CHAPTER 11

Rings

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

—Edmund Landau

11.1 DEFINITION OF A RING

Rings are algebraic structures closed under addition, subtraction, and multiplication, but not under division. The integers form our basic model for this concept.

Before going to the definition of a ring, we look at a few examples, 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.

• The *Gauss integers* , the complex numbers of the form $a + bi$, where a and b are integers, form a subring of $\mathbb{C}$ that we denote by $\mathbb{Z}[i]$:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}. \tag{11.1.1}$$

Its elements 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: the subring *generated by* α. This is the smallest subring of $\mathbb{C}$ that contains α, and it can be described in a general way. If a ring contains α, then it contains all positive powers of α because it is closed under multiplication. It also contains sums and differences of such powers, and it contains 1. Therefore it contains every complex number β that can be expressed as an integer combination of powers of α, or, saying this another way, can be obtained by evaluating a polynomial with integer coefficients at α:

$$\beta = a_n\alpha^n + \cdots + a_1\alpha + a_0, \quad \text{where } a_i \text{ are in } \mathbb{Z}. \tag{11.1.2}$$

On the other hand, the set of all such numbers is closed under the operations $+$, $-$, and $\times$, and it contains 1. So it is the subring generated by α.

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

• A complex number α is *algebraic* if it is a root of a (nonzero) polynomial with integer coefficients – that is, if some expression of the form (11.1.2) evaluates to zero. If there is no polynomial with integer coefficients having α as a root, α is *transcendental*. The numbers e and π are transcendental, though it isn't very easy to prove this.

When α is transcendental, two distinct polynomial expressions (11.1.2) represent distinct complex numbers. Then the elements of the ring $\mathbb{Z}[\alpha]$ correspond bijectively to polynomials $p(x)$ with integer coefficients, by the rule $p(x) \rightsquigarrow p(\alpha)$. When α is algebraic there will be many polynomial expressions that represent the same complex number. Some examples of algebraic numbers are: $i+3$, $1/7$, $7+\sqrt[3]{2}$, and $\sqrt{3}+\sqrt{-5}$.

The definition of a ring is similar to that of field (3.2.2). The only difference is that multiplicative inverses aren't required:

Definition 11.1.3 $(+, -, \times, 1)$ A *ring* R is a set with two laws of composition $+$ and $\times$, called addition and multiplication, that satisfy these axioms:

(a) With the law of composition $+$, R is an abelian group that we denote by R^+; its identity is denoted by 0.

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

(c) *distributive law*: For all a, b, and c in R, $(a+b)c = ac+bc$.

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

Note: There is a related concept, of a *noncommutative ring* – a structure that satisfies all axioms of (11.1.3) except the commutative law for multiplication. The set of all real $n \times n$ matrices is one example. Since we won't be studying noncommutative rings, we use the word "ring" to mean "commutative ring." □

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

$$a_n x^n + \cdots + a_1 x + a_0, \tag{11.1.4}$$

with a_i in R. The set of these polynomials forms a ring that we discuss in the next section.

Another example: The set $\mathcal{R}$ of continuous real-valued functions of a real variable x forms a ring, with addition and multiplication of functions: $[f+g](x) = f(x)+g(x)$ and $[fg](x) = f(x)g(x)$.

There is a ring that contains just one element, 0; it is called the *zero ring*. In the definition of a field (3.2.2), the set $F^\times$ obtained by deleting 0 is a group that contains the multiplicative identity 1. So 1 is not equal to 0 in a field. The relation $1 = 0$ hasn't been ruled out in a ring, but it occurs only once:

Proposition 11.1.5 A ring R in which the elements 1 and 0 are equal is the zero ring.

Proof. We first note that $0a = 0$ for every element a of a ring R. The proof is the same as for vector spaces: $0 = 0a - 0a = (0-0)a = 0a$. Assume that $1 = 0$ in R, and let a be any element. Then $a = 1a = 0a = 0$. The only element of R is 0. □

Though elements of a ring aren't required to have multiplicative inverses, a particular element may have an inverse, and the inverse is unique if it exists.

• A *unit* of a ring is an element that has a multiplicative inverse.

The units in the ring of integers are 1 and -1, and the units in the ring of Gauss integers are ± 1 and $\pm i$. The units in the ring $\mathbb{R}[x]$ of real polynomials are the nonzero constant polynomials. Fields are rings in which $0 \neq 1$ 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 element. The ambiguous term "unit" is poorly chosen, but it is too late to change it.

11.2 POLYNOMIAL RINGS

• A *polynomial* with coefficients in a ring R is a (finite) linear combination of powers of the variable:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \tag{11.2.1}$$

where the *coefficients* a_i are elements of R. Such an expression is sometimes called a *formal polynomial*, to distinguish it from a polynomial function. Every formal polynomial with real coefficients determines a polynomial function on the real numbers. But we use the word *polynomial* to mean formal polynomial.

The set of polynomials with coefficients in a ring R will be denoted by $R[x]$. Thus $\mathbb{Z}[x]$ denotes the set of polynomials with integer coefficients – the set of *integer polynomials*.

The *monomials* x^i are considered independent. So if

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \tag{11.2.2}$$

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, which may be denoted by $\deg f$, is the largest integer n such that the coefficient a_n of x_n is not zero. A polynomial of degree zero is called a *constant* polynomial. The zero polynomial is also called a constant polynomial, but its degree will not be defined.

The nonzero coefficient of highest degree of a polynomial is its *leading coefficient*, and a *monic* polynomial is one whose leading coefficient is 1.

The possibility that some coefficients of a polynomial may be zero creates a nuisance. We have to disregard terms with zero coefficient, so the polynomial $f(x)$ can be written in more than one way. This is irritating because it isn't an interesting point. One way to avoid ambiguity is to imagine listing the coefficients of all monomials, whether zero or not. This allows efficient verification of the ring axioms. So for the purpose of defining the ring operations, we write a polynomial as

$$f(x) = a_0 + a_1 x + a_1 x^2 + \cdots, \tag{11.2.3}$$

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

$$a = (a_0, a_1, \ldots), \tag{11.2.4}$$

where a_i are elements of R, all but a finite number zero. Every such vector corresponds to a polynomial.

When R is a field, these infinite vectors form the vector space Z with the infinite basis e_i that was defined in (3.7.2). The vector e_i corresponds to the monomial x^i, and the monomials form a basis of the space of all polynomials.

The definitions of addition and multiplication of polynomials mimic the familiar operations on polynomial functions. If $f(x)$ and $g(x)$ are polynomials, then with notation as above, their sum is

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots = \sum_k (a_k + b_k)x^k, \tag{11.2.5}$$

where the notation $(a_i + b_i)$ refers to addition in R. So if we think of a polynomial as a vector, addition is vector addition: $a + b = (a_0 + b_0,\ a_1 + b_1, \ldots)$.

The product of polynomials f and g is computed by expanding the product:

$$f(x)g(x) = (a_0 + a_1x + \cdots)(b_0 + b_1x + \cdots) = \sum_{i,j} a_i b_j x^{i+j}, \tag{11.2.6}$$

where the products a_ib_j are to be evaluated in the ring R. There will be finitely many nonzero coefficients a_ib_j. This is a correct formula, but the right side is not in the standard form (11.2.3), because the same monomial x^n appears several times – once for each pair i, j of indices such that $i + j = n$. So terms have to be collected on the right side. This leads to the definition

$$f(x)g(x) = p_0 + p_1x + p_2x^2 + \cdots, \tag{11.2.7}$$

with

$$p_k = \sum_{i+j=k} a_ib_j,$$

$$p_0 = a_0b_0, \quad p_1 = a_0b_1 + a_1b_0, \quad p_2 = a_0b_2 + a_1b_1 + a_2b_0, \ \ldots$$

Each p_k is evaluated using the laws of composition in the ring. However, when making computations, it may be desirable to defer the collection of terms temporarily.

Proposition 11.2.8 There is a unique commutative ring structure on the set of polynomials $R[x]$ having these properties:

- Addition of polynomials is defined by (11.2.5).
- Multiplication of polynomials is defined by (11.2.7).
- The ring R becomes a subring of $R[x]$ when the elements of R are identified with the constant polynomials.

Since polynomial algebra is familiar and since the proof of this proposition has no interesting features, we omit it. □

Division with remainder is an important operation on polynomials.

Proposition 11.2.9 Division with Remainder. Let R be a ring, let f be a monic polynomial and let g be any polynomial, both with coefficients in R. There are uniquely determined polynomials q and r in $R[x]$ such that

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

and such that the remainder r, if it is not zero, has degree less than the degree of f. Moreover, f divides g in $R[x]$ if and only if the remainder r is zero.

The proof of this proposition follows the algorithm for division of polynomials that one learns in school. □

Corollary 11.2.10 Division with remainder can be done whenever the leading coefficient of f is a unit. In particular, it can be done whenever the coefficient ring is a field and $f \neq 0$.

If the leading coefficient is a unit u, we can factor it out of f. □

However, one cannot divide $x^2 + 1$ by $2x + 1$ in the ring $\mathbb{Z}[x]$ of integer polynomials.

Corollary 11.2.11 Let $g(x)$ be a polynomial in $R[x]$, and let α be an element of R. The remainder of division of $g(x)$ by $x - \alpha$ is $g(\alpha)$. Thus $x - \alpha$ divides g in $R[x]$ if and only if $g(\alpha) = 0$.

This corollary is proved by substituting $x = \alpha$ into the equation $g(x) = (x - \alpha)q(x) + r$ and noting that r is a constant. □

Polynomials are fundamental to the theory of rings, and we will also want to use polynomials in several variables. There is no major change in the definitions.

- A *monomial* is a formal product of some variables $x_1, \ldots, x_n$ of the form

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

where the exponents i_ν are non-negative integers. The *degree* of a monomial, sometimes called the *total degree*, is the sum $i_1 + \cdots + i_n$.

An n-tuple $(i_1, \ldots, i_n)$ is called a *multi-index*, and vector notation $i = (i_1, \ldots, i_n)$ for multi-indices is convenient. Using multi-index notation, we may write a monomial symbolically as x^i:

$$x^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}. \tag{11.2.12}$$

The monomial x^0, with $0 = (0, \ldots, 0)$, is denoted by 1. A *polynomial* in the variables $x_1, \ldots, x_n$, with coefficients in a ring R, is a linear combination of finitely many monomials,

with coefficients in R. With multi-index notation, a polynomial $f(x) = f(x_1, \ldots, x_n)$ can be written in exactly one way in the form

$$f(x) = \sum_i a_i x^i, \tag{11.2.13}$$

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

A polynomial in which all monomials with nonzero coefficients have (total) degree d is called a *homogeneous* polynomial.

Using multi-index notation, formulas (11.2.5) and (11.2.7) define addition and multiplication of polynomials in several variables, and the analogue of Proposition 11.2.8 is true. However, division with remainder requires more thought. We will come back to it below (see Corollary 11.3.9).

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

$$R[x_1, \ldots, x_n] \quad \text{or} \quad R[x], \tag{11.2.14}$$

where the symbol x is understood to refer to the set of variables $\{x_1, \ldots, x_n\}$. When no set of variables has been introduced, $R[x]$ denotes the polynomial ring in one variable.

11.3 HOMOMORPHISMS AND IDEALS

• A *ring homomorphism* $\varphi: R \to R'$ is a map from one ring to another which is compatible with the laws of composition and which carries the unit element 1 of R to the unit element 1 in R' – a map such that, for all a and b in R,

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \text{and} \quad \varphi(1) = 1. \tag{11.3.1}$$

The map

$$\varphi : \mathbb{Z} \to \mathbb{F}_p \tag{11.3.2}$$

that sends an integer to its congruence class modulo p is a ring homomorphism.

An *isomorphism* of rings is a bijective homomorphism, and if there is an isomorphism from R to R', the two rings are said to be *isomorphic*. We often use the notation $R \approx R'$ to indicate that two rings R and R' are isomorphic.

A word about the third condition of (11.3.1): The assumption that a homomorphism φ is compatible with addition implies that it is a homomorphism from the additive group R^+ of R to the additive group R'^+. A group homomorphism carries the identity to the identity, so $\varphi(0) = 0$. But we can't conclude that $\varphi(1) = 1$ from compatibility with multiplication, so that condition must be listed separately. (R is not a group with respect to $\times$.) For example, the *zero map* $R \to R'$ that sends 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 is not called a ring homomorphism unless R' is the zero ring (see (11.1.5)).

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

$$\mathbb{R}[x] \to \mathbb{R}, \quad \text{that sends} \quad p(x) \rightsquigarrow p(a). \tag{11.3.3}$$

One can also evaluate real polynomials at a complex number such as i, to obtain a homomorphism $\mathbb{R}[x] \to \mathbb{C}$ that sends $p(x) \rightsquigarrow p(i)$.

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

Proposition 11.3.4 Substitution Principle. Let $\varphi: R \to R'$ be a ring homomorphism, and let $R[x]$ be the ring of polynomials with coefficients in R.

(a) Let α be an element of R'. There is a unique homomorphism $\Phi: R[x] \to R'$ that agrees with the map φ on constant polynomials, and that sends $x \rightsquigarrow \alpha$.

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

Proof. **(a)** Let us denote the image $\varphi(a)$ of an element a of R by a'. Using the fact that Φ is a homomorphism that restricts to φ on R and sends x to α, we see that it acts on a polynomial $f(x) = \sum a_i x^i$ by sending

$$\Phi\Big(\sum a_i x^i\Big) = \sum \Phi(a_i)\Phi(x)^i = \sum a_i' \alpha^i. \tag{11.3.5}$$

In words, Φ acts on the coefficients of a polynomial as φ, and it substitutes α for x. Since this formula describes Φ, 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 Φ is a homomorphism $R[x] \to R'$. It is clear that 1 is sent to 1, and it is easy to verify compatibility with addition of polynomials. Compatibility with multiplication is checked using formula (11.2.6):

$$\Phi(fg) = \Phi\Big(\sum a_i b_j x^{i+j}\Big) = \sum \Phi(a_i b_j x^{i+j}) = \sum_{i,j} a_i' b_j' \alpha^{i+j}$$
$$= \Big(\sum_i a_i' \alpha^i\Big)\Big(\sum_j b_j' \alpha^i\Big) = \Phi(f)\Phi(g).$$

With multi-index notation, the proof of **(b)** becomes the same as that of **(a)**. □

Here is a simple example of the substitution principle in which the coefficient ring R changes. Let $\psi: R \to S$ be a ring homomorphism. Composing ψ with the inclusion of S as a subring of the polynomial ring $S[x]$, we obtain a homomorphism $\varphi: R \to S[x]$. The substitution principle asserts that there is a unique extension of φ to a homomorphism $\Phi: R[x] \to S[x]$ that sends $x \rightsquigarrow x$. This map operates on the coefficients of a polynomial, while 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 $a_n' x^n + \cdots + a_1' x + a_0'$.

A particularly interesting case is that φ is the homomorphism $\mathbb{Z} \to \mathbb{F}_p$ that sends an integer a to its residue $\bar{a}$ modulo p. This map extends to a homomorphism $\Phi: \mathbb{Z}[x] \to \mathbb{F}_p[x]$, defined by

$$f(x) = a_n x^n + \cdots + a_0 \rightsquigarrow \bar{a}_n x^n + \cdots + \bar{a}_0 = \bar{f}(x), \tag{11.3.6}$$

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

Another example: Let R be any ring, and let P denote the polynomial ring $R[x]$. One can use the substitution principle to construct an isomorphism

$$R[x, y] \to P[y] = (R[x])[y]. \tag{11.3.7}$$

This is stated and proved below in Proposition 11.3.8. The domain is the ring of polynomials in two variables x and y, and the range is 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 $f(x, y)$. For example,

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

This procedure can be useful. For one thing, one may end up with a polynomial that is monic in the variable y, as happens in the example above. If so, one can do division with remainder (see Corollary 11.3.9 below).

Proposition 11.3.8 Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_n)$ denote sets of variables. There is a unique isomorphism $R[x, y] \to R[x][y]$, which is the identity on R and which sends the variables to themselves.

This is very elementary, but it would be boring to verify compatibility of multiplication in the two rings directly.

Proof. We note that since R is a subring of $R[x]$ and $R[x]$ is a subring of $R[x][y]$, R is also a subring of $R[x][y]$. Let φ be the inclusion of R into $R[x][y]$. The substitution principle tells us that there is a unique homomorphism $\Phi: R[x, y] \to R[x][y]$, which extends φ and sends the variables x_μ and y_ν wherever we want. So we can send the variables to themselves. The map Φ thus constructed is the required isomorphism. It isn't difficult to see that Φ is bijective. One way to show this would be to use the substitution principle again, to define the inverse map. □

Corollary 11.3.9 Let $f(x, y)$ and $g(x, y)$ be polynomials in two variables, elements of $R[x, y]$. Suppose that, when regarded as a polynomial in y, f is a monic polynomial of degree m. There are uniquely determined polynomials $q(x, y)$ and $r(x, y)$ such that $g = fq + r$, and such that if $r(x, y)$ is not zero, its degree in the variable y is less than m.

This follows from Propositions 11.2.9 and 11.3.8. □

Another case in which one can describe homomorphisms easily is when the domain is the ring of integers.

Proposition 11.3.10 Let R be a ring. There is exactly one homomorphism $\varphi: \mathbb{Z} \to R$ from the ring of integers to R. It is the map defined, for $n \geq 0$, by $\varphi(n) = 1 + \cdots + 1$ (n terms) and $\varphi(-n) = -\varphi(n)$.

Sketch of Proof. Let $\varphi: \mathbb{Z} \to R$ be a homomorphism. By definition of a homomorphism, $\varphi(1) = 1$ and $\varphi(n + 1) = \varphi(n) + \varphi(1)$. This recursive definition describes φ on the natural

numbers, and together with $\varphi(-n) = -\varphi(n)$ if $n > 0$ and $\varphi(0) = 0$, it determines φ uniquely. So it is the only map $\mathbb{Z} \to R$ that could be a homomorphism, and it isn't hard to convince oneself that it is one. To prove this formally, one would go back to the definitions of addition and multiplication of integers (see Appendix). □

Proposition (11.3.10) allows us to identify the image of an integer in an arbitrary ring R. We interpet the symbol 3, for example, as the element $1 + 1 + 1$ of R.

• Let $\varphi: R \to R'$ be a ring homomorphism. The *kernel* of φ is the set of elements of R that map to zero:

$$\ker \varphi = \{s \in R \mid \varphi(s) = 0\}. \tag{11.3.11}$$

This is the same as the kernel obtained when one regards φ as a homomorphism of additive groups $R^+ \to R'^+$. So what we have learned about kernels of group homomorphisms applies. For instance, φ is injective if and only if $\ker \varphi = \{0\}$.

As you will recall, the kernel of a group homomorphism is not only a subgroup, it is a normal subgroup. Similarly, the kernel of a ring homomorphism is closed under the operation of addition, and it has a property that is stronger than closure under multiplication:

(11.3.12) If s is in $\ker \varphi$, then for every element r of R, rs is in $\ker \varphi$.

For, if $\varphi(s) = 0$, then $\varphi(rs) = \varphi(r)\varphi(s) = \varphi(r)0 = 0$.

This property is abstracted in the concept of an ideal.

Definition 11.3.13 An *ideal* I of a ring R is a nonempty subset of R with these properties:

- I is closed under addition, and
- If s is in I and r is in R, then rs is in I.

The kernel of a ring homomorphism is an ideal.

The peculiar term "ideal" is an abbreviation of the phrase "ideal element" that was formerly used in number theory. We will see in Chapter 13 how it arose. A good way, probably a better way, to think of the definition of an ideal is this equivalent formulation:

(11.3.14) I is not empty, and a linear combination $r_1 s_1 + \cdots + r_k s_k$ of elements s_i of I with coefficients r_i in R is in I.

• In any ring R, the multiples of a particular element a form an ideal called the *principal ideal* generated by a. An element b of R is in this ideal if and only if b is a multiple of a, which is to say, if and only if a divides b in R.

There are several notations for this principal ideal:

$$(a) = aR = Ra = \{ra \mid r \in R\}. \tag{11.3.15}$$

The ring R itself is the principal ideal (1), and because of this it is called the *unit ideal*. It is the only ideal that contains a unit of the ring. The set consisting of zero alone is the principal ideal (0), and is called the *zero ideal*. An ideal I is *proper* if it is neither the zero ideal nor the unit ideal.

Every ideal I satisfies the requirements for a subring, except that the unit element 1 of R will not be in I unless I is the whole ring. Unless I is equal to R, it will not be what we call a subring.

Examples 11.3.16

(a) Let φ be the homomorphism $\mathbb{R}[x] \to \mathbb{R}$ defined by substituting the real number 2 for x. Its kernel, the set of polynomials that have 2 as a root, can be described as the set of polynomials divisible by $x-2$. This is a principal ideal that might be denoted by $(x-2)$.

(b) Let $\Phi : \mathbb{R}[x, y] \to \mathbb{R}[t]$ be the homomorphism that is the identity on the real numbers, and that sends $x \rightsquigarrow t^2$, $y \rightsquigarrow t^3$. Then it sends $g(x, y) \rightsquigarrow g(t^2, t^3)$. The polynomial $f(x, y) = y^2 - x^3$ is in the kernel of Φ. We'll show that the kernel is the principal ideal (f) generated by f, i.e., that if $g(x, y)$ is a polynomial and if $g(t^2, t^3) = 0$, then f divides g. To show this, we regard f as a polynomial in y whose coefficients are polynomials in x (see (11.3.8)). It is a monic polynomial in y, so we can do division with remainder: $g = fq + r$, where q and r are polynomials, and where the remainder r, if not zero, has degree at most 1 in y. We write the remainder as a polynomial in y: $r(x, y) = r_1(x)y + r_0(x)$. If $g(t^2, t^3) = 0$, then both g and fq are in the kernel of Φ, so r is too: $r(t^2, t^3) = r_1(t^2)t^3 + r_0(t^2) = 0$. The monomials that appear in $r_0(t^2)$ have even degree, while those in $r_1(t^2)t^3$ have odd degree. Therefore, in order for $r(t^2, t^3)$ to be zero, $r_0(x)$ and $r_1(x)$ must both be zero. Since the remainder is zero, f divides g. □

The notation (a) for a principal ideal is convenient, but it is ambiguous because the ring isn't mentioned. For instance, $(x-2)$ could stand for an ideal of $\mathbb{R}[x]$ or of $\mathbb{Z}[x]$, depending on the circumstances. When several rings are being discussed, a different notation may be preferable.

• The ideal *I generated by a set of elements* $\{a_1, \ldots, a_n\}$ of a ring R is the smallest ideal that contains those elements. It can be described as the set of all linear combinations

$$r_1a_1 + \cdots + r_na_n \tag{11.3.17}$$

with coefficients r_i in the ring. This ideal is often denoted by $(a_1, \ldots, a_n)$:

$$(a_1, \ldots, a_n) = \{r_1a_1 + \cdots + r_na_n \mid r_i \in R\}. \tag{11.3.18}$$

For instance, the kernel K of the homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{F}_p$ that sends $f(x)$ to the residue of $f(0)$ modulo p is the ideal (p, x) of $\mathbb{Z}[x]$ generated by p and x. Let's check this. First, p and x are in the kernel, so $(p, x) \subset K$. To show that $K \subset (p, x)$, we let $f(x) = a_nx^n + \cdots + a_1x + a_0$ be an integer polynomial. Then $f(0) = a_0$. If $a_0 \equiv 0$ modulo p, say $a_0 = bp$, then f is the linear combination $bp + (a_nx^{n-1} + \cdots + a_1)x$ of p and x. So f is in the ideal (p, x).

The number of elements required to generate an ideal can be arbitrarily large. The ideal (x^3, x^2y, xy^2, y^3) of the polynomial ring $\mathbb{C}[x, y]$ consists of the polynomials in which every term has degree at least 3. It cannot be generated by fewer than four elements.

In the rest of this section, we describe ideals in some simple cases.

Proposition 11.3.19

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

(b) A ring that has exactly two ideals is a field.

Proof. If an ideal I of a field F contains a nonzero element a, that element is invertible. Then I contains $a^{-1}a = 1$, and is the unit ideal. The only ideals of F are (0) and (1).

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 of R has a multiplicative inverse. We have seen that $1 = 0$ happens only in the zero ring. The zero ring has only one ideal, the zero 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.

To show that every nonzero element a of R has an inverse, we consider the principal ideal (a). It is not the zero ideal because it contains the element a. Therefore it is the unit ideal. The elements of (a) are the multiples of a, so 1 is a multiple of a, and therefore a is invertible. □

Corollary 11.3.20 Every homomorphism $\varphi: F \to R$ from a field F to a nonzero ring R is injective.

Proof. The kernel of φ is an ideal of F. So according to Proposition 11.3.19, the kernel is either (0) or (1). If $\ker \varphi$ were the unit ideal (1), φ would be the zero map. But the zero map isn't a homomorphism when R isn't the zero ring. Therefore $\ker \varphi = (0)$, and φ is injective. □

Proposition 11.3.21 The ideals in the ring of integers are the subgroups of $\mathbb{Z}^+$, and they are principal ideals.

An ideal of the ring $\mathbb{Z}$ of integers will be a subgroup of the additive group $\mathbb{Z}^+$. It was proved before (2.3.3) that every subgroup of $\mathbb{Z}^+$ has the form $\mathbb{Z}n$. □

The proof that subgroups of $\mathbb{Z}^+$ have the form $\mathbb{Z}n$ can be adapted to the polynomial ring $F[x]$.

Proposition 11.3.22 Every ideal in the ring $F[x]$ of polynomials in one variable x over a field F is a principal ideal. A nonzero ideal I in $F[x]$ is generated by the unique monic polynomial of lowest degree that it contains.

Proof. Let I be an ideal of $F[x]$. The zero ideal is principal, so we may assume that I is not the zero ideal. The first step in finding a generator for a nonzero subgroup of $\mathbb{Z}$ is to choose its smallest positive element. The substitute here is to choose a nonzero polynomial f in I of minimal degree. Since F is a field, we may choose f to be monic. We claim that I is the principal ideal (f) of polynomial multiples of f. Since f is in I, every multiple of f is in I, so $(f) \subset I$. To prove that $I \subset (f)$, we choose an element g of I, and we use division with remainder to write $g = fq + r$, where r, if not zero, has lower degree than f. Since g and f are in I, $g - fq = r$ is in I too. Since f has minimal degree among nonzero elements of I, the only possibility is that $r = 0$. Therefore f divides g, and g is in (f).

If f_1 and f_2 are two monic polynomials of lowest degree in I, their difference is in I and has lower degree than n, so it must be zero. Therefore the monic polynomial of lowest degree is unique. □

Example 11.3.23 Let $\gamma = \sqrt[3]{2}$ be the real cube root of 2, and let $\Phi : \mathbb{Q}[x] \to \mathbb{C}$ be the substitution map that sends $x \rightsquigarrow \gamma$. The kernel of this map is a principal ideal, generated by the monic polynomial of lowest degree in $\mathbb{Q}[x]$ that has γ as a root (11.3.22). The polynomial $x^3 - 2$ is in the kernel, and because $\sqrt[3]{2}$ is not a rational number, it is not the product $f = gh$ of two nonconstant polynomials with rational coefficients. So it is the lowest degree polynomial in the kernel, and therefore it generates the kernel.

We restrict the map Φ to the integer polynomial ring $\mathbb{Z}[x]$, obtaining a homomorphism $\Phi' : \mathbb{Z}[x] \to \mathbb{C}$. The next lemma shows that the kernel of Φ' is the principal ideal of $\mathbb{Z}[x]$ generated by the same polynomial f.

Lemma 11.3.24 Let f be a monic integer polynomial, and let g be another integer polynomial. If f divides g in $\mathbb{Q}[x]$, then f divides g in $\mathbb{Z}[x]$.

Proof. Since f is monic, we can do division with remainder in $\mathbb{Z}[x]$: $g = fq + r$. This equation remains true in the ring $\mathbb{Q}[x]$, and division with remainder in $\mathbb{Q}[x]$ gives the same result. In $\mathbb{Q}[x]$, f divides g. Therefore $r = 0$, and f divides g in $\mathbb{Z}[x]$. □

The proof of the following corollary is similar to the proof of existence of the greatest common divisor in the ring of integers ((2.3.5), see also (12.2.8)).

Corollary 11.3.25 Let R denote the polynomial ring $F[x]$ in one variable over a field F, and let f and g be elements of R, not both zero. Their *greatest common divisor* $d(x)$ is the unique monic polynomial that generates the ideal (f, g). It has these properties:

(a) $Rd = Rf + Rg$.

(b) d divides f and g.

(c) If a polynomial $e = e(x)$ divides both f and g, it also divides d.

(d) There are polynomials p and q such that $d = pf + qg$. □

The definition of the *characteristic* of a ring R is the same as for a field. It is the non-negative integer n that generates the kernel of the homomorphism $\varphi : \mathbb{Z} \to R$ (11.3.10). If $n = 0$, the characteristic is zero, and this means that no positive multiple of 1 in R is equal to zero. Otherwise n is the smallest positive integer such that "n times 1" is zero in R. The characteristic of a ring can be any non-negative integer.

11.4 QUOTIENT RINGS

Let I be an ideal of a ring R. The cosets of the additive subgroup I^+ of R^+ are the subsets $a + I$. It follows from what has been proved for groups that the set of cosets $\overline{R} = R/I$ is a group under addition. It is also a ring:

Theorem 11.4.1 Let I be an ideal of a ring R. There is a unique ring structure on the set $\overline{R}$ of additive cosets of I such that the map $\pi: R \to \overline{R}$ that sends $a \rightsquigarrow \bar{a} = [a + I]$ is a ring homomorphism. The kernel of π is the ideal I.

As with quotient groups, the map π is referred to as the *canonical map*, and $\overline{R}$ is called the *quotient ring*. The image $\bar{a}$ of an element a is called the *residue* of the element.

Proof. This proof has already been carried out for the ring of integers (Section 2.9). We want to put a ring structure on $\overline{R}$, and if we forget about multiplication and consider only the addition law, I becomes a normal subgroup of R^+, for which the proof has been given (2.12.2). What is left to do is to define multiplication, to verify the ring axioms, and to prove that π is a homomorphism. Let $\bar{a} = [a + I]$ and $\bar{b} = [b + I]$ be elements of $\overline{R}$. We would like to define the product by the setting $\bar{a}\bar{b} = [ab + I]$. The set of products

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

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

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

Since I is an ideal that contains u and v, it contains $av + bu + uv$. This is all that is needed to define the product coset: It is the coset that contains the set of products. That coset is unique because the cosets partition R.

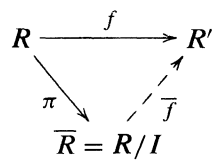
The proofs of the remaining assertions follow the patterns set in Section 2.9. □

As with groups, one often drops the bars over the letters that represent elements of a quotient ring $\overline{R}$, remembering that "$a = b$ in $\overline{R}$" means $\bar{a} = \bar{b}$.

The next theorems are analogous to ones that we have seen for groups:

Theorem 11.4.2 Mapping Property of Quotient Rings. Let $f: R \to R'$ be a ring homomorphism with kernel K and let I be another ideal. Let $\pi: R \to \overline{R}$ be the canonical map from R to $\overline{R} = R/I$.

(a) If $I \subset K$, there is a unique homomorphism $\overline{f}: \overline{R} \to R'$ such that $\overline{f}\pi = f$:



(b) *(First Isomorphism Theorem)* If f is surjective and $I = K$, $\overline{f}$ is an isomorphism. □

The First Isomorphism Theorem is our fundamental method of identifying quotient rings. However, it doesn't apply very often. Quotient rings will be new rings in most cases, and this is one reason that the quotient construction is important. The ring $\mathbb{C}[x, y]/(y^2 - x^3 + 1)$, for example, is completely different from any ring we have seen up to now. Its elements are functions on an elliptic curve (see [Silverman]).

The Correspondence Theorem for rings describes the fundamental relationship between ideals in a ring and a quotient ring.

Theorem 11.4.3 Correspondence Theorem. Let $\varphi: R \to \mathcal{R}$ be a *surjective* ring homomorphism with kernel K. There is a bijective correspondence between the set of all ideals of $\mathcal{R}$ and the set of ideals of R that contain K:

$$\{\text{ideals of } R \text{ that contain } K\} \longleftrightarrow \{\text{ideals of } \mathcal{R}\}.$$

This correspondence is defined as follows:

- If I is a ideal of R and if $K \subset I$, the corresponding ideal of $\mathcal{R}$ is $\varphi(I)$.
- If $\mathcal{I}$ is a ideal of $\mathcal{R}$, the corresponding ideal of R is $\varphi^{-1}(\mathcal{I})$.

If the ideal I of R corresponds to the ideal $\mathcal{I}$ of $\mathcal{R}$, the quotient rings R/I and $\mathcal{R}/\mathcal{I}$ are naturally isomorphic.

Note that the inclusion $K \subset I$ is the reverse of the one in the mapping property.

Proof of the Correspondence Theorem. We let $\mathcal{I}$ be an ideal of $\mathcal{R}$ and we let I be an ideal of R that contains K. We must check the following points:

- $\varphi(I)$ is an ideal of $\mathcal{R}$.
- $\varphi^{-1}(\mathcal{I})$ is an ideal of R, and it contains K.
- $\varphi(\varphi^{-1}(\mathcal{I})) = \mathcal{I}$, and $\varphi^{-1}(\varphi(I)) = I$.
- If $\varphi(I) = \mathcal{I}$, then $R/I \approx \mathcal{R}/\mathcal{I}$.

We go through these points in order, referring to the proof of the Correspondence Theorem 2.10.5 for groups when it applies. We have seen before that the image of a subgroup is a subgroup. So to show that $\varphi(I)$ is an ideal of $\mathcal{R}$, we need only prove that it is closed under multiplication by elements of $\mathcal{R}$. Let $\tilde{r}$ be in $\mathcal{R}$ and let $\tilde{x}$ be in $\varphi(I)$. Then $\tilde{x} = \varphi(x)$ for some x in I, and because φ is surjective, $\tilde{r} = \varphi(r)$ for some r in R. Since I is an ideal, rx is in I, and $\tilde{r}\tilde{x} = \varphi(rx)$, so $\tilde{r}\tilde{x}$ is in $\varphi(I)$.

Next, we verify that $\varphi^{-1}(\mathcal{I})$ is an ideal of R that contains K. This is true whether or not φ is surjective. Let's write $\varphi(a) = \tilde{a}$. By definition of the inverse image, a is in $\varphi^{-1}(\mathcal{I})$ if and only if $\tilde{a}$ is in $\mathcal{I}$. If a is in $\varphi^{-1}(\mathcal{I})$ and r is in R, then $\varphi(ra) = \tilde{r}\tilde{a}$ is in $\mathcal{I}$ because $\mathcal{I}$ is an ideal, and hence ra is in $\varphi^{-1}(\mathcal{I})$. The facts that $\varphi^{-1}(\mathcal{I})$ is closed under sums and that it contains K were shown in (2.10.4).

The third assertion, the bijectivity of the correspondence, follows from the case of a group homomorphism.

Finally, suppose that an ideal I of R that contains K corresponds to an ideal $\mathcal{I}$ of $\mathcal{R}$, that is, $\mathcal{I} = \varphi(I)$ and $I = \varphi^{-1}(\mathcal{I})$. Let $\tilde{\pi}: \mathcal{R} \to \mathcal{R}/\mathcal{I}$ be the canonical map, and let f denote the composed map $\tilde{\pi}\varphi: R \to \mathcal{R} \to \mathcal{R}/\mathcal{I}$. The kernel of f is the set of elements x in R such that $\tilde{\pi}\varphi(x) = 0$, which translates to $\varphi(x) \in \mathcal{I}$, or to $x \in \varphi^{-1}(\mathcal{I}) = I$. The kernel of f is I. The mapping property, applied to the map f, gives us a homomorphism $\overline{f}: R/I \to \mathcal{R}/\mathcal{I}$, and the First Isomorphism Theorem asserts that $\overline{f}$ is an isomorphism. □

To apply the Correspondence Theorem, it helps to know the ideals of one of the rings. The next examples illustrate this in very simple situations, in which one of the two rings is $\mathbb{C}[t]$. We will be able to use the fact that every ideal of $\mathbb{C}[t]$ is principal (11.3.22).

Example 11.4.4 **(a)** Let φ:$\mathbb{C}[x, y] \to \mathbb{C}[t]$ be the homomorphism that sends $x \rightsquigarrow t$ and $y \rightsquigarrow t^2$. This is a surjective map, and its kernel K is the principal ideal of $\mathbb{C}[x, y]$ generated by $y - x^2$. (The proof of this is similar to the one given in Example 11.3.16.)

The Correspondence Theorem relates ideals I of $\mathbb{C}[x, y]$ that contain $y - x^2$ to ideals J of $\mathbb{C}[t]$, by $J = \varphi(I)$ and $I = \varphi^{-1}(J)$. Here J will be a principal ideal, generated by a polynomial $p(t)$. Let I_1 denote the ideal of $\mathbb{C}[x, y]$ generated by $y - x^2$ and $p(x)$. Then I_1 contains K, and its image is equal to J. The Correspondence Theorem asserts that $I_1 = I$. Every ideal of the polynomial ring $\mathbb{C}[x, y]$ that contains $y - x^2$ has the form $I = (y - x^2, p(x))$, for some polynomial $p(x)$.

(b) We identify the ideals of the quotient ring $R' = \mathbb{C}[t]/(t^2 - 1)$ using the canonical homomorphism $\pi : \mathbb{C}[t] \to R'$. The kernel of π is the principal ideal $(t^2 - 1)$. Let I be an ideal of $\mathbb{C}[t]$ that contains $t^2 - 1$. Then I is principal, generated by a monic polynomial f, and the fact that $t^2 - 1$ is in I means that f divides $t^2 - 1$. The monic divisors of $t^2 - 1$ are: $1, t - 1, t + 1$ and $t^2 - 1$. Therefore the ring R' contains exactly four ideals. They are the principal ideals generated by the residues of the divisors of $t^2 - 1$. □

Adding Relations

We reinterpret the quotient ring construction when the ideal I is principal, say $I = (a)$. In this situation, we think of $\overline{R} = R/I$ as the ring obtained by imposing the relation $a = 0$ on R, or of killing the element a. For instance, the field $\mathbb{F}_7$ will be thought of as the ring obtained by killing 7 in the ring $\mathbb{Z}$ of integers.

Let's examine the collapsing that takes place in the map $\pi: R \to \overline{R}$. Its kernel is the ideal I, so a is in the kernel: $\pi(a) = 0$. If b is any element of R, the elements that have the same image in $\overline{R}$ as b are those in the coset $b + I$, and since $I = (a)$ those elements have the form $b + ra$. We see that imposing the relation $a = 0$ in the ring R forces us also to set $b = b + ra$ for all b and r in R, and that these are the only consequences of killing a.

Any number of relations $a_1 = 0, \ldots, a_n = 0$ can be introduced, by working modulo the ideal I generated by $a_1, \ldots, a_n$, the set of linear combinations $r_1a_1 + \cdots + r_na_n$, with coefficients r_i in R. The quotient ring $\overline{R} = R/I$ is viewed as the ring obtained by killing the n elements. Two elements b and b' of R have the same image in $\overline{R}$ if and only if b' has the form $b + r_1a_1 + \cdots + r_na_n$ for some r_i in R.

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

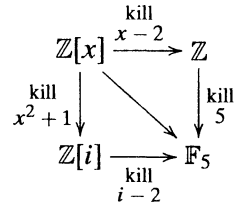
Here the Correspondence Theorem asserts something that is intuitively clear: Introducing relations one at a time or all together leads to isomorphic results. To spell this out, let a and b be elements of a ring R, and let $\overline{R} = R/(a)$ be the result of killing a in R. Let $\overline{b}$ be the residue of b in $\overline{R}$. The Correspondence Theorem tells us that the principal ideal $(\overline{b})$ of $\overline{R}$ corresponds to the ideal (a, b) of R, and that $R/(a, b)$ is isomorphic to $\overline{R}/(\overline{b})$. Killing a and b in R at the same time gives the same result as killing $\overline{b}$ in the ring $\overline{R}$ that is obtained by killing a first.

Example 11.4.5 We ask to identify the quotient ring $\overline{R} = \mathbb{Z}[i]/(i-2)$, the ring obtained from the Gauss integers by introducing the relation $i - 2 = 0$. Instead of analyzing this directly, we note that the kernel of the map $\mathbb{Z}[x] \to \mathbb{Z}[i]$ sending $x \rightsquigarrow i$ is the principal ideal of $\mathbb{Z}[x]$ generated by $f = x^2 + 1$. The First Isomorphism Theorem tells us that $\mathbb{Z}[x]/(f) \approx \mathbb{Z}[i]$. The image of $g = x - 2$ is $i - 2$, so $\overline{R}$ can also be obtained by introducing the two relations $f = 0$ and $g = 0$ into the integer polynomial ring. Let $I = (f, g)$ be the ideal of $\mathbb{Z}[x]$ generated by the two polynomials f and g. Then $\overline{R} \approx \mathbb{Z}[x]/I$.

To form $\overline{R}$, we may introduce the two relations in the opposite order, first killing g, then f. The principal ideal (g) of $\mathbb{Z}[x]$ is the kernel of the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ that sends $x \rightsquigarrow 2$. So when we kill $x - 2$ in $\mathbb{Z}[x]$, we obtain a ring isomorphic to $\mathbb{Z}$, in which the residue of x is 2. Then the residue of $f = x^2 + 1$ becomes 5. So we can also obtain $\overline{R}$ by killing 5 in $\mathbb{Z}$, and therefore $\overline{R} \approx \mathbb{F}_5$.

The rings we have mentioned are summed up in this diagram:

(11.4.6)



□

11.5 ADJOINING ELEMENTS

In this section we discuss a procedure closely related to that of adding relations: adjoining new elements to a ring. Our model for this procedure is the construction of the complex number field from the real numbers. That construction is completely formal: The complex number i has no properties other than its defining property: $i^2 = -1$. We will now describe the general principle behind this construction. We start with an arbitrary ring R, and consider the problem of building a bigger ring containing the elements of R and also a new element, which we denote by α. We will probably want α to satisfy some relation such as $\alpha^2 + 1 = 0$. A ring that contains another ring as a subring is called a *ring extension*. 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, the smallest subring containing R and α. The subring is denoted by $R[\alpha]$. We described this ring in Section 11.1 in the case $R = \mathbb{Z}$, and the description is no different in general: $R[\alpha]$ consists of the elements β of R' that have polynomial expressions

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

with coefficients r_i in R.

But as happens when we construct $\mathbb{C}$ from $\mathbb{R}$, we may not yet have an extension containing α. Then we must construct the extension abstractly. We start with the polynomial ring $R[x]$. It is generated by R and x. The element x of satisfies no relations other than those implied by the ring axioms, and we will probably want our new element α to satisfy some relations. But now that we have the ring $R[x]$ in hand, we can add relations to it using the

procedure explained in the previous section *on the polynomial ring* $R[x]$. The fact that R is replaced by $R[x]$ complicates the notation, but aside from this, nothing is different.

For example, we construct the complex numbers by introducing the relation $x^2+1=0$ into the ring $P=\mathbb{R}[x]$ of real polynomials. We form the quotient ring $\overline{P}=P/(x^2+1)$, and the residue of x becomes our element i. The relation $\bar{x}^2+1=0$ holds in $\overline{P}$ because the map $\pi: P \to \overline{P}$ is a homomorphism and because x^2+1 is in its kernel. So $\overline{P}$ is isomorphic to $\mathbb{C}$.

In general, say that we want to adjoin an element α to a ring R, and that we want α to satisfy the polynomial relation $f(x)=0$, where

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, \quad \text{with } a_i \text{ in } R. \tag{11.5.1}$$

The solution is $R'=R[x]/(f)$, where (f) is the principal ideal of $R[x]$ generated by f.

We let α denote the residue $\bar{x}$ of x in R'. Then because the map $\pi: R[x] \to R[x]/(f)$ is a homomorphism,

$$\pi(f(x))=\overline{f(x)}=\bar{a}_n\alpha^n+\cdots+\bar{a}_0=0. \tag{11.5.2}$$

Here $\bar{a}_i$ is the image in R' of the constant polynomial a_i. So, dropping bars, α satisfies the relation $f(\alpha)=0$. The ring obtained in this way may be denoted by $R[\alpha]$ too.

An example: Let a be an element of a ring R. An inverse of a is an element α that satisfies the relation

$$a\alpha-1=0. \tag{11.5.3}$$

So we can adjoin an inverse by forming the quotient ring $R'=R[x]/(ax-1)$.

The most important case is that our element α is a root of a monic polynomial:

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, \quad \text{with } a_i \text{ in } R. \tag{11.5.4}$$

We can describe the ring $R[\alpha]$ precisely in this case.

Proposition 11.5.5 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 $R[x]/(f)$ obtained by adjoining an element satisfying the relation $f(\alpha)=0$.

(a) The set $(1, \alpha, \ldots, \alpha^{n-1})$ is a *basis* of $R[\alpha]$ over R: every element of $R[\alpha]$ can be written uniquely as a linear combination of this basis, with coefficients in R.

(b) Addition of two linear combinations is vector addition.

(c) Multiplication of linear combinations is as follows: Let β_1 and β_2 be elements of $R[\alpha]$, and let $g_1(x)$ and $g_2(x)$ be polynomials such that $\beta_1=g_1(\alpha)$ and $\beta_2=g_2(\alpha)$. One divides the product polynomial g_1g_2 by f, say $g_1g_2=fq+r$, where the remainder $r(x)$, if not zero, has degree $<n$. Then $\beta_1\beta_2=r(\alpha)$.

The next lemma should be clear.

Lemma 11.5.6 Let f be a *monic* polynomial of degree n in a polynomial ring $R[x]$. Every nonzero element of (f) has degree at least n. □

Proof of the proposition. **(a)** Since $R[\alpha]$ is a quotient of the polynomial ring $R[x]$, every element β of $R[\alpha]$ is the residue of a polynomial $g(x)$, i.e., $\beta = g(\alpha)$. Since f is monic, we can perform division with remainder: $g(x) = f(x)q(x) + r(x)$, where $r(x)$ is either zero or else has degree less than n (11.2.9). Then since $f(\alpha) = 0$, $\beta = g(\alpha) = r(\alpha)$. In this way, β is written as a combination of the basis. The expression for β is unique because the principal ideal (f) contains no element of degree $<n$. This also proves **(c)**, and **(b)** follows from the fact that addition in $R[x]$ is vector addition. □

Examples 11.5.7 **(a)** The kernel of the substitution map $\mathbb{Z}[x] \to \mathbb{C}$ that sends $x \rightsquigarrow \gamma = \sqrt[3]{2}$ is the principal ideal $(x^3 - 2)$ of $\mathbb{Z}[x]$ (11.3.23). So $\mathbb{Z}[\gamma]$ is isomorphic to $\mathbb{Z}[x]/(x^3 - 2)$. The proposition shows that $(1, \gamma, \gamma^2)$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[\gamma]$. Its elements are linear combinations $a_0 + a_1\gamma + a_2\gamma^2$, where a_i are integers. If $\beta_1 = (\gamma^2 - \gamma)$ and $\beta_2 = (\gamma^2 + 1)$, then

$$\beta_1\beta_2 = \gamma^4 - \gamma^3 + \gamma^2 - \gamma = f(\gamma)(\gamma - 1) + (\gamma^2 + \gamma - 2) = \gamma^2 + \gamma - 2.$$

(b) Let R' be obtained by adjoining an element δ to $\mathbb{F}_5$ with the relation $\delta^2 - 3 = 0$. Here δ becomes an abstract square root of 3. Proposition 11.5.5 tells us that the elements of R' are the 25 linear expressions $a + b\delta$ with coefficients a and b in $\mathbb{F}_5$.

We'll show that R' is a field of order 25 by showing that every nonzero element $a + b\delta$ of R' is invertible. To see this, consider the product $c = (a + b\delta)(a - b\delta) = (a^2 - 3b^2)$. This is is an element of $\mathbb{F}_5$, and because 3 isn't a square in $\mathbb{F}_5$, it isn't zero unless both a and b are zero. So if $a + b\delta \neq 0$, c is invertible in $\mathbb{F}_5$. Then the inverse of $a + b\delta$ is $(a - b\delta)c^{-1}$.

(c) The procedure used in **(b)** doesn't yield a field when it is applied to $\mathbb{F}_{11}$. The reason is that $\mathbb{F}_{11}$ already contains two square roots of 3, namely ± 5. If R' is the ring obtained by adjoining δ with the relation $\delta^2 - 3 = 0$, we are adjoining an abstract square root of 3, though $\mathbb{F}_{11}$ already contains two square roots. At first glance one might expect to get $\mathbb{F}_{11}$ back. We don't, because we haven't told δ to be equal to 5 or -5. We've told δ only that its square is 3. So $\delta - 5$ and $\delta + 5$ are not zero, but $(\delta + 5)(\delta - 5) = \delta^2 - 3 = 0$. This cannot happen in a field. □

It is harder to analyze the structure of the ring obtained by adjoining an element when the polynomial relation isn't monic.

• There is a point that we have suppressed in our discussion, and we consider it now: When we adjoin an element α to a ring R with some relation $f(\alpha) = 0$, will our original R be a subring of the ring R' that we construct? We know that R is contained in the polynomial ring $R[x]$, as the subring of constant polynomials, and we also have the canonical map $\pi : R[x] \to R' = R[x]/(f)$. Restricting π to the constant polynomials gives us a homomorphism $R \to R'$, let's call it ψ. Is ψ injective? If it isn't injective, we cannot identify R with a subring of R'.

The kernel of ψ is the set of constant polynomials in the ideal:

$$\ker \psi = R \cap (f). \tag{11.5.8}$$

It is fairly likely that $\ker\psi$ is zero because f will have positive degree. There will have to be a lot of cancellation to make a polynomial multiple of f have degree zero. The kernel

is zero when α is required to satisfy a monic polynomial relation. But it isn't always zero. For instance, let R be the ring $\mathbb{Z}/(6)$ of congruence classes modulo 6, and let f be the polynomial $2x + 1$ in $R[x]$. Then $3f = 3$. The kernel of the map $R \to R/(f)$ is not zero.

11.6 PRODUCT RINGS

The product $G \times G'$ of two groups was defined in Chapter 2. It is the product set, and the law of composition is componentwise: $(x, x')(y, y') = (xy, x'y')$. The analogous construction can be made with rings.

Proposition 11.6.1 Let R and R' be rings.

(a) The product set $R \times R'$ is a ring called the *product ring*, with component-wise addition and multiplication:

$$(x, x') + (y, y') = (x + y, x' + y') \quad \text{and} \quad (x, x')(y, y') = (xy, x'y'),$$

(b) The additive and multiplicative identities in $R \times R'$ are $(0, 0)$ and $(1, 1)$, respectively.

(c) The projections $\pi : R \times R' \to R$ and $\pi' : R \times R' \to R'$ defined by $\pi(x, x') = x$ and $\pi'(x, x') = x'$ are ring homomorphisms. The kernels of π and π' are the ideals $\{0\} \times R'$ and $R \times \{0\}$, respectively, of $R \times R'$.

(d) The kernel $R \times \{0\}$ of π' is a ring, with multiplicative identity $e = (1, 0)$. It is not a subring of $R \times R'$ unless R' is the zero ring. Similarly, $\{0\} \times R'$ is a ring with identity $e' = (0, 1)$. It is not a subring of $R \times R'$ unless R is the zero ring.

The proofs of these assertions are very elementary. We omit them, but see the next proposition for part **(d)**. □

To determine whether or not a given ring is isomorphic to a product ring, one looks for the elements that in a product ring would be $(1, 0)$ and $(0, 1)$. They are idempotent elements.

- An *idempotent* element e of a ring S is an element of S such that $e^2 = e$.

Proposition 11.6.2 Let e be an idempotent element of a ring S.

(a) The element $e' = 1 - e$ is also idempotent, $e + e' = 1$, and $ee' = 0$.

(b) With the laws of composition obtained by restriction from S, the principal ideal eS is a ring with identity element e, and multiplication by e defines a ring homomorphism $S \to eS$.

(c) The ideal eS is not a subring of S unless e is the unit element 1 of S and $e' = 0$.

(d) The ring S is isomorphic to the product ring $eS \times e'S$.

Proof. **(a)** $e'^2 = (1 - e)^2 = 1 - 2e + e = e'$, and $ee' = e(1 - e) = e - e = 0$.

(b) Every ideal I of a ring S has the properties of a ring except for the existence of a multiplicative identity. In this case, e is an identity element for eS, because if a is in eS, say $a = es$, then $ea = e^2s = es = a$. The ring axioms show that multiplication by e is a homomorphism: $e(a + b) = ea + eb$, $e(ab) = e^2ab = (ea)(eb)$, and $e1 = e$.

(c) To be a subring of S, eS must contain the identity 1 of S. If it does, then e and 1 will both be identity elements of eS, and since the identity in a ring is unique, $e = 1$ and $e' = 0$.

(d) The rule $\varphi(x) = (ex, e'x)$ defines a homomorphism $\varphi: S \to eS \times e'S$, because both of the maps $x \rightsquigarrow ex$ and $x \rightsquigarrow e'x$ are homomorphisms and the laws of compostition in the product ring are componentwise. We verify that this homomorphism is bijective. First, if $\varphi(x) = (0, 0)$, then $ex = 0$ and $e'x = 0$. If so, then $x = (e + e')x = ex + e'x = 0$ too. This shows that φ is injective. To show that φ is surjective, let (u, v) be an element of $eS \times e'S$, say $u = ex$ and $v = e'y$. Then $\varphi(u + v) = (e(ex + e'y), e'(ex + e'y)) = (u, v)$. So (u, v) is in the image, and therefore φ is surjective. □

Examples 11.6.3 **(a)** We go back to the ring R' obtained by adjoining an abstract square root of 3 to $\mathbb{F}_{11}$. Its elements are the 11^2 linear combinations $a + b\delta$, with a and b in $\mathbb{F}_{11}$ and $\delta^2 = 3$. We saw in (11.5.7)**(c)** that this ring is not a field, the reason being that $\mathbb{F}_{11}$ already contains two square roots ± 5 of 3. The elements $e = \delta - 5$ and $e' = -\delta - 5$ are idempotents in R', and $e + e' = 1$. Therefore R' is isomorphic to the product $eR' \times e'R'$. Since the order of R' is 11^2, $|eR'| = |e'R'| = 11$. The rings eR' and $e'R'$ are both isomorphic to $\mathbb{F}_{11}$, and R' is isomorphic to the product ring $\mathbb{F}_{11} \times \mathbb{F}_{11}$.

(b) We define a homomorphism $\varphi: \mathbb{C}[x, y] \to \mathbb{C}[x] \times \mathbb{C}[y]$ from the polynomial ring in two variables to the product ring by $\varphi(f(x, y)) = (f(x, 0), f(0, y))$. Its kernel is the set of polynomials $f(x, y)$ divisible both by y and by x, which is the principal ideal of $\mathbb{C}[x, y]$ generated by xy. The map isn't quite surjective. Its image is the subring of the product consisting of pairs $(p(x), q(y))$ of polynomials with the same constant term. So the quotient $\mathbb{C}[x, y]/(xy)$ is isomorphic to that subring. □

11.7 FRACTIONS

In this section we consider the use of fractions in rings other than the integers. For instance, a fraction p/q of polynomials p and q, with q not zero, is called a *rational function*.

Let's review the arithmetic of integer fractions. In order to apply the statements below to other rings, we denote the ring of integers by the neutral symbol R.

- A *fraction* is a symbol a/b, or $\frac{a}{b}$, where a and b are elements of R and b is not zero.
- Elements of R are viewed as fractions by the rule $a = a/1$.
- Two fractions a_1/b_1 and a_2/b_2 are equivalent, $a_1/b_1 \approx a_2/b_2$, if the elements of R that are obtained by "cross multiplying" are equal, i.e., if $a_1b_2 = a_2b_1$.
- Sums and products of fractions are given by $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$, and $\dfrac{a}{b}\dfrac{c}{d} = \dfrac{ac}{bd}$.

We use the term "equivalent" in the third item because, strictly speaking, the fractions aren't actually *equal*.

A problem arises when one replaces the integers by an arbitrary ring R: In the definition of addition, the denominator of the sum is the product bd. Since denominators aren't allowed to be zero, bd had better not be zero. Since b and d are denominators, they aren't zero individually, but we need to know that the product of nonzero elements of R is nonzero. This turns out to be the only problem, but it isn't always true. For example, in the

ring $\mathbb{Z}/(6)$ of congruence classes modulo 6, the classes 2 and 3 are not zero, but $2 \cdot 3 = 0$. Or, in a product $R \times R'$ of nonzero rings, the idempotents $(1, 0)$ and $(0, 1)$ are nonzero elements whose product is zero. One cannot work with fractions in those rings.

• An *integral domain* R, or just a *domain* for short, is a ring with this property: R is not the zero ring, and if a and b are elements of R whose product ab is zero, then $a = 0$ or $b = 0$.

Any subring of a field is a domain, and if R is a domain, the polynomial ring $R[x]$ is also a domain.

An element a of a ring is called a *zero divisor* if it is nonzero, and if there is another nonzero element b such that $ab = 0$. An integral domain is a nonzero ring which contains no zero divisors.

An integral domain R satisfies the *cancellation law*:

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

For, from $ab = ac$ it follows that $a(b - c) = 0$. Then since $a \neq 0$ and since R is a domain, $b - c = 0$. □

Theorem 11.7.2 Let F be the set of equivalence classes of fractions of elements of an integral domain R.

(a) With the laws defined as above, F is a field, called the *fraction field* of R.

(b) R embeds as a subring of F by the rule $a \rightsquigarrow a/1$.

(c) *Mapping Property:* If R is embedded as a subring of another field $\mathcal{F}$, the rule $a/b = ab^{-1}$ embeds F into $\mathcal{F}$ too.

The phrase "mapping property" is explained as follows: To write the property carefully, one should imagine that the embedding of R into $\mathcal{F}$ is given by an injective ring homomorphism $\varphi: R \to \mathcal{F}$. The assertion is then that the rule $\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$ extends φ to an injective homomorphism $\Phi: F \to \mathcal{F}$.

The proof of Theorem 11.7.2 has many parts. One must verify that what we call equivalence of fractions is indeed an equivalence relation, that addition and multiplication are well-defined on equivalence classes, that the axioms for a field hold, and that sending $a \rightsquigarrow a/1$ is an injective homomorphism $R \to F$. Then one must check the mapping property. All of these verifications are straightfoward.

If we were the first people who wished to use fractions in a ring, we'd be nervous and would want to go carefully through each of the verifications. But they have been made many times. It seems sufficient to check a few of them to get a sense of what is involved.

Let us check that equivalence of fractions is a transitive relation. 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 $a_2b_3 = a_3b_2$. We multiply by b_3 and b_1:

$$a_1b_2b_3 = a_2b_1b_3 \quad \text{and} \quad a_2b_3b_1 = a_3b_2b_1.$$

Therefore $a_1b_2b_3 = a_3b_2b_1$. Cancelling b_2, $a_3b_1 = a_1b_3$. Thus $a_1/b_1 \approx a_3/b_3$. Since we used the cancellation law, the fact that R is a domain is essential here.

Next, we show that addition of fractions is well-defined. Suppose that $a/b \approx a'/b'$ and $c/d \approx c'/d'$. We must show that $a/b + c/d \approx a'/b' + c'/d'$, and to do that, we cross

multiply the expressions for the sums. We must show that $u = (ad + bc)(b'd')$ is equal to $v = (a'd' + b'c')(bd)$. The relations $ab' = a'b$ and $cd' = c'd$ show that

$$u = adb'd' + bcb'd' = a'dbd' + bc'b'd = v.$$

Verification of the mapping property is routine too. The only thing worth remarking is that, if R is contained in $\mathcal{F}$ and if a/b is a fraction, then $b \neq 0$, so the rule $a/b = ab^{-1}$ makes sense.

As mentioned above, a fraction of polynomials is called a *rational function*, and the fraction field of the polynomial ring $K[x]$, where K is a field, is called the *field of rational functions* in x, with coefficients in K. This field is usually denoted by $K(x)$:

$$K(x) = \left\{ \begin{array}{l} \text{equivalence classes of fractions } f/g, \text{ where } f \text{ and } g \\ \text{are polynomials, and } g \text{ is not the zero polynomial} \end{array} \right\}. \tag{11.7.3}$$

The rational functions we define here are equivalence classes of fractions of the formal polynomials that were defined in Section 11.2. If $K = \mathbb{R}$, 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 the formally defined rational functions, which are fractions of formal polynomials, from the functions that they define.

11.8 MAXIMAL IDEALS

In this section we investigate the kernels of *surjective* homomorphisms

$$\varphi: R \to F \tag{11.8.1}$$

from a ring R to a field F.

Let φ be such a map. The field F has just two ideals, the zero ideal (0) and the unit ideal (1) (11.3.19). The inverse image of the zero ideal is the kernel I of φ, and the inverse image of the unit ideal is the unit ideal of R. The Correspondence Theorem tells us that the only ideals of R that contain I are I and R. Because of this, I is called a maximal ideal.

- A *maximal ideal* M of a ring R is an ideal that isn't equal to R, and that isn't contained in any ideal other than M and R: If an ideal I contains M, then $I = M$ or $I = R$.

Proposition 11.8.2

(a) Let $\varphi : R \to R'$ be a surjective ring homomorphism, with kernel I. The image R' is a field if and only if I is a maximal ideal.

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

(c) The zero ideal of a ring R is maximal if and only if R is a field.

Proof. **(a)** A ring is a field if it contains precisely two ideals (11.3.19), so the Correspondence Theorem asserts that the image of φ is a field if and only if there are two precisely ideals that contain its kernel I. This will be true if and only if I is a maximal ideal.

Parts **(b)** and **(c)** follow when **(a)** is applied to the canonical map $R \to R/I$. □

Proposition 11.8.3 The maximal ideals of the ring $\mathbb{Z}$ of integers are the principal ideals generated by prime integers. □

Proof. Every ideal of $\mathbb{Z}$ is principal. Consider a principal ideal (n), with $n \geq 0$. If n is a prime, say $n = p$, then $\mathbb{Z}/(n) = \mathbb{F}_p$, a field. The ideal (n) is maximal. If n is not prime, there are three possibilities: $n = 0$, $n = 1$, or n factors. Neither the zero ideal nor the unit ideal is maximal. If n factors, say $n = ab$, with $1 < a < n$, then $1 \notin (a)$, $a \notin (n)$, and $n \in (a)$. Therefore $(n) < (a) < (1)$. The ideal (n) is not maximal. □

• A polynomial with coefficients in a field is called *irreducible* if it is not constant and if is not the product of two polynomials, neither of which is a constant.

Proposition 11.8.4

(a) Let F be a field. The maximal ideals of $F[x]$ are the principal ideals generated by the monic irreducible polynomials.

(b) Let $\varphi: F[x] \to R'$ be a homomorphism to an integral domain R', and let P be the kernel of φ. Either P is a maximal ideal, or $P = (0)$.

The proof of part **(a)** is analogous to the proof just given. We omit the proof of **(b)**. □

Corollary 11.8.5 There is a bijective correspondence between maximal ideals of the polynomial ring $\mathbb{C}[x]$ in one variable and points in the complex plane. The maximal ideal M_a that corresponds to a point a of $\mathbb{C}$ is the kernel of the substitution homomorphism $s_a: \mathbb{C}[x] \to \mathbb{C}$ that sends $x \rightsquigarrow a$. It is the principal ideal generated by the linear polynomial $x - a$.

Proof. The kernel M_a of the substitution homomorphism s_a consists of the polynomials that have a as a root, which are those divisible by $x - a$. So $M_a = (x - a)$. Conversely, let M be a maximal ideal of $\mathbb{C}[x]$. Then M is generated by a monic irreducible polynomial. The monic irreducible polynomials in $\mathbb{C}[x]$ are the polynomials $x - a$. □

The next theorem extends this corollary to polynomials rings in several variables.

Theorem 11.8.6 Hilbert's Nullstellensatz.[1] 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 $a = (a_1, \ldots, a_n)$ of $\mathbb{C}^n$ corresponds to the kernel M_a of the substitution map $s_a: \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$ that sends $x_i \rightsquigarrow a_i$. The kernel M_a is generated by the n linear polynomials $x_i - a_i$.

Proof. Let a be a point of $\mathbb{C}^n$, and let M_a be the kernel of s_a. Since s_a is surjective and since $\mathbb{C}$ is a field, M_a is a maximal ideal. To verify that M_a is generated by the linear polynomials as asserted, we first consider the case that the point a is the origin $(0, \ldots, 0)$. We must show that the kernel of the map s_0 that evaluates a polynomial at the origin is generated by the variables $x_1, \ldots, x_n$. Well, $f(0, \ldots, 0) = 0$ if and only if the constant term of f is zero. If so, then every monomial that occurs in f is divisible by at least one of the variables, so f can

[1] The German word *Nullstellensatz* is a combination of three words whose translations are zero, places, theorem.

be written as a linear combination of the variables, with polynomial coefficients. The proof for an arbitrary point a can be made using the change of variable $x_i = x_i' + a_i$ to move a to the origin.

It is harder to prove that every maximal ideal has the form M_a. Let M be a maximal ideal, and let $\mathcal{F}$ denote the field $\mathbb{C}[x_1, \ldots, x_n]/M$. We restrict the canonical map (11.4.1) $\pi: \mathbb{C}[x_1, \ldots, x_n] \to \mathcal{F}$ to the subring $\mathbb{C}[x_1]$ of polynomials in in the first variable, obtaining a homomorphism $\varphi_1: \mathbb{C}[x_1] \to \mathcal{F}$. Proposition 11.8.4 shows that the kernel of φ is either the zero ideal, or one of the maximal ideals $(x_1 - a_1)$ of $\mathbb{C}[x_1]$. We'll show that it cannot be the zero ideal. The same will be true when the index 1 is replaced by any other index, so M will contain linear polynomials of the form $x_i - a_i$ for each i. This will show that M contains one of the ideals M_a, and since M_a is maximal, M will be equal to that ideal.

In what follows, we drop the subscript from x_1. We suppose that $\ker \varphi = (0)$. Then φ maps $\mathbb{C}[x]$ isomorphically to its image, a subring of $\mathcal{F}$. The mapping property of fraction fields shows that this map extends to an injective map $\mathbb{C}(x) \to \mathcal{F}$, where $\mathbb{C}(x)$ is the field of rational functions – the field of fractions of the polynomial ring $\mathbb{C}[x]$. So $\mathcal{F}$ contains a field isomorphic to $\mathbb{C}(x)$. The next lemma shows that this is impossible. Therefore $\ker\varphi \neq (0)$.

Lemma 11.8.7

(a) Let R be a ring that contains the complex numbers $\mathbb{C}$ as a subring. The laws of composition on R can be used to make R into a complex vector space.

(b) As a vector space, the field $\mathcal{F} = \mathbb{C}[x_1, \ldots, x_n]/M$ is spanned by a countable set of elements.

(c) Let V be a vector space over a field, and suppose that V is spanned by a countable set of vectors. Then every independent subset of V is finite or countably infinite.

(d) When $\mathbb{C}(x)$ is made into a vector space over $\mathbb{C}$, the uncountable set of rational functions $(x - \alpha)^{-1}$, with α in $\mathbb{C}$, is independent.

Assume that the lemma has been proved. Then **(b)** and **(c)** show that every independent set in $\mathcal{F}$ is finite or countably infinite. On the other hand, $\mathcal{F}$ contains a subring isomorphic to $\mathbb{C}(x)$, so by **(d)**, $\mathcal{F}$ contains an uncountable independent set. This is a contradiction. □

Proof of the Lemma. **(a)** For addition, one uses the addition law in R. Scalar multiplication ca of an element a of R by an element c of $\mathbb{C}$ is defined by multiplying these elements in R. The axioms for a vector space follow from the ring axioms.

(b) The surjective homomorphism $\pi: \mathbb{C}[x_1, \ldots, x_n] \to \mathcal{F}$ defines a map $\mathbb{C} \to \mathcal{F}$, by means of which we identify $\mathbb{C}$ as a subring of $\mathcal{F}$, and make $\mathcal{F}$ into a complex vector space. The countable set of monomials $x_1^{e_1} \cdots x_n^{e_n}$ forms a basis for $\mathbb{C}[x_1, \ldots, x_n]$, and since π is surjective, the images of these monomials span $\mathcal{F}$.

(c) Let S be a countable set that spans V, say $S = \{v_1, v_2, \ldots\}$. It could be finite or infinite. Let S_n be the subset $(v_1, \ldots, v_n)$ consisting of the first n elements of S, and let V_n be the span of S_n. If S is infinite, there will be infinitely many of these subspaces. Since S spans V, every element of V is a linear combination of finitely many elements of S, so it is in one of the spaces V_n. In other words, $\bigcup V_n = V$.

Let L be an independent set in V, and let $L_n = L \cap V_n$. Then L_n is a linearly independent subset of the space V_n, which is spanned by a set of n elements. So $|L_n| \leq n$ (3.4.18). Moreover, $L = \bigcup L_n$ because $V = \bigcup V_n$. The union of countably many finite sets is finite or countably infinite.

(d) We must remember that linear combinations can involve only finitely many vectors. So we ask: Can we have a linear relation

$$\sum_{\nu=1}^{k} \frac{c_\nu}{x - \alpha_\nu} = 0,$$

where $\alpha_1, \ldots, \alpha_k$ are distinct complex numbers and the coefficients c_ν aren't zero? No. Such a linear combination of formal rational functions defines a complex valued function except at the points $x = \alpha_\nu$. If the linear combination were zero, the function it defines would be identically zero. But $(x - \alpha_1)^{-1}$ takes on arbitrarily large values near α_1, while $(x - \alpha_\nu)^{-1}$ is bounded near α_1 for $\nu = 2, \ldots, k$. So the linear combination does not define the zero function. □

11.9 ALGEBRAIC GEOMETRY

A point $(a_1, \ldots, a_n)$ of $\mathbb{C}^n$ is called a *zero* of a polynomial $f(x_1, \ldots, x_n)$ of n variables if $f(a_1, \ldots, a_n) = 0$. We also say that the polynomial f *vanishes* at such a point. The *common zeros* of a set $\{f_1, \ldots, f_r\}$ of polynomials are the points of $\mathbb{C}^n$ at which all of them vanish – the solutions of the system of equations $f_1 = \cdots = f_r = 0$.

- A subset V of complex n-space $\mathbb{C}^n$ that is the set of common zeros of a finite number of polynomials in n variables is called an *algebraic variety*, or just a *variety*.

For instance, a *complex line* in the (x, y)-plane $\mathbb{C}^2$ 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) of $\mathbb{C}^2$ is the set of common zeros of the two polynomials $x - a$ and $y - b$. The group $SL_2(\mathbb{C})$ is a variety in $\mathbb{C}^{2\times 2}$. It is the set of zeros of the polynomial $x_{11}x_{22} - x_{12}x_{21} - 1$.

The Nullstellensatz provides an important link between algebra and geometry. It tells us that the maximal ideals in the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ correspond to points in $\mathbb{C}^n$. This correspondence also relates algebraic varieties to quotient rings of the polynomial ring.

Theorem 11.9.1 Let I be the ideal of $\mathbb{C}[x_1, \ldots, x_n]$ generated by some polynomials $f_1, \ldots f_r$, and let R be the quotient ring $\mathbb{C}[x_1, \ldots, x_n]/I$. Let V be the variety of (common) zeros of the polynomials $f_1, \ldots, f_r$ in $\mathbb{C}^n$. The maximal ideals of R are in bijective correspondence with the points of V.

Proof. The maximal ideals of R correspond to the maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ that contain I (Correspondence Theorem). An ideal of $\mathbb{C}[x_1, \ldots, x_n]$ will contain I if and only if it contains the generators $f_1, \ldots, f_r$ of I. Every maximal ideal of the ring $\mathbb{C}[x_1, \ldots, x_n]$ is the kernel M_a of the substitution map that sends $x_i \rightsquigarrow a_i$ for some point $a = (a_1, \ldots, a_n)$ of $\mathbb{C}^n$, and the polynomials $f_1, \ldots, f_r$ are in M_a if and only if $f_1(a) = \cdots = f_r(a) = 0$, which is to say, if and only if a is a point of V. □

As this theorem suggests, algebraic properties of the ring $R = \mathbb{C}[x]/I$ are closely related to geometric properties of the variety V. The analysis of this relationship is the field of mathematics called algebraic geometry.

A simple question one might ask about a set is whether or not it is empty. Is it possible for a ring to have no maximal ideals at all? This happens only for the zero ring.

Theorem 11.9.2 Let R be a ring. Every ideal I of R that is not R itself is contained in a maximal ideal.

To find a maximal ideal, one might try this procedure: If I is not maximal, choose a proper ideal I' that is larger than I. Replace I by I', and repeat. The proof follows this line of reasoning, but one may have to repeat the procedure many times, possibly uncountably often. Because of this, the proof requires the *Axiom of Choice*, or *Zorn's Lemma* (see the Appendix). The Hilbert Basis Theorem, which we will prove later (14.6.7), shows that for most rings that we study, the proof requires only a weak countable version of the Axiom of Choice. Rather than enter into a discussion of the Axiom of Choice here, we defer further discussion of the proof to Chapter 14. □

Corollary 11.9.3 The only ring R having no maximal ideals is the zero ring.

This follows from the theorem, because every nonzero ring R contains an ideal different from R: the zero ideal. □

Putting Theorems 11.9.1 and 11.9.2 together gives us another corollary:

Corollary 11.9.4 If a system of polynomial equations $f_1 = \cdots = f_r = 0$ in n variables has no solution in $\mathbb{C}^n$, then 1 is a linear combination $1 = \sum g_i f_i$ with polynomial coefficients g_i.

Proof. If the system has no solution, there is no maximal ideal that contains the ideal $I = (f_1, \ldots, f_r)$. So I is the unit ideal, and 1 is in I. □

Example 11.9.5 Most choices of three polynomials f_1, f_2, f_3 in two variables have no common solutions. For instance, the ideal of $\mathbb{C}[t, x]$ generated by

$$f_1 = t^2 + x^2 - 2, \quad f_2 = tx - 1, \quad f_3 = t^3 + 5tx^2 + 1 \tag{11.9.6}$$

is the unit ideal. This can be proved by showing that the equations $f_1 = f_2 = f_3 = 0$ have no solution in $\mathbb{C}^2$. □

It isn't easy to get a clear geometric picture of an algebraic variety in $\mathbb{C}^n$, but the general shape of a variety in $\mathbb{C}^2$ can be described fairly simply, and we do that here. We work with the polynomial ring in the two variables t and x.

Lemma 11.9.7 Let $f(t, x)$ be a polynomial, and let α be a complex number. The following are equivalent:

(a) $f(t, x)$ vanishes at every point of the locus $\{t = \alpha\}$ in $\mathbb{C}^2$,

(b) The one-variable polynomial $f(\alpha, x)$ is the zero polynomial,

(c) $t - \alpha$ divides f in $\mathbb{C}[t, x]$.

Proof. If f vanishes at every point of the locus $t = \alpha$, the polynomial $f(\alpha, x)$ is zero for every x. Then since a nonzero polynomial in one variable has finitely many roots, $f(\alpha, x)$ is the zero polynomial. This shows that **(a)** implies **(b)**.

A change of variable $t = t' + \alpha$ reduces the proof that **(b)** implies **(c)** to the case that $\alpha = 0$. If $f(0, x)$ is the zero polynomial, then t divides every monomial that occurs in f, and t divides f. Finally, the implication **(c)** implies **(a)** is clear. □

Let $\mathcal{F}$ denote the field of rational functions $\mathbb{C}(t)$ in t, the field of fractions of the ring $\mathbb{C}[t]$. The ring $\mathbb{C}[t, x]$ is a subring of the one-variable polynomial ring $\mathcal{F}[x]$; its elements are polynomials in x,

$$f(t, x) = a_n(t)x^n + \cdots + a_1(t)x + a_0(t), \tag{11.9.8}$$

whose coefficients $a_i(t)$ are rational functions in t. It can be helpful to begin by studying a problem about $\mathbb{C}[t, x]$ in the ring $\mathcal{F}[x]$, because its algebra is simpler. Division with remainder is available, and every ideal of $\mathcal{F}[x]$ is principal.

Proposition 11.9.9 Let $h(t, x)$ and $f(t, x)$ be nonzero elements of $\mathbb{C}[t, x]$. Suppose that h is not divisible by any polynomial of the form $t - \alpha$. If h divides f in $\mathcal{F}[x]$, then h divides f in $\mathbb{C}[t, x]$.

Proof. We divide by h in $\mathcal{F}[x]$, say $f = hq$, and we show that q is an element of $\mathbb{C}[t, x]$. Since q is an element of $\mathcal{F}[x]$, it is a polynomial in x whose coefficients are rational functions in t. We multiply both sides of the equation $f = hq$ by a monic polynomial in t to clear denominators in these coefficients. This gives us an equation of the form

$$u(t)f(t, x) = h(t, x)q_1(t, x),$$

where $u(t)$ is a monic polynomial in t, and q_1 is an element of $\mathbb{C}[t, x]$. We use induction on the degree of u. If u has positive degree, it will have a complex root α. Then $t - \alpha$ divides the left side of this equation, so it divides the right side too. This means that $h(\alpha, x)q_1(\alpha, x)$ is the zero polynomial in x. By hypothesis, $t - \alpha$ does not divide h, so $h(\alpha, x)$ is not zero. Since the polynomial ring $\mathbb{C}[x]$ is a domain, $q_1(\alpha, x) = 0$, and the lemma shows that $t - \alpha$ divides $q_1(t, x)$. We cancel $t - \alpha$ from u and q_1. Induction completes the proof. □

Theorem 11.9.10 Two nonzero polynomials $f(t, x)$ and $g(t, x)$ in two variables have only finitely many common zeros in $\mathbb{C}^2$, unless they have a common nonconstant factor in $\mathbb{C}[t, x]$.

If the degrees of the polynomials f and g are m and n respectively, the number of common zeros is at most mn. This is known as the *Bézout bound*. For instance, two

quadratic polynomials have at most four common zeros. (The analogue of this statement for real polynomials is that two conics intersect in at most four points.) It is harder to prove the Bézout bound than the finiteness. We won't need that bound, so we won't prove it.

Proof of Theorem 11.9.10. Assume that f and g have no common factor. Let I denote the ideal generated by f and g in $\mathcal{F}[x]$, where $\mathcal{F} = \mathbb{C}(t)$, as above. This is a principal ideal, generated by the (monic) greatest common divisor h of f and g in $\mathcal{F}[x]$.

If $h \neq 1$, it will be a polynomial whose coefficients may have denominators that are polynomials in t. We multiply by a polynomial in t to clear these denominators, obtaining a polynomial h_1 in $\mathbb{C}[t, x]$. We may assume that h_1 isn't divisible by any polynomial $t - \alpha$. Since the denominators are units in $\mathcal{F}$ and since h divides f and g in $\mathcal{F}[x]$, h_1 also divides f and g in $\mathcal{F}[x]$. Proposition 11.9.9 shows that h_1 divides f and g in $\mathbb{C}[t, x]$. Then f and g have a common nonconstant factor in $\mathbb{C}[t, x]$. We're assuming that this is not the case.

So the greatest common divisor of f and g in $\mathcal{F}[x]$ is 1, and $1 = rf + sg$, where r and s are elements of $\mathcal{F}[x]$. We clear denominators from r and s, multiplying both sides of the equation by a suitable polynomial $u(t)$. This gives us an equation of the form

$$u(t) = r_1(t, x) f(t, x) + s_1(t, x) g(t, x),$$

where all terms on the right are polynomials in $\mathbb{C}[t, x]$. This equation shows that if (t_0, x_0) is a common zero of f and g, then t_0 must be a root of u. But u is a polynomial in t, and a nonzero polynomial in one variable has finitely many roots. So at the common zeros of f and g, the variable t takes on only finitely many values. Similar reasoning shows that x takes on only finitely many values. This gives us only finitely many possibilities for the common zeros. □

Theorem 11.9.10 suggests that the most interesting varieties in $\mathbb{C}^2$ are those defined as the locus of zeros of a single polynomial $f(t, x)$.

- The locus X of zeros in $\mathbb{C}^2$ of a polynomial $f(t, x)$ is called the *Riemann surface* of f.

It is also called a *plane algebraic curve* – a confusing phrase. As a topological space, the locus X has dimension two. Calling it an algebraic curve refers to the fact that the points of X depend only on one *complex* parameter. We give a rough description of a Riemann surface here. Let's assume that the polynomial f is *irreducible* – that it is not a product of two nonconstant polynomials, and also that it has positive degree in the variable x. Let

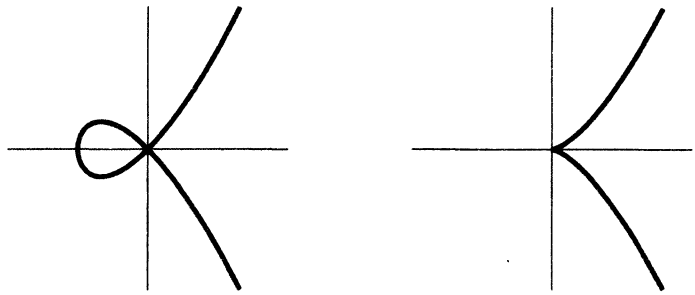
$$X = \{(t, x) \in \mathbb{C}^2 \mid f(t, x) = 0\} \tag{11.9.11}$$

be its Riemann surface, and let T denote the complex t-plane. Sending $(t, x) \rightsquigarrow t$ defines a continuous map that we call a *projection*

$$\pi: X \to T. \tag{11.9.12}$$

We will describe X in terms of this projection. However, our description will require that a finite set of "bad points" be removed from X. In fact, what is usually called the Riemann surface agrees with our definition only when suitable finite subsets are removed. The locus $\{f = 0\}$ may be "singular" at some points, and some other points of X may be "at infinity." The points at infinity are explained below (see (11.9.17)).

The simplest examples of singular points are *nodes*, at which the surface crosses itself, and *cusps*. The locus $x^2 = t^3 - t^2$ has a node at the origin, and the locus $x^2 = t^3$ has a cusp at the origin. The real points of these Riemann surfaces are shown here.



a node a cusp

(11.9.13) Some Singular Curves

To avoid repetition of the disclaimer "except on a finite set," we write X' for the complement of an unspecified finite subset of X, which is allowed to vary. Whenever a construction runs into trouble at some point, we simply delete that point. Essentially everything we do here and when we come back to Riemann surfaces in Chapter 15 will be valid only for X'. We keep X on hand for reference.

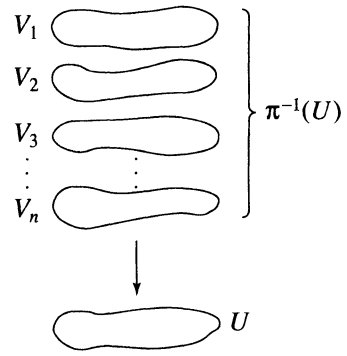
Our description of the Riemann surface will be as a branched covering of the complex t-plane T. The definition of covering space that we give here assumes that the spaces are Hausdorff spaces ([Munkres] p. 98). You can ignore this point if you don't know what it means. The sets in which we are interested are Hausdorff spaces because they are subsets of $\mathbb{C}^2$.

Definition 11.9.14 Let X and T be Hausdorff spaces. A continuous map $\pi: X \to T$ is an n-sheeted *covering space* if every fibre consists of n points, and if it has this property: Let x_0 be a point of X and let $\pi(x_0) = t_0$. Then π maps an open neigborhood U of x_0 in X homeomorphically to an open neighborhood V of t_0 in T.

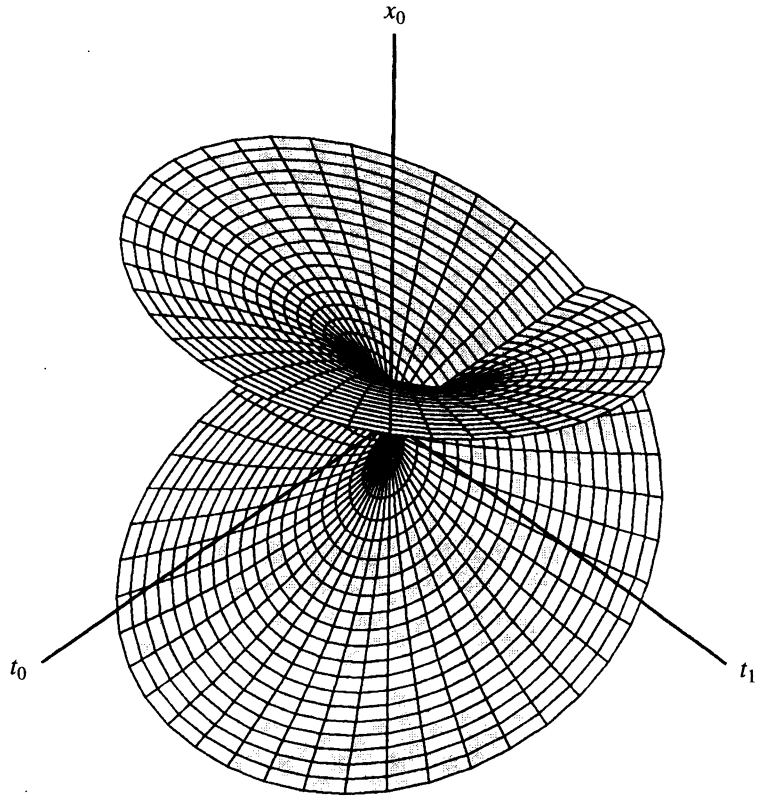
A map π from X to the complex plane T is an n-sheeted *branched covering* if X contains no isolated points, the fibres of π are finite, and if there is a finite set Δ of points of T called *branch points*, such that the map $(X - \pi^{-1}\Delta) \to (T - \Delta)$ is an n-sheeted covering space. For emphasis, a covering space is sometimes called an *unbranched covering*.

Figure 11.9.15 below depicts the Riemann surface of the polynomial $x^2 - t$, a two-sheeted covering of T that is branched at the point $t = 0$. The figure has been obtained by writing t and x in terms of their real and imaginary parts, $t = t_0 + t_1 i$ and $x = x_0 + x_1 i$, and dropping the imaginary part x_1 of x, to obtain a surface in three-dimensional space. Its further projection to the plane is depicted using standard graphics.

The projected surface intersects itself along the negative t_0-axis, though the Riemann surface itself does not. Every negative real number t has two purely imaginary square roots. The real parts of these square roots are zero, and this produces the self-crossing in the projected surface.



(11.9.14) Part of an unbranched covering.



(11.9.15) The Riemann surface $x^2 = t$.

Given a branched covering $X \to T$, we refer to the points in the set Δ as its *branch points*, though this is imprecise: The defining property continues to hold when we add any finite set of points to Δ. So we allow the possibility that some points of Δ don't need to be included – that they aren't "true" branch points.

Theorem 11.9.16 Let $f(t, x)$ be an irreducible polynomial in $\mathbb{C}[t, x]$ which has positive degree n in the variable x. The Riemann surface of f is an n-sheeted branched covering of the complex plane T.

Proof. The main step is to verify the first condition of (11.9.14), that the fibre $\pi^{-1}(t_0)$ consists of precisely n points except on a finite subset Δ.

The points of the fibre $\pi^{-1}(t_0)$ are the points (t_0, x_0) such that x_0 is a root of the one-variable polynomial $f(t_0, x)$. We must show that, except for a finite set of values $t = t_0$, this polynomial has n distinct roots. We write $f(t, x)$ as a polynomial in x whose coefficients are polynomials in t, say $f(x) = a_n(t)x^n + \cdots + a_0(t)$, and we denote $a_i(t_0)$ by a_i^0. The polynomial $f(t_0, x) = a_n^0 x^n + \cdots + a_1^0 x + a_0^0$ has degree at most n, so it has at most n roots. Therefore the fibre $\pi^{-1}(p)$ contains at most n points. It will have fewer than n points if either

(11.9.17)

(a) the degree of $f(t_0, x)$ is less than n, or

(b) $f(t_0, x)$ has a multiple root.

The first case occurs when t_0 is a root of $a_n(t)$. (If t_0 is a root of $a_n(t)$, one of the roots of $f(t_1, x)$ tends to infinity as $t_1 \to t_0$.) Since $a_n(t)$ is a polynomial, there are finitely many such values.

Consider the second case. A complex number x_0 is a multiple root of a polynomial $h(x)$ if $(x - x_0)^2$ divides $h(x)$, and this happens if and only if x_0 is a common root of $h(x)$ and its derivative $h'(x)$ (see Exercise 3.5). Here $h(x) = f(t_0, x)$. The first variable is fixed, so the derivative is the partial derivative $\frac{\partial f}{\partial x}$. Going back to the polynomial $f(t, x)$ in two variables, we see that the second case occurs at the points (t_0, x_0) that are common zeros of f and $\frac{\partial f}{\partial x}$. Now f cannot divide its partial derivative, which has lower degree in x. Since f is assumed to be irreducible, f and $\frac{\partial f}{\partial x}$ have no common nonconstant factor. Theorem 11.9.10 tells us that there are finitely many common zeros.

We now check the second condition of (11.9.14). Let t_0 be a point of T such that the fibre $\pi^{-1}(t_0)$ consists of n points, and let (t_0, x_0) be a point of X in the fibre. Then x_0 is a simple root of $f(t_0, x)$, and therefore $\frac{\partial f}{\partial x}$ is not zero at this point. The Implicit Function Theorem A.4.3 implies that one can solve for x as a function $x(t)$ of t in a neighborhood of t_0, such that $x(t_0) = x_0$. The neighborhood U referred to in the definition of covering space is the graph of this function. □

To me algebraic geometry is algebra with a kick.

—Solomon Lefschetz

EXERCISES

Section 1 Definition of a Ring

1.1. Prove that $7 + \sqrt[3]{2}$ and $\sqrt{3} + \sqrt{-5}$ are algebraic numbers.

1.2. Prove that, for $n \neq 0$, $\cos(2\pi/n)$ is an algebraic number.

1.3. Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing the rational numbers $\mathbb{Q}$ and the elements $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Let $\gamma = \alpha + \beta$. Is $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$? Is $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\gamma]$?

1.4. Let $\alpha = \frac{1}{2}i$. Prove that the elements of $\mathbb{Z}[\alpha]$ are dense in the complex plane.

1.5. Determine all subrings of $\mathbb{R}$ that are discrete sets.

1.6. Decide whether or not S is a subring of R, when

(a) S is the set of all rational numbers a/b, where b is not divisible by 3, and $R = \mathbb{Q}$,

(b) S is the set of functions which are linear combinations with integer coefficients of the functions $\{1, \cos nt, \sin nt\}$, $n \in \mathbb{Z}$, and R is the set of all real valued functions of t.

1.7. 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 $A + B = (A \cup B) - (A \cap B)$ and $A \cdot B = A \cap B$.

(b) R is the set of continuous functions $\mathbb{R} \to \mathbb{R}$. Addition and multiplication are defined by the rules $[f + g](x) = f(x) + g(x)$ and $[f \circ g](x) = f(g(x))$.

1.8. Determine the units in: **(a)** $\mathbb{Z}/12\mathbb{Z}$, **(b)** $\mathbb{Z}/8\mathbb{Z}$, **(c)** $\mathbb{Z}/n\mathbb{Z}$.

1.9. Let R be a set with two laws of composition satisfying all ring axioms except the commutative law for addition. Use the distributive law to prove that the commutative law for addition holds, so that R is a ring.

Section 2 Polynomial Rings

2.1. For which positive integers n does $x^2 + x + 1$ divide $x^4 + 3x^3 + x^2 + 7x + 5$ in $[\mathbb{Z}/(n)][x]$?

2.2. Let F be a field. The set of all formal power series $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots$, with a_i in F, forms a ring that is often denoted by $F[[t]]$. By *formal* power series we mean that the coefficients form an arbitrary sequence of elements of F. There is no requirement of convergence. Prove that $F[[t]]$ is a ring, and determine the units in this ring.

Section 3 Homomorphisms and Ideals

3.1. Prove that an ideal of a ring R is a subgroup of the additive group R^+.

3.2. Prove that every nonzero ideal in the ring of Gauss integers contains a nonzero integer.

3.3. Find generators for the kernels of the following maps:

(a) $\mathbb{R}[x, y] \to \mathbb{R}$ defined by $f(x, y) \rightsquigarrow f(0, 0)$,

(b) $\mathbb{R}[x] \to \mathbb{C}$ defined by $f(x) \rightsquigarrow f(2 + i)$,

(c) $\mathbb{Z}[x] \to \mathbb{R}$ defined by $f(x) \rightsquigarrow f(1 + \sqrt{2})$,

(d) $\mathbb{Z}[x] \to \mathbb{C}$ defined by $x \rightsquigarrow \sqrt{2} + \sqrt{3}$.

(e) $\mathbb{C}[x, y, z] \to \mathbb{C}[t]$ defined by $x \rightsquigarrow t$, $y \rightsquigarrow t^2$, $z \rightsquigarrow t^3$.

3.4. Let $\varphi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ be the homomorphism that sends $x \rightsquigarrow t+1$ and $y \rightsquigarrow t^3 - 1$. Determine the kernel K of φ, and prove that every ideal I of $\mathbb{C}[x, y]$ that contains K can be generated by two elements.

3.5. The derivative of a polynomial f with coefficients in a field F is defined by the calculus formula $(a_n x^n + \cdots + a_1 x + a_0)' = n a_n x^{n-1} + \cdots + 1 a_1$. The integer coefficients are interpreted in F using the unique homomorphism $\mathbb{Z} \to F$.

(a) Prove the product rule $(fg)' = f'g + fg'$ and the chain rule $(f \circ g)' = (f' \circ g)g'$.

(b) Let α be an element of F. Prove that α is a multiple root of a polynomial f if and only if it is a common root of f and of its derivative f'.

3.6. An *automorphism* of a ring R is an isomorphism from R to itself. Let R be a ring, and let $f(y)$ be a polynomial in one variable with coefficients in R. Prove that the map $R[x, y] \to R[x, y]$ defined by $x \rightsquigarrow x + f(y)$, $y \rightsquigarrow y$ is an automorphism of $R[x, y]$.

3.7. Determine the automorphisms of the polynomial ring $\mathbb{Z}[x]$ (see Exercise 3.6).

3.8. Let R be a ring of prime characteristic p. Prove that the map $R \to R$ defined by $x \rightsquigarrow x^p$ is a ring homomorphism. (It is called the *Frobenius map.*)

3.9. **(a)** An element x of a ring R is called *nilpotent* if some power is zero. Prove that if x is nilpotent, then $1 + x$ is a unit.

(b) Suppose that R has prime characteristic $p \neq 0$. Prove that if a is nilpotent then $1 + a$ is *unipotent*, that is, some power of $1 + a$ is equal to 1.

3.10. Determine all ideals of the ring $F[[t]]$ of formal power series with coefficients in a field F (see Exercise 2.2).

3.11. Let R be a ring, and let I be an ideal of the polynomial ring $R[x]$. Let n be the lowest degree among nonzero elements of I. Prove or disprove: I contains a monic polynomial of degree n if and only if it is a principal ideal.

3.12. Let I and J be ideals of a ring R. Prove that the set $I + J$ of elements of the form $x + y$, with x in I and y in J, is an ideal. This ideal is called the *sum* of the ideals I and J.

3.13. Let I and J be ideals of a ring R. Prove that the intersection $I \cap J$ is an ideal. 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 $\sum x_\nu y_\nu$ of products of elements of I and J is an ideal. This ideal is called the *product ideal*, and is denoted by IJ. Is there a relation between IJ and $I \cap J$?

Section 4 Quotient Rings

4.1. Consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ that sends $x \rightsquigarrow 1$. Explain what the Correspondence Theorem, when applied to this map, says about ideals of $\mathbb{Z}[x]$.

4.2. What does the Correspondence Theorem tell us about ideals of $\mathbb{Z}[x]$ that contain $x^2 + 1$?

4.3. Identify the following rings: **(a)** $\mathbb{Z}[x]/(x^2 - 3, 2x + 4)$, **(b)** $\mathbb{Z}[i]/(2 + i)$, **(c)** $\mathbb{Z}[x]/(6, 2x - 1)$, **(d)** $\mathbb{Z}[x]/(2x^2 - 4, 4x - 5)$, **(e)** $\mathbb{Z}[x]/(x^2 + 3, 5)$.

4.4. Are the rings $\mathbb{Z}[x]/(x^2 + 7)$ and $\mathbb{Z}[x]/(2x^2 + 7)$ isomorphic?

Section 5 Adjoining Elements

5.1. Let $f = x^4 + x^3 + x^2 + x + 1$ and let α denote the residue of x in the ring $R = \mathbb{Z}[x]/(f)$. Express $(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1)$ in terms of the basis $(1, \alpha, \alpha^2, \alpha^3)$ of R.

5.2. Let a be an element of a ring R. If we adjoin an element α with the relation $\alpha = a$, we expect to get a ring isomorphic to R. Prove that this is true.

5.3. Describe the ring obtained from $\mathbb{Z}/12\mathbb{Z}$ by adjoining an inverse of 2.

5.4. Determine the structure of the ring R' obtained from $\mathbb{Z}$ by adjoining an element α satisfying each set of relations.

(a) $2\alpha = 6, 6\alpha = 15$, **(b)** $2\alpha - 6 = 0, \alpha - 10 = 0$, **(c)** $\alpha^3 + \alpha^2 + 1 = 0, \alpha^2 + \alpha = 0$.

5.5. Are there fields F such that the rings $F[x]/(x^2)$ and $F[x]/(x^2 - 1)$ are isomorphic?

5.6. Let a be an element of a ring R, and let R' be the ring $R[x]/(ax - 1)$ obtained by adjoining an inverse of a to R. Let α denote the residue of x (the inverse of a in R').

(a) Show that every element β of R' can be written in the form $\beta = \alpha^k b$, with b in R.

(b) Prove that the kernel of the map $R \to R'$ is the set of elements b of R such that $a^n b = 0$ for some $n > 0$.

(c) Prove that R' is the zero ring if and only if a is nilpotent (see Exercise 3.9).

5.7. Let F be a field and let $R = F[t]$ be the polynomial ring. Let R' be the ring extension $R[x]/(tx - 1)$ obtained by adjoining an inverse of t to R. Prove that this ring can be identified as the ring of *Laurent polynomials*, which are finite linear combinations of powers of t, negative exponents included.

Section 6 Product Rings

6.1. Let $\varphi: \mathbb{R}[x] \to \mathbb{C} \times \mathbb{C}$ be the homomorphism defined by $\varphi(x) = (1, i)$ and $\varphi(r) = (r, r)$ for r in $\mathbb{R}$. Determine the kernel and the image of φ.

6.2. Is $\mathbb{Z}/(6)$ isomorphic to the product ring $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$? Is $\mathbb{Z}/(8)$ isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(4)$?

6.3. Classify rings of order 10.

6.4. In each case, describe the ring obtained from the field $\mathbb{F}_2$ by adjoining an element α satisfying the given relation:

(a) $\alpha^2 + \alpha + 1 = 0$, **(b)** $\alpha^2 + 1 = 0$, **(c)** $\alpha^2 + \alpha = 0$.

6.5. Suppose we adjoin an element α satisfying the relation $\alpha^2 = 1$ to the real numbers $\mathbb{R}$. Prove that the resulting ring is isomorphic to the product $\mathbb{R} \times \mathbb{R}$.

6.6. Describe the ring obtained from the product ring $\mathbb{R} \times \mathbb{R}$ by inverting the element $(2, 0)$.

6.7. Prove that in the ring $\mathbb{Z}[x]$, the intersection $(2) \cap (x)$ of the principal ideals (2) and (x) is the principal ideal $(2x)$, and that the quotient ring $R = \mathbb{Z}[x]/(2x)$ is isomorphic to the subring of the product ring $\mathbb{F}_2[x] \times \mathbb{Z}$ of pairs $(f(x), n)$ such that $f(0) \equiv n$ modulo 2.

6.8. Let I and J be ideals of a ring R such that $I + J = R$.

(a) Prove that $IJ = I \cap J$ (see Exercise 3.13).

(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 $x - a \in I$.)

(c) Prove that if $IJ = 0$, then R is isomorphic to the product ring $(R/I) \times (R/J)$.

(d) Describe the idempotents corresponding to the product decomposition in **(c)**.

Section 7 Fractions

7.1. Prove that a domain of finite order is a field.

7.2. Let R be a domain. Prove that the polynomial ring $R[x]$ is a domain, and identify the units in $R[x]$.

7.3. Is there a domain that contains exactly 15 elements?

7.4. Prove that the field of fractions of the formal power series ring $F[[x]]$ over a field F can be obtained by inverting the element x. Find a neat description of the elements of that field (see Exercise 11.2.1).

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

Section 8 Maximal Ideals

8.1. Which principal ideals in $\mathbb{Z}[x]$ are maximal ideals?

8.2. Determine the maximal ideals of each of the following rings:
(a) $\mathbb{R} \times \mathbb{R}$, **(b)** $\mathbb{R}[x]/(x^2)$, **(c)** $\mathbb{R}[x]/(x^2 - 3x + 2)$, **(d)** $\mathbb{R}[x]/(x^2 + x + 1)$.

8.3. 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.

8.4. Establish a bijective correspondence between maximal ideals of $\mathbb{R}[x]$ and points in the upper half plane.

Section 9 Algebraic Geometry

9.1. 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 $R = \mathbb{C}[x, y]/I$? $(x - 1, y - 4)$, $(x + 1, y + 4)$, $(x^3 - 17, y^2)$.

9.2. Let $f_1, \ldots, f_r$ be complex polynomials in the variables $x_1, \ldots, x_n$, let V be the variety of their common zeros, and let I be the ideal of the polynomial ring $R = \mathbb{C}[x_1, \ldots, x_n]$ that they generate. Define a homomorphism from the quotient ring $\overline{R} = R/I$ to the ring $\mathcal{R}$ of continuous, complex-valued functions on V.

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

9.4. Let U and V be varieties in $\mathbb{C}^n$. Prove that the union $U \cup V$ and the intersection $U \cap V$ are varieties. What does the statement $U \cap V = \emptyset$ mean algebraically? What about the statement $U \cup V = \mathbb{C}^n$?

9.5. Prove that the variety of zeros of a set $\{f_1, \ldots, f_r\}$ of polynomials depends only on the ideal that they generate.

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

9.7. Determine the points of intersection in $\mathbb{C}^2$ of the two loci in each of the following cases:
(a) $y^2 - x^3 + x^2 = 1$, $x + y = 1$, **(b)** $x^2 + xy + y^2 = 1$, $x^2 + 2y^2 = 1$,
(c) $y^2 = x^3$, $xy = 1$, **(d)** $x + y^2 = 0$, $y + x^2 + 2xy^2 + y^4 = 0$.

9.8. Which ideals in the polynomial ring $\mathbb{C}[x, y]$ contain $x^2 + y^2 - 5$ and $xy - 2$?

9.9. An *irreducible* plane algebraic curve C is the locus of zeros in $\mathbb{C}^2$ of an irreducible polynomial $f(x, y)$. A point p of C is a *singular point* of the curve if $f = \partial f/\partial x = \partial f/\partial y = 0$ at p. Otherwise p is a *nonsingular point*. Prove that an irreducible curve has only finitely many singular points.

9.10. Let L be the (complex) line $\{ax + by + c = 0\}$ in $\mathbb{C}^2$, and let C be the algebraic curve $\{f(x, y) = 0\}$, where f is an irreducible polynomial of degree d. Prove $C \cap L$ contains at most d points unless $C = L$.

9.11. Let C_1 and C_2 be the zeros of quadratic polynomials f_1 and f_2 respectively that don't have a common linear factor.

(a) Let p and q be distinct points of intersection of C_1 and C_2, and let L be the (complex) line through p and q. Prove that there are constants c_1 and c_2, not both zero, so that $g = c_1 f_1 + c_2 f_2$ vanishes identically on L. Prove also that g is the product of linear polynomials.

Hint: Force g to vanish at a third point of L.

(b) Prove that C_1 and C_2 have at most 4 points in common.

9.12. Prove in two ways that the three polynomials $f_1 = t^2+x^2-2$, $f_2 = tx-1$, $f_3 = t^3+5tx^2+1$ generate the unit ideal in $\mathbb{C}[x, y]$: by showing that they have no common zeros, and also by writing 1 as a linear combination of f_1, f_2, f_3, with polynomial coefficients.

***9.13.** Let $\varphi : \mathbb{C}[x, y] \to \mathbb{C}[t]$ be a homomorphism that is the identity on $\mathbb{C}$ and sends $x \rightsquigarrow x(t)$, $y \rightsquigarrow y(t)$, and such that $x(t)$ and $y(t)$ are not both constant. Prove that the kernel of φ is a principal ideal.

Miscellaneous Exercises

M.1. Prove or disprove: If $a^2 = a$ for every a in a nonzero ring R, then R has characteristic 2.

M.2. A semigroup S is a set with an associative law of composition having an identity element. Let S be a commutative semigroup that satisfies the cancellation law: $ab = ac$ implies $b = c$. Prove that S can be embedded into a group.

M.3. Let R denote the set of sequences $a = (a_1, a_2, a_3, \ldots)$ of real numbers that are eventually constant: $a_n = a_{n+1} = \ldots$ for sufficiently large n. Addition and multiplication are componentwise, that is, addition is vector addition and multiplication is defined by $ab = (a_1b_1, a_2b_2, \ldots)$. Prove that R is a ring, and determine its maximal ideals.

M.4. **(a)** Classify rings R that contain $\mathbb{C}$ and have dimension 2 as vector space over $\mathbb{C}$.

(b) Do the same for rings that have dimension 3.

M.5. Define $\varphi: \mathbb{C}[x, y] \to \mathbb{C}[x] \times \mathbb{C}[y] \times \mathbb{C}[t]$ by $f(x, y) \rightsquigarrow (f(x, 0), f(0, y), f(t, t))$. Determine the image of this map, and find generators for the kernel.

M.6. Prove that the locus $y = \sin x$ in $\mathbb{R}^2$ doesn't lie on any algebraic curve in $\mathbb{C}^2$.

***M.7.** Let X denote the closed unit interval $[0, 1]$, and let R be the ring of continuous functions $X \to \mathbb{R}$.

(a) Let $f_1, \ldots, f_n$ be functions with no common zero on X. Prove that the ideal generated by these functions is the unit ideal.

Hint: Consider $f_1^2 + \cdots + f_n^2$.

(b) Establish a bijective correspondence between maximal ideals of R and points on the interval.