g(x, y)$ in two variables have only finitely many common zeros, unless they have a nonconstant polynomial factor in common.

If the degrees of f and g are m and n respectively, the number of common zeros is bounded by mn. This is known as the *Bezout* bound. For instance, two conics intersect in at most four points. It is somewhat harder to prove the Bezout bound than just the finiteness, and we won't give a proof.

Proof of Proposition (8.8). We assume that f and g have no common nonconstant factor. Let F denote the field of rational functions in x, the field of fractions of the ring $\mathbb{C}[x]$. It is useful to regard f and g as elements of the polynomial ring $F[y]$ in one variable, because we can use the fact that every ideal of $F[y]$ is principal. Let I denote the ideal generated by f, g in $F[y]$. This is a principal ideal, generated by the greatest common divisor h of f and g in $F[y]$ (3.22). If f and g have no common nonconstant factor in $F[y]$, then I is the unit ideal.

Our assumption is that f and g have no common factor in $\mathbb{C}[x, y]$, not that they have no common factor in $F[y]$, so we need to relate these two properties. Factoring polynomials is one of the topics of the next chapter, so we state the fact which we need here and defer the proof (see Chapter 11 (3.9)).

(8.9) **Lemma.** Let $f, g \in \mathbb{C}[x, y]$, and let F be the field of rational functions in x. If f and g have a common factor in $F[y]$ which is not an element of F, then they have a common nonconstant factor in $\mathbb{C}[x, y]$.

We return to the proof of the proposition. Since our two polynomials f, g have no common factor in $\mathbb{C}[x, y]$, they are relatively prime in $F[y]$, so the ideal I they generate in $F[y]$ is the unit ideal. We may therefore write $1 = rf + sg$, where r, s are elements of $F[y]$. Then r, s have denominators which are polynomials in x alone, and we may clear these denominators, multiplying both sides of the equation by a suitable polynomial $p(x)$. This results in an equation of the form

$$p(x) = u(x, y)f(x, y) + v(x, y)g(x, y),$$

where $u, v \in \mathbb{C}[x, y]$. It follows from this equation that a common zero of f and g must also be a zero of p. But p is a polynomial in x alone, and a polynomial in one variable has only finitely many roots. So the variable x takes on only finitely many values at the common zeros of f, g. The same thing is true of the variable y. It follows that the common zeros form a finite set. □

This proposition shows that the most interesting varieties in $\mathbb{C}^2$ are those which are defined as the zeros of a single polynomial $f(x, y)$. These loci are called *algebraic curves,* or *Riemann surfaces,* and their geometry can be quite subtle. A Riemann surface is two-dimensional, so calling it an algebraic curve would seem to be a misnomer. This use of the term *curve* refers to the fact that such a locus can be described analytically by one *complex* parameter, near a point.

A rough description of such a variety, when f is irreducible, follows. (A polynomial is called irreducible if it is not the product of two nonconstant polynomials.)

We regard $f(x, y)$ as a polynomial in y whose coefficients are polynomials in x, say

$$f(x, y) = u_n(x)y^n + \cdots + u_1(x)y + u_0(x), \tag{8.10}$$

with $u_i(x) \in \mathbb{C}[x]$.

(8.11) **Proposition.** Let $f(x, y)$ be an irreducible polynomial in $\mathbb{C}[x, y]$ which is not a polynomial in x alone, and let S be the locus of zeros of f in $\mathbb{C}^2$. Let n denote the degree of f, as a polynomial in y.

(a) For every value a of the variable x, there are at most n points of S whose x-coordinate is a.

(b) There is a finite set Δ of values of x such that if $a \notin \Delta$ then there are exactly n points of S whose x-coordinate is a.

Proof. Let $a \in \mathbb{C}$, and consider the polynomial $f(a, y)$. The points $(a, b) \in S$ are those such that b is a root of $f(a,y)$. This polynomial is not identically zero, because if it were, then $x - a$ would divide each of the coefficients $u_i(x)$, and hence it would divide f. But f is assumed to be irreducible. Next, the degree of $f(a, y)$ in y is at most n, and so it has at most n roots. It will have fewer than n roots if either

(8.12)

(i) The degree of $f(a, y)$ is less than n, or

(ii) the degree of $f(a, y)$ is n, but this polynomial has a multiple root.

Case (i) occurs when the leading coefficient $u_n(x)$ vanishes at a, that is, when a is a root of $u_n(x)$. Since u_n is a polynomial in x, there are finitely many such values.

Now a complex number b is a multiple root of a polynomial $h(y)$ [meaning that $(y - b)^2$ divides $h(y)$] if and only if it is a root of $h(y)$ and of its derivative $h'(y)$. The proof of this fact is left as an exercise. In our situation, $h(y) = f(a, y)$. The first variable is fixed, so the derivative is the partial derivative with respect to y. Thus case (ii) occurs at points (a, b) which are common zeros of f and $\partial f/\partial y$. Note that f does not divide the partial derivative $\partial f/\partial y$, because the degree of the partial derivative in y is $n - 1$, which is less than the degree of f in y. Since f is assumed to be irreducible, f and $\partial f/\partial y$ have no nonconstant factor in common. Proposition (8.8) tells us that there are finitely many common zeros. □

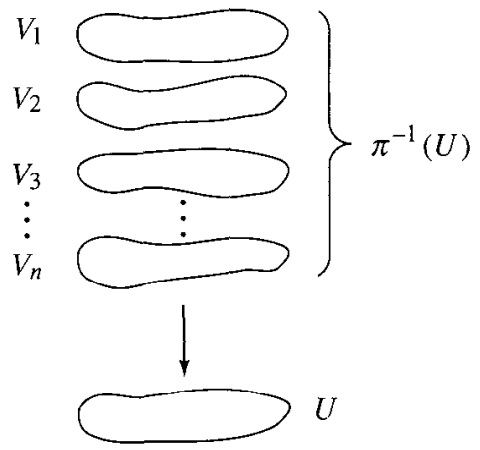
Proposition (8.11) can be summed up by saying that S is an n-sheeted covering of the complex x-plane P. Since there is a finite set Δ above which S has fewer than n sheets, it is called a branched covering. For example, consider the locus $x^2 + xy^2 - 1 = 0$. This equation has two solutions y for every value of x except $x = 0, \pm 1$. There is no solution with $x = 0$, and there is only one with $x = 1$ or -1. So this locus is a branched double covering of P.

Here is the precise definition of a branched covering:

(8.13) **Definition.** An *n-sheeted branched covering* of the complex plane P is a topological space S together with a continuous map π: $S \longrightarrow P$, such that

(a) π is n-to-one on the complement of a finite set Δ in P.

(b) For every point $x_0 \in P - \Delta$, there is an open neighborhood U of x, so that $\pi^{-1}(U)$ is made up of n disconnected parts ($\pi^{-1}(U) = V_1 \cup \cdots \cup V_n$), each V_i is open in S, and π maps V_i homeomorphically to U.



(8.14) **Figure.** Part of an n-sheeted covering.

(8.15) **Corollary.** Let $f(x, y)$ be an irreducible polynomial in $\mathbb{C}[x, y]$ which has degree $n > 0$ in the variable y. The Riemann surface of $f(x, y)$ is an n-sheeted branched covering of the plane.

Proof. The fact that the Riemann surface S of f has the first property of a branched covering is Proposition (8.11). So it remains to verify property (8.13b). Consider a point x_0 at which $f(x_0, y)$ has n roots $y_1, \ldots, y_n$. Then $(\partial f/\partial y)(x_0, y_1) \neq 0$ because y_1 is not a multiple root of $f(x_0, y_1)$. The Implicit Function Theorem [Appendix (4.1)] applies and tells us that equation (8.2) can be solved for $y = \alpha_1(x)$ as a continuous function of x in some neighborhood U of x_0, in such a way that $y_1 = \alpha_1(x_0)$. Similarly, we can solve for $y = \alpha_i(x)$ such that $y_i = \alpha_i(x_0)$. Cutting down the size of U, we may assume that each $\alpha_i(x)$ is defined on U. Since $y_1, \ldots, y_n$ are all distinct and the $\alpha_i(x)$ are continuous functions, they have no common values provided U is made sufficiently small.

Consider the graphs of the n continuous functions α_i:

$$V_i = \{(x, \alpha_i(x)) \mid x \in U\}. \tag{8.16}$$

They are disjoint because the $\alpha_i(x)$ have no common values on U. The map $V_i \longrightarrow U$ is a homeomorphism because it has the continuous inverse function $U \rightsquigarrow V_i$. The inverse sends $x \rightsquigarrow (x, \alpha_i(x))$. And

$$\pi^{-1}(U) = V_1 \cup \cdots \cup V_n$$

because S has at most n points above any x, and the n points have been exhibited as $(x, \alpha_i(x)) \in V_i$. Each of the sets V_i is closed in $U \times \mathbb{C}$, because it is the set of zeros

of the continuous function $y-\alpha_i(x)$. Then V_i is also closed in the subset $\pi^{-1}(U)$ of $U \times \mathbb{C}$. It follows that V_1 is open in $\pi^{-1}(U)$, because it is the complement of the closed set $V_2 \cup \ldots \cup V_n$. Since U is open in $\mathbb{C}$, its inverse image $\pi^{-1}(U)$ is open in S. Thus V_1 is open in an open subset of S, which shows that V_1 is open in S too. Similarly, V_i is open for each i. □

We will look at these loci again in Chapter 13.

In helping geometry, modern algebra is helping itself above all.

Oscar Zariski

EXERCISES

1. Definition of a Ring

1. Prove the following identities in an arbitrary ring R.
   (a) $0a = 0$ **(b)** $-a = (-1)a$ **(c)** $(-a)b = -(ab)$
2. Describe explicitly the smallest subring of the complex numbers which contains the real cube root of 2.
3. Let $\alpha = \frac{1}{2}i$. Prove that the elements of $\mathbb{Z}[\alpha]$ form a dense subset of the complex plane.
4. Prove that $7 + \sqrt[3]{2}$ and $\sqrt{3} + \sqrt{-5}$ are algebraic numbers.
5. Prove that for all integers n, $\cos(2\pi/n)$ is an algebraic number.
6. Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$, $\alpha = \sqrt{2}$, and $\beta = \sqrt{3}$, and let $\gamma = \alpha + \beta$. Prove that $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$.
7. Let S be a subring of $\mathbb{R}$ which is a discrete set in the sense of Chapter 5 (4.3). Prove that $S = \mathbb{Z}$.
8. In each case, decide whether or not S is a subring of R.
   (a) S is the set of all rational numbers of the form a/b, where b is not divisible by 3, and $R = \mathbb{Q}$.
   (b) S is the set of functions which are linear combinations of the functions $\{1, \cos nt, \sin nt \mid n \in \mathbb{Z}\}$, and R is the set of all functions $\mathbb{R} \longrightarrow \mathbb{R}$.
   (c) (not commutative) S is the set of real matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, and R is the set of all real 2×2 matrices.
9. In each case, decide whether the given structure forms a ring. If it is not a ring, determine which of the ring axioms hold and which fail:
   (a) U is an arbitrary set, and R is the set of subsets of U. Addition and multiplication of elements of R are defined by the rules $A + B = A \cup B$ and $A \cdot B = A \cap B$.
   (b) U is an arbitrary set, and R is the set of subsets of U. Addition and multiplication of elements of R are defined by the rules $A + B = (A \cup B) - (A \cap B)$ and $A \cdot B = A \cap B$.
   (c) R is the set of continuous functions $\mathbb{R} \longrightarrow \mathbb{R}$. Addition and multiplication are defined by the rules $[f + g](x) = f(x) + g(x)$ and $[f \circ g](x) = f(g(x))$.
10. Determine all rings which contain the zero ring as a subring.

11. Describe the group of units in each ring.
(a) $\mathbb{Z}/12\mathbb{Z}$ (b) $\mathbb{Z}/7\mathbb{Z}$ (c) $\mathbb{Z}/8\mathbb{Z}$ (d) $\mathbb{Z}/n\mathbb{Z}$
12. Prove that the units in the ring of Gauss integers are $\{\pm 1, \pm i\}$.
13. An element x of a ring R is called *nilpotent* if some power of x is zero. Prove that if x is nilpotent, then $1 + x$ is a unit in R.
14. Prove that the product set $R \times R'$ of two rings is a ring with component-wise addition and multiplication:

$$(a, a') + (b, b') = (a + b, a' + b') \quad \text{and} \quad (a, a')(b, b') = (ab, a'b').$$

This ring is called the *product ring*.

2. Formal Construction of Integers and Polynomials

1. Prove that every natural number n except 1 has the form m' for some natural number m.
2. Prove the following laws for the natural numbers.
(a) the commutative law for addition
(b) the associative law for multiplication
(c) the distributive law
(d) the cancellation law for addition: if $a + b = a + c$, then $b = c$
(e) the cancellation law for multiplication: if $ab = ac$, then $b = c$
3. The relation $<$ on $\mathbb{N}$ can be defined by the rule $a < b$ if $b = a + n$ for some n. Assume that the elementary properties of addition have been proved.
(a) Prove that if $a < b$, then $a + n < b + n$ for all n.
(b) Prove that the relation $<$ is transitive.
(c) Prove that if a, b are natural numbers, then precisely one of the following holds:

$$a < b, \; a = b, \; b < a.$$

(d) Prove that if $n \neq 1$, then $a < an$.
4. Prove the principle of *complete induction:* Let S be a subset of $\mathbb{N}$ with the following property: If n is a natural number such that $m \in S$ for every $m < n$, then $n \in S$. Then $S = \mathbb{N}$.
*5. Define the set $\mathbb{Z}$ of all integers, using two copies of $\mathbb{N}$ and an element representing zero, define addition and multiplication, and derive the fact that $\mathbb{Z}$ is a ring from the properties of addition and multiplication of natural numbers.
6. Let R be a ring. The set of all formal power series $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots$, with $a_i \in R$, forms a ring which is usually denoted by $R[[t]]$. (By *formal power series* we mean that there is no requirement of convergence.)
(a) Prove that the formal power series form a ring.
(b) Prove that a power series $p(t)$ is invertible if and only if a_0 is a unit of R.
7. Prove that the units of the polynomial ring $\mathbb{R}[x]$ are the nonzero constant polynomials.

3. Homomorphisms and Ideals

1. Show that the inverse of a ring isomorphism $\varphi: R \longrightarrow R'$ is an isomorphism.
2. Prove or disprove: If an ideal I contains a unit, then it is the unit ideal.
3. For which integers n does $x^2 + x + 1$ divide $x^4 + 3x^3 + x^2 + 6x + 10$ in $\mathbb{Z}/n\mathbb{Z}[x]$?

4. Prove that in the ring $\mathbb{Z}[x]$, $(2) \cap (x) = (2x)$.
5. Prove the equivalence of the two definitions (3.11) and (3.12) of an ideal.
6. Is the set of polynomials $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ such that 2^{k+1} divides a_k an ideal in $\mathbb{Z}[x]$?
7. Prove that every nonzero ideal in the ring of Gauss integers contains a nonzero integer.
8. Describe the kernel of the following maps.
   (a) $\mathbb{R}[x, y] \longrightarrow \mathbb{R}$ defined by $f(x, y) \rightsquigarrow f(0, 0)$
   (b) $\mathbb{R}[x] \longrightarrow \mathbb{C}$ defomed by $f(x) \rightsquigarrow f(2 + i)$
9. Describe the kernel of the map $\mathbb{Z}[x] \longrightarrow \mathbb{R}$ defined by $f(x) \rightsquigarrow f(1 + \sqrt{2})$.
10. Describe the kernel of the homomorphism φ: $\mathbb{C}[x, y, z] \longrightarrow \mathbb{C}[t]$ defined by $\varphi(x) = t$, $\varphi(y) = t^2$, $\varphi(z) = t^3$.
11. **(a)** Prove that the kernel of the homomorphism φ: $\mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$ defined by $x \rightsquigarrow t^2$, $y \rightsquigarrow t^3$ is the principal ideal generated by the polynomial $y^2 - x^3$.
    (b) Determine the image of φ explicitly.
12. Prove the existence of the homomorphism (3.8).
13. State and prove an analogue of (3.8) when $\mathbb{R}$ is replaced by an arbitrary infinite field.
14. Prove that if two rings R, R′ are isomorphic, so are the polynomial rings $R[x]$ and $R'[x]$.
15. Let R be a ring, and let $f(y) \in R[y]$ be a polynomial in one variable with coefficients in R. Prove that the map $R[x, y] \longrightarrow R[x, y]$ defined by $x \rightsquigarrow x + f(y)$, $y \rightsquigarrow y$ is an automorphism of $R[x, y]$.
16. Prove that a polynomial $f(x) = \Sigma a_i x^i$ can be expanded in powers of $x - a$: $f(x) = \Sigma c_i (x - a)^i$, and that the coefficients c_i are polynomials in the coefficients a_i, with integer coefficients.
17. Let R, R' be rings, and let $R \times R'$ be their product. Which of the following maps are ring homomorphisms?
    (a) $R \longrightarrow R \times R'$, $r \rightsquigarrow (r, 0)$
    (b) $R \longrightarrow R \times R$, $r \rightsquigarrow (r, r)$
    (c) $R \times R' \longrightarrow R$, $(r_1, r_2) \rightsquigarrow r_1$
    (d) $R \times R \longrightarrow R$, $(r_1, r_2) \rightsquigarrow r_1 r_2$
    (e) $R \times R \longrightarrow R$, $(r_1, r_2) \rightsquigarrow r_1 + r_2$
18. **(a)** Is $\mathbb{Z}/(10)$ isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(5)$?
    (b) Is $\mathbb{Z}/(8)$ isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(4)$?
19. Let R be a ring of characteristic p. Prove that the map $R \longrightarrow R$ defined by $x \rightsquigarrow x^p$ is a ring homomorphism. This map is called the *Frobenius homomorphism.*
20. Determine all automorphisms of the ring $\mathbb{Z}[x]$.
21. Prove that the map $\mathbb{Z} \longrightarrow R$ (3.9) is compatible with multiplication of positive integers.
22. Prove that the characteristic of a field is either zero or a prime integer.
23. Let R be a ring of characteristic p. Prove that if a is nilpotent then $1 + a$ is *unipotent,* that is, some power of $1 + a$ is equal to 1.
24. **(a)** The *nilradical* N of a ring R is the set of its nilpotent elements. Prove that N is an ideal.
    (b) Determine the nilradicals of the rings $\mathbb{Z}/(12)$, $\mathbb{Z}/(n)$, and $\mathbb{Z}$.
25. **(a)** Prove Corollary (3.20).
    (b) Prove Corollary (3.22).

26. Determine all ideals of the ring $\mathbb{R}[[t]]$ of formal power series with real coefficients.

27. Find an ideal in the polynomial ring $F[x, y]$ in two variables which is not principal.

***28.** Let R be a ring, and let I be an ideal of the polynomial ring $R[x]$. Suppose that the lowest degree of a nonzero element of I is n and that I contains a monic polynomial of degree n. Prove that I is a principal ideal.

29. Let I, J be ideals of a ring R. Show by example that $I \cup J$ need not be an ideal, but show that $I + J = \{r \in R \mid r = x + y, \text{ with } x \in I, y \in J\}$ is an ideal. This ideal is called the *sum* of the ideals I, J.

30. **(a)** Let I, J be ideals of a ring R. Prove that $I \cap J$ is an ideal.
(b) Show by example that the set of products $\{xy \mid x \in I, y \in J\}$ need not be an ideal, but that the set of finite sums $\Sigma\, x_\nu y_\nu$ of products of elements of I and J is an ideal. This ideal is called the *product ideal*.
(c) Prove that $IJ \subset I \cap J$.
(d) Show by example that IJ and $I \cap J$ need not be equal.

31. Let I, J, J' be ideals in a ring R. Is it true that $I(J + J') = IJ + IJ'$?

***32.** If R is a noncommutative ring, the definition of an *ideal* is a set I which is closed under addition and such that if $r \in R$ and $x \in I$, then both rx and xr are in I. Show that the noncommutative ring of $n \times n$ real matrices has no proper ideal.

33. Prove or disprove: If $a^2 = a$ for all a in a ring R, then R has characteristic 2.

34. An element e of a ring S is called *idempotent* if $e^2 = e$. Note that in a product $R \times R'$ of rings, the element $e = (1, 0)$ is idempotent. The object of this exercise is to prove a converse.
(a) Prove that if e is idempotent, then $e' = 1 - e$ is also idempotent.
(b) Let e be an idempotent element of a ring S. Prove that the principal ideal eS is a ring, with identity element e. It will probably not be a subring of S because it will not contain 1 unless $e = 1$.
(c) Let e be idempotent, and let $e' = 1 - e$. Prove that S is isomorphic to the product ring $(eS) \times (e'S)$.

4. Quotient Rings and Relations in a Ring

1. Prove that the image of the homomorphism φ of Proposition (4.9) is the subring described in the proposition.

2. Determine the structure of the ring $\mathbb{Z}[x]/(x^2 + 3, p)$, where (a) $p = 3$, (b) $p = 5$.

3. Describe each of the following rings.
(a) $\mathbb{Z}[x]/(x^2 - 3, 2x + 4)$ **(b)** $\mathbb{Z}[i]/(2 + i)$

4. Prove Proposition (4.2).

5. Let R' be obtained from a ring R by introducing the relation $\alpha = 0$, and let $\psi\colon R \longrightarrow R'$ be the canonical map. Prove the following *universal property* for this construction: Let $\varphi\colon R \longrightarrow \tilde{R}$ be a ring homomorphism, and assume that $\varphi(\alpha) = 0$ in $\tilde{R}$. There is a unique homomorphism $\varphi'\colon R' \longrightarrow \tilde{R}$ such that $\varphi' \circ \psi = \varphi$.

6. Let I, J be ideals in a ring R. Prove that the residue of any element of $I \cap J$ in R/IJ is nilpotent.

7. Let I, J be ideals of a ring R such that $I + J = R$.
(a) Prove that $IJ = I \cap J$.

*(b) Prove the *Chinese Remainder Theorem:* For any pair a, b of elements of R, there is an element x such that $x \equiv a$ (modulo I) and $x \equiv b$ (modulo J). [The notation $x \equiv a$ (modulo I) means $x - a \in I$.]

8. Let I, J be ideals of a ring R such that $I + J = R$ and $IJ = 0$.
   (a) Prove that R is isomorphic to the product $(R/I) \times (R/J)$.
   (b) Describe the idempotents corresponding to this product decomposition (see exercise 34, Section 3).

5. Adjunction of Elements

1. Describe the ring obtained from $\mathbb{Z}$ by adjoining an element α satisfying the two relations $2\alpha - 6 = 0$ and $\alpha - 10 = 0$.
2. Suppose we adjoin an element α to $\mathbb{R}$ satisfying the relation $\alpha^2 = 1$. Prove that the resulting ring is isomorphic to the product ring $\mathbb{R} \times \mathbb{R}$, and find the element of $\mathbb{R} \times \mathbb{R}$ which corresponds to α.
3. Describe the ring obtained from the product ring $\mathbb{R} \times \mathbb{R}$ by inverting the element $(2, 0)$.
4. Prove that the elements $1, t - \alpha, (t - \alpha)^2, \ldots, (t - \alpha)^{n-1}$ form a $\mathbb{C}$-basis for $\mathbb{C}[t]/((t - \alpha)^n)$.
5. Let α denote the residue of x in the ring $R' = \mathbb{Z}[x]/(x^4 + x^3 + x^2 + x + 1)$. Compute the expressions for $(\alpha^3 + \alpha^2 + \alpha)(\alpha + 1)$ and α^5 in terms of the basis $(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$.
6. In each case, describe the ring obtained from $\mathbb{F}_2$ by adjoining an element α satisfying the given relation.
   (a) $\alpha^2 + \alpha + 1 = 0$ (b) $\alpha^2 + 1 = 0$
7. Analyze the ring obtained from $\mathbb{Z}$ by adjoining an element α which satisfies the pair of relations $\alpha^3 + \alpha^2 + 1 = 0$ and $\alpha^2 + \alpha = 0$.
8. Let $a \in R$. If we adjoin an element α with the relation $\alpha = a$, we expect to get back a ring isomorphic to R. Prove that this is so.
9. Describe the ring obtained from $\mathbb{Z}/12\mathbb{Z}$ by adjoining an inverse of 2.
10. Determine the structure of the ring R' obtained from $\mathbb{Z}$ by adjoining element α satisfying each set of relations.
    (a) $2\alpha = 6, 6\alpha = 15$ (b) $2\alpha = 6, 6\alpha = 18$ (c) $2\alpha = 6, 6\alpha = 8$
11. Let $R = \mathbb{Z}/(10)$. Determine the structure of the ring obtained by adjoining an element α satisfying each relation.
    (a) $2\alpha - 6 = 0$ (b) $2\alpha - 5 = 0$
12. Let a be a unit in a ring R. Describe the ring $R' = R[x]/(ax - 1)$.
13. (a) Prove that the ring obtained by inverting x in the polynomial ring $R[x]$ is isomorphic to the ring of Laurent polynomials, as asserted in (5.9).
    (b) Do the formal Laurent series $\sum_{-\infty}^{\infty} a_n x^n$ form a ring?
14. Let a be an element of a ring R, and let $R' = R[x]/(ax - 1)$ be the ring obtained by adjoining an inverse of a to R. Prove that the kernel of the map $R \longrightarrow R'$ is the set of elements $b \in R$ such that $a^n b = 0$ for some $n > 0$.
15. Let a be an element of a ring R, and let R' be the ring obtained from R by adjoining an inverse of a. Prove that R' is the zero ring if and only if a is nilpotent.

16. Let F be a field. Prove that the rings $F[x]/(x^2)$ and $F[x]/(x^2 - 1)$ are isomorphic if and only if F has characteristic 2.
17. Let $\bar{R} = \mathbb{Z}[x]/(2x)$. Prove that every element of $\bar{R}$ has a unique expression in the form $a_0 + a_1x + \cdots + a_nx^n$, where a_i are integers and $a_1, \ldots, a_n$ are either 0 or 1.

6. Integral Domains and Fraction Fields

1. Prove that a subring of an integral domain is an integral domain.
2. Prove that an integral domain with finitely many elements is a field.
3. Let R be an integral domain. Prove that the polynomial ring $R[x]$ is an integral domain.
4. Let R be an integral domain. Prove that the invertible elements of the polynomial ring $R[x]$ are the units in R.
5. Is there an integral domain containing exactly 10 elements?
6. Prove that the field of fractions of the formal power series ring $F[[x]]$ over a field F is obtained by inverting the single element x, and describe the elements of this field as certain power series with negative exponents.
7. Carry out the verification that the equivalence classes of fractions from an integral domain form a field.
8. A semigroup S is a set with an associative law of composition having an identity element. Let S be a commutative semigroup which satisfies the cancellation law: $ab = ac$ implies $b = c$. Use fractions to prove that S can be embedded into a group.

*9. A subset S of an integral domain R which is closed under multiplication and which does not contain 0 is called a *multiplicative set*. Given a multiplicative set S, we define S-fractions to be elements of the form a/b, where $b \in S$. Show that the equivalence classes of S-fractions form a ring.

7. Maximal Ideals

1. Prove that the maximal ideals of the ring of integers are the principal ideals generated by prime integers.
2. Determine the maximal ideals of each of the following.
   (a) $\mathbb{R} \times \mathbb{R}$ **(b)** $\mathbb{R}[x]/(x^2)$ **(c)** $\mathbb{R}[x]/(x^2 - 3x + 2)$ **(d)** $\mathbb{R}[x]/(x^2 + x + 1)$
3. Prove that the ideal $(x + y^2, y + x^2 + 2xy^2 + y^4)$ in $\mathbb{C}[x, y]$ is a maximal ideal.
4. Let R be a ring, and let I be an ideal of R. Let M be an ideal of R containing I, and let $\bar{M} = M/I$ be the corresponding ideal of $\bar{R}$. Prove that M is maximal if and only if $\bar{M}$ is.
5. Let I be the principal ideal of $\mathbb{C}[x, y]$ generated by the polynomial $y^2 + x^3 - 17$. Which of the following sets generate maximal ideals in the quotient ring $R = \mathbb{C}[x, y]/I$?
   (a) $(x - 1, y - 4)$ **(b)** $(x + 1, y + 4)$ **(c)** $(x^3 - 17, y^2)$
6. Prove that the ring $\mathbb{F}_5[x]/(x^2 + x + 1)$ is a field.
7. Prove that the ring $\mathbb{F}_2[x]/(x^3 + x + 1)$ is a field, but that $\mathbb{F}_3[x]/(x^3 + x + 1)$ is not a field.
8. Let $R = \mathbb{C}[x_1, \ldots, x_n]/I$ be a quotient of a polynomial ring over $\mathbb{C}$, and let M be a maximal ideal of R. Prove that $R/M \approx \mathbb{C}$.
9. Define a bijective correspondence between maximal ideals of $\mathbb{R}[x]$ and points in the upper half plane.

10. Let R be a ring, with M an ideal of R. Suppose that every element of R which is not in M is a unit of R. Prove that M is a maximal ideal and that moreover it is the only maximal ideal of R.

11. Let P be an ideal of a ring R. Prove that $\bar{R} = R/P$ is an integral domain if and only if $P \neq R$, and that if $a, b \in R$ and $ab \in P$, then $a \in P$ or $b \in P$. (An ideal P satisfying these conditions is called a *prime ideal.*)

12. Let $\varphi\colon R \longrightarrow R'$ be a ring homomorphism, and let P' be a prime ideal of R'.
(a) Prove that $\varphi^{-1}(P')$ is a prime ideal of R.
(b) Give an example in which P' is a maximal ideal, but $\varphi^{-1}(P')$ is not maximal.

***13.** Let R be an integral domain with fraction field F, and let P be a prime ideal of R. Let R_p be the subset of F defined by

$$R_p = \{a/d \mid a, d \in R, d \notin P\}.$$

This subset is called the *localization of R at P.*
(a) Prove that R_p is a subring of F.
(b) Determine all maximal ideals of R_p.

14. Find an example of a "ring without unit element" and an ideal not contained in a maximal ideal.

8. Algebraic Geometry

1. Determine the points of intersection of the two complex plane curves in each of the following.
(a) $y^2 - x^3 + x^2 = 1, \quad x + y = 1$
(b) $x^2 + xy + y^2 = 1, \quad x^2 + 2y^2 = 1$
(c) $y^2 = x^3, \quad xy = 1$
(d) $x + y + y^2 = 0, \quad x - y + y^2 = 0$
(e) $x + y^2 = 0, \quad y + x^2 + 2xy^2 + y^4 = 0$

2. Prove that two quadratic polynomials f, g in two variables have at most four common zeros, unless they have a nonconstant factor in common.

3. Derive the Hilbert Nullstellensatz from its classical form (8.7).

4. Let U, V be varieties in $\mathbb{C}^n$. Prove that $U \cup V$ and $U \cap V$ are varieties.

5. Let $f_1, \ldots, f_r;\ g_1, \ldots, g_s \in \mathbb{C}[x_1, \ldots, x_n]$, and let U, V be the zeros of $\{f_1, \ldots, f_r\}$, $\{g_1, \ldots, g_s\}$ respectively. Prove that if U and V do not meet, then $(f_1, \ldots, f_r; g_1, \ldots, g_s)$ is the unit ideal.

6. Let $f = f_1 \cdots f_m$ and $g = g_1 \cdots g_n$, where f_i, g_j are irreducible polynomials in $\mathbb{C}[x, y]$. Let $S_i = \{f_i = 0\}$ and $T_j = \{g_j = 0\}$ be the Riemann surfaces defined by these polynomials, and let V be the variety $f = g = 0$. Describe V in terms of S_i, T_j.

7. Prove that the variety defined by a set $\{f_1, \ldots, f_r\}$ of polynomials depends only on the ideal $(f_1, \ldots, f_r)$ they generate.

8. Let R be a ring containing $\mathbb{C}$ as subring.
(a) Show how to make R into a vector space over $\mathbb{C}$.
(b) Assume that R is a finite-dimensional vector space over $\mathbb{C}$ and that R contains exactly one maximal ideal M. Prove that M is the *nilradical* of R, that is, that M consists precisely of its nilpotent elements.

9. Prove that the complex conic $xy = 1$ is homeomorphic to the plane, with one point deleted.

10. Prove that every variety in $\mathbb{C}^2$ is the union of finitely many points and algebraic curves.

11. The three polynomials $f_1 = x^2 + y^2 - 1$, $f_2 = x^2 - y + 1$, and $f_3 = xy - 1$ generate the unit ideal in $\mathbb{C}[x, y]$. Prove this in two ways: (i) by showing that they have no common zeros, and (ii) by writing 1 as a linear combination of f_1, f_2, f_3, with polynomial coefficients.

12. **(a)** Determine the points of intersection of the algebraic curve S: $y^2 = x^3 - x^2$ and the line L: $y = \lambda x$.
(b) Parametrize the points of S as a function of λ.
(c) Relate S to the complex λ-plane, using this parametrization.

***13.** The *radical* of an ideal I is the set of elements $r \in R$ such that some power of r is in I.
(a) Prove that the radical of I is an ideal.
(b) Prove that the varieties defined by two sets of polynomials $\{f_1, \ldots, f_r\}, \{g_1, \ldots, g_s\}$ are equal if and only if the two ideals $(f_1, \ldots, f_r), (g_1, \ldots, g_s)$ have the same radicals.

***14.** Let $R = \mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Let A be a ring containing $\mathbb{C}$ as subring. Find a bijective correspondence between the following sets:
(i) homomorphisms φ: $R \longrightarrow A$ which restrict to the identity on $\mathbb{C}$, and
(ii) n-tuples $a = (a_1, \ldots, a_n)$ of elements of A which solve the system of equations $f_1 = \ldots = f_m = 0$, that is, such that $f_i(a) = 0$ for $i = 1, \ldots, m$.

Miscellaneous Exercises

1. Let F be a field, and let K denote the vector space F^2. Define multiplication by the rules $(a_1, a_2) \cdot (b_1, b_2) = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)$.
(a) Prove that this law and vector addition make K into a ring.
(b) Prove that K is a field if and only if there is no element in F whose square is -1.
(c) Assume that -1 is a square in F and that F does not have characteristic 2. Prove that K is isomorphic to the product ring $F \times F$.

2. **(a)** We can define the derivative of an arbitrary polynomial $f(x)$ with coefficients in a ring R by the calculus formula $(a_nx^n + \cdots + a_1x + a_0)' = na_nx^{n-1} + \cdots + 1a_1$. The integer coefficients are interpreted in R using the homomorphism (3.9). Prove the product formula $(fg)' = f'g + fg'$ and the chain rule $(f \circ g)' = (f' \circ g)g'$.
(b) Let $f(x)$ be a polynomial with coefficients in a field F, and let α be an element of F. Prove that α is a multiple root of f if and only if it is a common root of f and of its derivative f'.
(c) Let $F = \mathbb{F}_5$. Determine whether or not the following polynomials have multiple roots in F: $x^{15} - x$, $x^{15} - 2x^5 + 1$.

3. Let R be a set with two laws of composition satisfying all the ring axioms except the commutative law for addition. Prove that this law holds by expanding the product $(a + b)(c + d)$ in two ways using the distributive law.

4. Let R be a ring. Determine the units in the polynomial ring $R[x]$.

5. Let R denote the set of sequences $a = (a_1, a_2, a_3, \ldots)$ of real numbers which are eventually constant: $a_n = a_{n+1} = \ldots$ for sufficiently large n. Addition and multiplication are component-wise; that is, addition is vector addition and $ab = (a_1b_1, a_2b_2, \ldots)$.
(a) Prove that R is a ring.
(b) Determine the maximal ideals of R.

6. **(a)** Classify rings R which contain $\mathbb{C}$ and have dimension 2 as vector space over $\mathbb{C}$.
***(b)** Do the same as (a) for dimension 3.

*7. Consider the map φ: $\mathbb{C}[x,y] \longrightarrow \mathbb{C}[x] \times \mathbb{C}[y] \times \mathbb{C}[t]$ defined by $f(x,y) \rightsquigarrow (f(x,0), f(0,y), f(t,t))$. Determine the image of φ explicitly.

8. Let S be a subring of a ring R. The *conductor* C of S in R is the set of elements $\alpha \in R$ such that $\alpha R \subset S$.
   (a) Prove that C is an ideal of R and also an ideal of S.
   (b) Prove that C is the largest ideal of S which is also an ideal of R.
   (c) Determine the conductor in each of the following three cases:
   (i) $R = \mathbb{C}[t]$, $S = \mathbb{C}[t^2, t^3]$;
   (ii) $R = \mathbb{Z}[\zeta]$, $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$, $S = \mathbb{Z}[\sqrt{-3}]$;
   (iii) $R = \mathbb{C}[t, t^{-1}]$, $S = \mathbb{C}[t]$.

9. A *line* in $\mathbb{C}^2$ is the locus of a linear equation L: $\{ax + by + c = 0\}$. Prove that there is a unique line through two points $(x_0, y_0), (x_1, y_1)$, and also that there is a unique line through a point (x_0, y_0) with a given tangent direction (u_0, v_0).

10. An algebraic curve C in $\mathbb{C}^2$ is called *irreducible* if it is the locus of zeros of an irreducible polynomial $f(x,y)$—one which can not be factored as a product of nonconstant polynomials. A point $p \in C$ is called a *singular point* of the curve if $\partial f/\partial x = \partial f/\partial y = 0$ at p. Otherwise p is a *nonsingular* point. Prove that an irreducible curve has only finitely many singular points.

11. Let L: $ax + by + c = 0$ be a line and C: $\{f = 0\}$ a curve in $\mathbb{C}^2$. Assume that $b \neq 0$. Then we can use the equation of the line to eliminate y from the equation $f(x,y) = 0$ of C, obtaining a polynomial $g(x)$ in x. Show that its roots are the x-coordinates of the intersection points.

12. With the notation as in the preceding problem, the *multiplicity of intersection* of L and C at a point $p = (x_0, y_0)$ is the multiplicity of x_0 as a root of $g(x)$. The line is called a *tangent line* to C at p if the multiplicity of intersection is at least 2. Show that if p is a nonsingular point of C, then there is a unique tangent line at (x_0, y_0), and compute it.

13. Show that if p is a singular point of a curve C, then the multiplicity of intersection of every line through p is at least 2.

14. The *degree* of an irreducible curve C: $\{f = 0\}$ is defined to be the degree of the irreducible polynomial f.
   (a) Prove that a line L meets C in at most d points, unless $C = L$.
   *(b) Prove that there exist lines which meet C in precisely d points.

15. Determine the singular points of $x^3 + y^3 - 3xy = 0$.

*16. Prove that an irreducible cubic curve can have at most one singular point.

*17. A nonsingular point p of a curve C is called a *flex point* if the tangent line L to C at p has an intersection of multiplicity at least 3 with C at p.
   (a) Prove that the flex points are the nonsingular points of C at which the *Hessian*

$$\det \begin{bmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial f}{\partial x} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} & \frac{\partial f}{\partial y} \\ \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} & f \end{bmatrix}$$

   vanishes.
   (b) Determine the flex points of the cubic curves $y^2 - x^3$ and $y^2 - x^3 + x^2$.

*18. Let C be an irreducible cubic curve, and let L be a line joining two flex points of C. Prove that if L meets C in a third point, then that point is also a flex.

19. Let $U = \{f_i(x_1,\dots,x_m) = 0\}$, $V = \{g_j(y_1,\dots,y_n) = 0\}$ be two varieties. Show that the variety defined by the equations $\{f_i(x) = 0, g_j(y) = 0\}$ in $\mathbb{C}^{m+n}$ is the product set $U \times V$.

20. Prove that the locus $y = \sin x$ in $\mathbb{R}^2$ doesn't lie on any algebraic curve.

*21. Let f, g be polynomials in $\mathbb{C}[x, y]$ with no common factor. Prove that the ring $R = \mathbb{C}[x, y]/(f, g)$ is a finite-dimensional vector space over $\mathbb{C}$.

22. (a) Let s, c denote the functions $\sin x$, $\cos x$ on the real line. Prove that the ring $\mathbb{R}[s, c]$ they generate is an integral domain.
(b) Let $K = \mathbb{R}(s, c)$ denote the field of fractions of $\mathbb{R}[s, c]$. Prove that the field K is isomorphic to the field of rational functions $\mathbb{R}(x)$.

*23. Let $f(x)$, $g(x)$ be polynomials with coefficients in a ring R with $f \neq 0$. Prove that if the product $f(x)g(x)$ is zero, then there is a nonzero element $c \in R$ such that $cg(x) = 0$.

*24. Let X denote the closed unit interval $[0, 1]$, and let R be the ring of continuous functions $X \longrightarrow \mathbb{R}$.
(a) Prove that a function f which does not vanish at any point of X is invertible in R.
(b) Let $f_1,\dots, f_n$ be functions with no common zero on X. Prove that the ideal generated by these functions is the unit ideal. (Hint: Consider $f_1^2 + \cdots + f_n^2$.)
(c) Establish a bijective correspondence between maximal ideals of R and points on the interval.
(d) Prove that the maximal ideals containing a function f correspond to points of the interval at which $f = 0$.
(e) Generalize these results to functions on an arbitrary compact set X in $\mathbb{R}^k$.
(f) Describe the situation in the case $X = \mathbb{R}$.