CHAPTER II

Rings

§1. RINGS AND HOMOMORPHISMS

A **ring** A is a set, together with two laws of composition called multiplication and addition respectively, and written as a product and as a sum respectively, satisfying the following conditions:

RI 1. With respect to addition, A is a commutative group.

RI 2. The multiplication is associative, and has a unit element.

RI 3. For all $x, y, z \in A$ we have

$$(x + y)z = xz + yz \qquad \text{and} \qquad z(x + y) = zx + zy.$$

(This is called **distributivity**.)

As usual, we denote the unit element for addition by 0, and the unit element for multiplication by 1. We do not assume that $1 \neq 0$. We observe that $0x = 0$ for all $x \in A$. *Proof*: We have $0x + x = (0 + 1)x = 1x = x$. Hence $0x = 0$. In particular, if $1 = 0$, then A consists of 0 alone.

For any $x, y \in A$ we have $(-x)y = -(xy)$. *Proof*: We have

$$xy + (-x)y = \big(x + (-x)\big)y = 0y = 0,$$

so $(-x)y$ is the additive inverse of xy.

Other standard laws relating addition and multiplication are easily proved, for instance $(-x)(-y) = xy$. We leave these as exercises.

Let A be a ring, and let U be the set of elements of A which have both a right and left inverse. Then U is a multiplicative group. Indeed, if a has a

S. Lang, *Algebra*

right inverse b, so that $ab = 1$, and a left inverse c, so that $ca = 1$, then $cab = b$, whence $c = b$, and we see that c (or b) is a two-sided inverse, and that c itself has a two-sided inverse, namely a. Therefore U satisfies all the axioms of a multiplicative group, and is called the group of **units** of A. It is sometimes denoted by A^*, and is also called the group of **invertible** elements of A. A ring A such that $1 \neq 0$, and such that every non-zero element is invertible is called a **division ring**.

Note. The elements of a ring which are *left* invertible do not necessarily form a group.

Example. (The Shift Operator). Let E be the set of all sequences

$$a = (a_1, a_2, a_3, \dots)$$

of integers. One can define addition componentwise. Let R be the set of all mappings $f: E \to E$ of E into itself such that $f(a + b) = f(a) + f(b)$. The law of composition is defined to be composition of mappings. Then R is a ring. (Proof?) Let

$$T(a_1, a_2, a_3, \dots) = (0, a_1, a_2, a_3, \dots).$$

Verify that T is left invertible but not right invertible.

A ring A is said to be **commutative** if $xy = yx$ for all $x, y \in A$. A commutative division ring is called a **field**. We observe that by definition, a field contains at least two elements, namely 0 and 1.

A subset B of a ring A is called a **subring** if it is an additive subgroup, if it contains the multiplicative unit, and if $x, y \in B$ implies $xy \in B$. If that is the case, then B itself is a ring, the laws of operation in B being the same as the laws of operation in A.

For example, the **center** of a ring A is the subset of A consisting of all elements $a \in A$ such that $ax = xa$ for all $x \in A$. One sees immediately that the center of A is a subring.

Just as we proved general associativity from the associativity for three factors, one can prove general distributivity. If $x, y_1, \dots, y_n$ are elements of a ring A, then by induction one sees that

$$x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n.$$

If x_i $(i = 1, \dots, n)$ and y_j $(j = 1, \dots, m)$ are elements of A, then it is also easily proved that

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{m} x_i y_j.$$

Furthermore, distributivity holds for subtraction, e.g.

$$x(y_1 - y_2) = xy_1 - xy_2.$$

We leave all the proofs to the reader.

Examples. *Let S be a set and A a ring. Let* $\mathrm{Map}(S, A)$ *be the set of mappings of S into A. Then* $\mathrm{Map}(S, A)$ *is a ring if for $f, g \in$* $\mathrm{Map}(S, A)$ *we define*

$$(fg)(x) = f(x)g(x) \qquad \text{and} \qquad (f + g)(x) = f(x) + g(x)$$

for all $x \in S$. The multiplicative unit is the constant map whose value is the multiplicative unit of A. The additive unit is the constant map whose value is the additive unit of A, namely 0. The verification that $\mathrm{Map}(S, A)$ is a ring under the above laws of composition is trivial and left to the reader.

Let M be an additive abelian group, and let A be the set $\mathrm{End}(M)$ of group-homomorphisms of M into itself. We define addition in A to be the addition of mappings, and we define multiplication to be **composition** of mappings. Then it is trivially verified that A is a ring. Its unit element is of course the identity mapping. In general, A is not commutative.

Readers have no doubt met polynomials over a field previously. These provide a basic example of a ring, and will be defined officially for this book in §3.

Let K be a field. The set of $n \times n$ matrices with components in K is a ring. Its units consist of those matrices which are invertible, or equivalently have a non-zero determinant.

Let S be a set and R the set of real-valued functions on S. Then R is a commutative ring. Its units consist of those functions which are nowhere 0. This is a special case of the ring $\mathrm{Map}(S, A)$ considered above.

The convolution product. We shall now give examples of rings whose product is given by what is called convolution. Let G be a group and let K be a field. Denote by $K[G]$ the set of all formal linear combinations $\alpha = \sum a_x x$ with $x \in G$ and $a_x \in K$, such that all but a finite number of a_x are equal to 0. (See §3, and also Chapter III, §4.) If $\beta = \sum b_x x \in K[G]$, then one can define the product

$$\alpha\beta = \sum_{x \in G} \sum_{y \in G} a_x b_y xy = \sum_{z \in G} \left(\sum_{xy=z} a_x b_y \right) z.$$

With this product, the **group ring** $K[G]$ is a ring, which will be studied extensively in Chapter XVIII when G is a finite group. Note that $K[G]$ is commutative if and only if G is commutative. The second sum on the right above defines what is called a **convolution product**. If f, g are two functions on a group G, we define their **convolution** $f * g$ by

$$(f * g)(z) = \sum_{xy=z} f(x)g(y).$$

Of course this must make sense. If G is infinite, one may restrict this definition to functions which are 0 except at a finite number of elements. Exercise 12 will give an example (actually on a monoid) when another type of restriction allows for a finite sum on the right.

Example from analysis. In analysis one considers a situation as follows. Let $L^1 = L^1(\mathbf{R})$ be the space of functions which are absolutely integrable.

Given functions $f, g \in L^1$, one defines their **convolution product** $f * g$ by

$$(f * g)(x) = \int_{\mathbf{R}} f(x - y)g(y)\,dy.$$

Then this product satisfies all the axioms of a ring, except that there is no unit element. In the case of the group ring or the convolution of Exercise 12, there is a unit element. (What is it?) Note that the convolution product in the case of $L^1(\mathbf{R})$ is commutative, basically because $\mathbf{R}$ is a commutative additive group. More generally, let G be a locally compact group with a Haar measure μ. Then the convolution product is defined by the similar formula

$$(f * g)(x) = \int_G f(xy^{-1})g(y)\,d\mu(y).$$

After these examples, we return to the general theory of rings.

A **left ideal** $\mathfrak{a}$ in a ring A is a subset of A which is a subgroup of the additive group of A, such that $A\mathfrak{a} \subset \mathfrak{a}$ (and hence $A\mathfrak{a} = \mathfrak{a}$ since A contains 1). To define a right ideal, we require $\mathfrak{a}A = \mathfrak{a}$, and a **two-sided ideal** is a subset which is both a left and a right ideal. A two-sided ideal is called simply an **ideal** in this section. Note that (0) and A itself are ideals.

If A is a ring and $a \in A$, then Aa is a left ideal, called **principal**. We say that a is a generator of $\mathfrak{a}$ (over A). Similarly, AaA is a principal two-sided ideal if we define AaA to be the set of all sums $\sum x_i a y_i$ with $x_i, y_i \in A$. Cf. below the definition of the product of ideals. More generally, let $a_1, \ldots, a_n$ be elements of A. We denote by $(a_1, \ldots, a_n)$ the set of elements of A which can be written in the form

$$x_1 a_1 + \cdots + x_n a_n \quad \text{with} \quad x_i \in A.$$

Then this set of elements is immediately verified to be a left ideal, and $a_1, \ldots, a_n$ are called **generators** of the left ideal.

If $\{\mathfrak{a}_i\}_{i \in I}$ is a family of ideals, then their intersection

$$\bigcap_{i \in I} \mathfrak{a}_i$$

is also an ideal. Similarly for left ideals. Readers will easily verify that if $\mathfrak{a} = (a_1, \ldots, a_n)$, then $\mathfrak{a}$ is the intersection of all left ideals containing the elements $a_1, \ldots, a_n$.

A ring A is said to be **commutative** if $xy = yx$ for all $x, y \in A$. In that case, every left or right ideal is two-sided.

A **commutative** ring such that every ideal is principal and such that $1 \neq 0$ is called a **principal** ring.

Examples. The integers $\mathbf{Z}$ form a ring, which is commutative. Let $\mathfrak{a}$ be an ideal $\neq \mathbf{Z}$ and $\neq 0$. If $n \in \mathfrak{a}$, then $-n \in \mathfrak{a}$. Let d be the smallest integer > 0 lying in $\mathfrak{a}$. If $n \in \mathfrak{a}$ then there exist integers q, r with $0 \leqq r < d$ such that

$$n = dq + r.$$

Since $\mathfrak{a}$ is an ideal, it follows that r lies in $\mathfrak{a}$, hence $r = 0$. Hence $\mathfrak{a}$ consists of all multiples qd of d, with $q \in \mathbf{Z}$, and $\mathbf{Z}$ *is a principal ring.*

A similar example is the ring of polynomials in one variable over a field, as will be proved in Chapter IV, also using the Euclidean algorithm.

Let R be the ring of algebraic integers in a number field K. (For definitions, see Chapter VII.) Then R is not necessarily principal, but let $\mathfrak{p}$ be a prime ideal, and let $R_{\mathfrak{p}}$ be the ring of all elements a/b with $a, b \in R$ and $b \notin \mathfrak{p}$. Then in algebraic number theory, it is shown that $R_{\mathfrak{p}}$ is principal, with one prime ideal $\mathfrak{m}_{\mathfrak{p}}$ consisting of all elements a/b as above but with $a \in \mathfrak{p}$. See Exercises 15, 16, and 17.

An example from analysis. Let A be the set of entire functions on the complex plane. Then A is a commutative ring, and every finitely generated ideal is principal. Given a discrete set of complex numbers $\{z_i\}$ and integers $m_i \geqq 0$, there exists an entire function f having zeros at z_i of multiplicity m_i and no other zeros. Every principal ideal is of the form Af for some such f. The group of units A^* in A consists of the functions which have no zeros. It is a nice exercise in analysis to prove the above statements (using the Weierstrass factorization theorem).

We now return to general notions. Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals of A. We define $\mathfrak{ab}$ to be the set of all sums

$$x_1 y_1 + \cdots + x_n y_n$$

with $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{b}$. Then one verifies immediately that $\mathfrak{ab}$ is an ideal, and that the set of ideals forms a multiplicative monoid, the unit element being the ring itself. This unit element is called the **unit ideal**, and is often written (1). If $\mathfrak{a}$, $\mathfrak{b}$ are left ideals, we define their product $\mathfrak{ab}$ as above. It is also a left ideal, and if $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are left ideals, then we again have associativity: $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$.

If $\mathfrak{a}$, $\mathfrak{b}$ are left ideals of A, then $\mathfrak{a} + \mathfrak{b}$ (the sum being taken as additive subgroup of A) is obviously a left ideal. Similarly for right and two-sided ideals. Thus ideals also form a monoid under addition. We also have distributivity: If $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $\mathfrak{b}$ are ideals of A, then clearly

$$\mathfrak{b}(\mathfrak{a}_1 + \cdots + \mathfrak{a}_n) = \mathfrak{b}\mathfrak{a}_1 + \cdots + \mathfrak{b}\mathfrak{a}_n,$$

and similarly on the other side. (However, the set of ideals does not form a ring!)

Let $\mathfrak{a}$ be a left ideal. Define $\mathfrak{a}A$ to be the set of all sums $a_1 x_1 + \cdots + a_n x_n$ with $a_i \in \mathfrak{a}$ and $x_i \in A$. Then $\mathfrak{a}A$ is an ideal (two-sided).

Suppose that A is commutative. Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals. Then trivially

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b},$$

but equality does not necessarily hold. However, as an exercise, prove that if $\mathfrak{a} + \mathfrak{b} = A$ then $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

As should be known to the reader, the integers $\mathbf{Z}$ satisfy another property besides every ideal being principal, namely unique factorization into primes.

We shall discuss the general phenomenon in §4. Be it noted here only that if a ring A has the property of unique factorization into prime elements, and p is a prime element, then the ideal (p) is prime, and the ring $R_{(p)}$ (defined as above) is principal. See Exercise 6. Thus principal rings may be obtained in a natural way from rings which are not principal.

As Dedekind found out, some form of unique factorization can be recovered in some cases, replacing unique factorization into prime elements by unique factorization of (non-zero) ideals into prime ideals.

Example. There are cases when the non-zero ideals give rise to a group. Let $\mathfrak{o}$ be a subring of a field K such that every element of K is a quotient of elements of $\mathfrak{o}$; that is, of the form a/b with $a, b \in \mathfrak{o}$ and $b \neq 0$. By a **fractional ideal** $\mathfrak{a}$ we mean a non-zero additive subgroup of K such that $\mathfrak{o}\mathfrak{a} \subset \mathfrak{a}$ (and therefore $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ since $\mathfrak{o}$ contains the unit element); and such that there exists an element $c \in \mathfrak{o}$, $c \neq 0$, such that $c\mathfrak{a} \subset \mathfrak{o}$. We might say that a fractional ideal has bounded denominator. A **Dedekind ring** is a ring $\mathfrak{o}$ as above such that the fractional ideals form a group under multiplication. As proved in books on algebraic number theory, the ring of algebraic integers in a number field is a Dedekind ring. Do Exercise 14 to get the property of unique factorization into prime ideals. See Exercise 7 of Chapter VII for a sketch of this proof.

If $a \in K$, $a \neq 0$, then $\mathfrak{o}a$ is a fractional ideal, and such ideals are called **principal**. The principal fractional ideals form a subgroup. The factor group is called the **ideal class group**, or **Picard group** of $\mathfrak{o}$, and is denoted by Pic($\mathfrak{o}$). See Exercises 13–19 for some elementary facts about Dedekind rings. It is a basic problem to determine Pic($\mathfrak{o}$) for various Dedekind rings arising in algebraic number theory and function theory. See my book *Algebraic Number Theory* for the beginnings of the theory in number fields. In the case of function theory, one is led to questions in algebraic geometry, notably the study of groups of divisor classes on algebraic varieties and all that this entails. The property that the fractional ideals form a group is essentially associated with the ring having "dimension 1" (which we do not define here). In general one is led into the study of modules under various equivalence relations; see for instance the comments at the end of Chapter III, §4.

We return to the general theory of rings.

By a **ring-homomorphism** one means a mapping $f: A \to B$ where A, B are rings, and such that f is a monoid-homomorphism for the multiplicative structures on A and B, and also a monoid-homomorphism for the additive structure. In other words, f must satisfy:

$$f(a + a') = f(a) + f(a'), \qquad f(aa') = f(a)f(a'),$$
$$f(1) = 1, \qquad f(0) = 0,$$

for all $a, a' \in A$. Its **kernel** is defined to be the kernel of f viewed as additive homomorphism.

The kernel of a ring-homomorphism $f: A \to B$ is an ideal of A, as one verifies at once.

Conversely, let $\mathfrak{a}$ be an ideal of the ring A. We can construct the **factor ring** $A/\mathfrak{a}$ as follows. Viewing A and $\mathfrak{a}$ as additive groups, let $A/\mathfrak{a}$ be the factor group. We define a multiplicative law of composition on $A/\mathfrak{a}$: If $x + \mathfrak{a}$ and $y + \mathfrak{a}$ are two cosets of $\mathfrak{a}$, we define $(x + \mathfrak{a})(y + \mathfrak{a})$ to be the coset $(xy + \mathfrak{a})$. This coset is well defined, for if x_1, y_1 are in the same coset as x, y respectively, then one verifies at once that $x_1 y_1$ is in the same coset as xy. Our multiplicative law of composition is then obviously associative, has a unit element, namely the coset $1 + \mathfrak{a}$, and the distributive law is satisfied since it is satisfied for coset representatives. We have therefore defined a ring structure on $A/\mathfrak{a}$, and the canonical map

$$f: A \to A/\mathfrak{a}$$

is then clearly a ring-homomorphism.

If $g: A \to A'$ is a ring-homomorphism whose kernel contains $\mathfrak{a}$, then there exists a unique ring-homomorphism $g_*: A/\mathfrak{a} \to A'$ making the following diagram commutative:

$$\begin{tikzcd}
A \arrow[rr, "g"] \arrow[dr, "f"'] & & A' \\
& A/\mathfrak{a} \arrow[ur, "g_*"'] &
\end{tikzcd}$$

Indeed, viewing f, g as group-homomorphisms (for the additive structures), there is a unique group-homomorphism g_* making our diagram commutative. We contend that g_* is in fact a ring-homomorphism. We could leave the trivial proof to the reader, but we carry it out in full. If $x \in A$, then $g(x) = g_* f(x)$. Hence for $x, y \in A$,

$$\begin{aligned} g_*(f(x)f(y)) &= g_*(f(xy)) = g(xy) = g(x)g(y) \\ &= g_* f(x) g_* f(y). \end{aligned}$$

Given $\xi, \eta \in A/\mathfrak{a}$, there exist $x, y \in A$ such that $\xi = f(x)$ and $\eta = f(y)$. Since $f(1) = 1$, we get $g_* f(1) = g(1) = 1$, and hence the two conditions that g_* be a multiplicative monoid-homomorphism are satisfied, as was to be shown.

The statement we have just proved is equivalent to saying that the canonical map $f: A \to A/\mathfrak{a}$ is universal in the category of homomorphisms whose kernel contains $\mathfrak{a}$.

Let A be a ring, and denote its unit element by e for the moment. The map

$$\lambda: \mathbf{Z} \to A$$

such that $\lambda(n) = ne$ is a ring-homomorphism (obvious), and its kernel is an ideal (n), generated by an integer $n \geqq 0$. We have a canonical injective homomorphism $\mathbf{Z}/n\mathbf{Z} \to A$, which is a (ring) isomorphism between $\mathbf{Z}/n\mathbf{Z}$ and a subring of A. If $n\mathbf{Z}$ is a prime ideal, then $n = 0$ or $n = p$ for some prime number p. In the first case, A contains as a subring a ring which is isomorphic to $\mathbf{Z}$, and which is often identified with $\mathbf{Z}$. In that case, we say that A has **characteristic** 0. If on the other hand $n = p$, then we say that A has **characteristic** p, and A contains (an isomorphic image of) $\mathbf{Z}/p\mathbf{Z}$ as a subring. We abbreviate $\mathbf{Z}/p\mathbf{Z}$ by $\mathbf{F}_p$.

If K is a field, then K has characteristic 0 or $p > 0$. In the first case, K contains as a subfield an isomorphic image of the rational numbers, and in the second case, it contains an isomorphic image of $\mathbf{F}_p$. In either case, this subfield will be called the **prime field** (contained in K). Since this prime field is the smallest subfield of K containing 1 and has no automorphism except the identity, it is customary to identify it with $\mathbf{Q}$ or $\mathbf{F}_p$ as the case may be. By the **prime ring** (in K) we shall mean either the integers $\mathbf{Z}$ if K has characteristic 0, or $\mathbf{F}_p$ if K has characteristic p.

Let A be a subring of a ring B. Let S be a subset of B commuting with A; in other words we have $as = sa$ for all $a \in A$ and $s \in S$. We denote by $A[S]$ the set of all elements

$$\sum a_{i_1 \cdots i_n} s_1^{i_1} \cdots s_n^{i_n},$$

the sum ranging over a finite number of n-tuples $(i_1, \ldots, i_n)$ of integers $\geqq 0$, and $a_{i_1 \cdots i_n} \in A$, $s_1, \ldots, s_n \in S$. If $B = A[S]$, we say that S is a set of **generators** (or more precisely, **ring generators**) for B over A, or that B is **generated** by S over A. If S is finite, we say that B is **finitely generated as a ring over** A. One might say that $A[S]$ consists of all not-necessarily-commutative polynomials in elements of S with coefficients in A. Note that elements of S may not commute with each other.

Example. The ring of matrices over a field is finitely generated over that field, but matrices don't necessarily commute.

As with groups, we observe that a homomorphism is uniquely determined by its effect on generators. In other words, let $f: A \to A'$ be a ring-homomorphism, and let $B = A[S]$ as above. Then there exists at most one extension of f to a ring-homomorphism of B having prescribed values on S.

Let A be a ring, $\mathfrak{a}$ an ideal, and S a subset of A. We write

$$S \equiv 0 \pmod{\mathfrak{a}}$$

if $S \subset \mathfrak{a}$. If $x, y \in A$, we write

$$x \equiv y \pmod{\mathfrak{a}}$$

if $x - y \in \mathfrak{a}$. If $\mathfrak{a}$ is principal, equal to (a), then we also write

$$x \equiv y \pmod{a}.$$

If $f: A \to A/\mathfrak{a}$ is the canonical homomorphism, then $x \equiv y \pmod{\mathfrak{a}}$ means that $f(x) = f(y)$. The congruence notation is sometimes convenient when we want to avoid writing explicitly the canonical map f.

The factor ring $A/\mathfrak{a}$ is also called a **residue class ring**. Cosets of $\mathfrak{a}$ in A are called **residue classes** modulo $\mathfrak{a}$, and if $x \in A$, then the coset $x + \mathfrak{a}$ is called the **residue class of x modulo** $\mathfrak{a}$.

We have defined the notion of an isomorphism in any category, and so a ring-isomorphism is a ring-homomorphism which has a two-sided inverse. As usual we have the criterion:

A ring-homomorphism $f: A \to B$ which is bijective is an isomorphism.

Indeed, there exists a set-theoretic inverse $g: B \to A$, and it is trivial to verify that g is a ring-homomorphism.

Instead of saying "ring-homomorphism" we sometimes say simply "homomorphism" if the reference to rings is clear. We note that rings form a category (the morphisms being the homomorphisms).

Let $f: A \to B$ be a ring-homomorphism. Then the image $f(A)$ of f is a subring of B. Proof obvious.

It is clear that an injective ring-homomorphism $f: A \to B$ establishes a ring-isomorphism between A and its image. Such a homomorphism will be called an **embedding** (of rings).

Let $f: A \to A'$ be a ring-homomorphism, and let $\mathfrak{a}'$ be an ideal of A'. Then $f^{-1}(\mathfrak{a}')$ is an ideal $\mathfrak{a}$ in A, and we have an induced injective homomorphism

$$A/\mathfrak{a} \to A'/\mathfrak{a}'.$$

The trivial proof is left to the reader.

Proposition 1.1. *Products exist in the category of rings.*

In fact, let $\{A_i\}_{i \in I}$ be a family of rings, and let $A = \prod A_i$ be their product as additive abelian groups. We define a multiplication in A in the obvious way: If $(x_i)_{i \in I}$ and $(y_i)_{i \in I}$ are two elements of A, we define their product to be $(x_i y_i)_{i \in I}$, i.e. we define multiplication componentwise, just as we did for addition. The multiplicative unit is simply the element of the product whose i-th component is the unit element of A_i. It is then clear that we obtain a ring structure on A, and that the projection on the i-th factor is a ring-homomorphism. Furthermore, A together with these projections clearly satisfies the required universal property.

Note that the usual inclusion of A_i on the i-th factor is *not* a ring-homomorphism because it does not map the unit element e_i of A_i on the unit element of A. Indeed, it maps e_i on the element of A having e_i as i-th component, and 0 $(= 0_i)$ as all other components.

Let A be a ring. Elements x, y of A are said to be **zero divisors** if $x \neq 0$, $y \neq 0$, and $xy = 0$. Most of the rings without zero divisors which we consider will be commutative. In view of this, we define a ring A to be **entire** if $1 \neq 0$, if A is commutative, and if there are no zero divisors in the ring. (Entire rings are also called **integral domains**. However, linguistically, I feel the need for an adjective. "Integral" would do, except that in English, "integral" has been used for "integral over a ring" as in Chapter VII, §1. In French, as in English, two words exist with similar roots: "integral" and "entire". The French have used both words. Why not do the same in English? There is a slight psychological impediment, in that it would have been better if the use of "integral" and "entire" were reversed to fit the long-standing French use. I don't know what to do about this.)

Examples. The ring of integers $\mathbf{Z}$ is without zero divisors, and is therefore entire. If S is a set with at least 2 elements, and A is a ring with $1 \neq 0$, then the ring of mappings $\mathrm{Map}(S, A)$ has zero divisors. (Proof?)

Let m be a positive integer $\neq 1$. The ring $\mathbf{Z}/m\mathbf{Z}$ has zero divisors if and only if m is not a prime number. (Proof left as an exercise.) The ring of $n \times n$ matrices over a field has zero divisors if $n \geqq 2$. (Proof?)

The next criterion is used very frequently.

Let A be an entire ring, and let a, b be non-zero elements of A. Then a, b generate the same ideal if and only if there exists a unit u of A such that $b = au$.

Proof. If such a unit exists we have $Ab = Aua = Aa$. Conversely, assume $Aa = Ab$. Then we can write $a = bc$ and $b = ad$ with some elements $c, d \in A$. Hence $a = adc$, whence $a(1 - dc) = 0$, and therefore $dc = 1$. Hence c is a unit.

§2. COMMUTATIVE RINGS

Throughout this section, we let A denote a commutative ring.

A **prime** ideal in A is an ideal $\mathfrak{p} \neq A$ such that $A/\mathfrak{p}$ is entire. Equivalently, we could say that it is an ideal $\mathfrak{p} \neq A$ such that, whenever $x, y \in A$ and $xy \in \mathfrak{p}$, then $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. A prime ideal is often called simply a **prime**.

Let $\mathfrak{m}$ be an ideal. We say that $\mathfrak{m}$ is a **maximal** ideal if $\mathfrak{m} \neq A$ and if there is no ideal $\mathfrak{a} \neq A$ containing $\mathfrak{m}$ and $\neq \mathfrak{m}$.

Every maximal ideal is prime.

Proof. Let $\mathfrak{m}$ be maximal and let $x, y \in A$ be such that $xy \in \mathfrak{m}$. Suppose $x \notin \mathfrak{m}$. Then $\mathfrak{m} + Ax$ is an ideal properly containing $\mathfrak{m}$, hence equal to A. Hence we can write

$$1 = u + ax$$

with $u \in \mathfrak{m}$ and $a \in A$. Multiplying by y we find

$$y = yu + axy,$$

whence $y \in \mathfrak{m}$ and $\mathfrak{m}$ is therefore prime.

Let $\mathfrak{a}$ be an ideal $\neq A$. Then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$.

Proof. The set of ideals containing $\mathfrak{a}$ and $\neq A$ is inductively ordered by ascending inclusion. Indeed, if $\{\mathfrak{b}_i\}$ is a totally ordered set of such ideals, then $1 \notin \mathfrak{b}_i$ for any i, and hence 1 does not lie in the ideal $\mathfrak{b} = \bigcup \mathfrak{b}_i$, which dominates all $\mathfrak{b}_i$. If $\mathfrak{m}$ is a maximal element in our set, then $\mathfrak{m} \neq A$ and $\mathfrak{m}$ is a maximal ideal, as desired.

The ideal $\{0\}$ is a prime ideal of A if and only if A is entire.

(Proof obvious.)

We defined a **field** K to be a commutative ring such that $1 \neq 0$, and such that the multiplicative monoid of non-zero elements of K is a group (i.e. such that whenever $x \in K$ and $x \neq 0$ then there exists an inverse for x). We note that the only ideals of a field K are K and the zero ideal.

If $\mathfrak{m}$ is a maximal ideal of A, then $A/\mathfrak{m}$ is a field.

Proof. If $x \in A$, we denote by $\bar{x}$ its residue class mod $\mathfrak{m}$. Since $\mathfrak{m} \neq A$ we note that $A/\mathfrak{m}$ has a unit element $\neq 0$. Any non-zero element of $A/\mathfrak{m}$ can be written as $\bar{x}$ for some $x \in A$, $x \notin \mathfrak{m}$. To find its inverse, note that $\mathfrak{m} + Ax$ is an ideal of $A \neq \mathfrak{m}$ and hence equal to A. Hence we can write

$$1 = u + yx$$

with $u \in \mathfrak{m}$ and $y \in A$. This means that $\bar{y}\bar{x} = 1$ (i.e. $= \bar{1}$) and hence that $\bar{x}$ has an inverse, as desired.

Conversely, we leave it as an exercise to the reader to prove that:

If $\mathfrak{m}$ is an ideal of A such that $A/\mathfrak{m}$ is a field, then $\mathfrak{m}$ is maximal.

Let $f: A \to A'$ be a homomorphism of commutative rings. Let $\mathfrak{p}'$ be a prime ideal of A', and let $\mathfrak{p} = f^{-1}(\mathfrak{p}')$. Then $\mathfrak{p}$ is prime.

To prove this, let $x, y \in A$, and $xy \in \mathfrak{p}$. Suppose $x \notin \mathfrak{p}$. Then $f(x) \notin \mathfrak{p}'$. But $f(x)f(y) = f(xy) \in \mathfrak{p}'$. Hence $f(y) \in \mathfrak{p}'$, as desired.

As an exercise, prove that if f is surjective, and if $\mathfrak{m}'$ is maximal in A', then $f^{-1}(\mathfrak{m}')$ is maximal in A.

Example. Let $\mathbf{Z}$ be the ring of integers. Since an ideal is also an additive subgroup of $\mathbf{Z}$, every ideal $\neq \{0\}$ is principal, of the form $n\mathbf{Z}$ for some integer $n > 0$ (uniquely determined by the ideal). Let $\mathfrak{p}$ be a prime ideal $\neq \{0\}$, $\mathfrak{p} = n\mathbf{Z}$. Then n must be a prime number, as follows essentially directly from the definition of a prime ideal. Conversely, if p is a prime number, then $p\mathbf{Z}$ is a prime ideal (trivial exercise). Furthermore, $p\mathbf{Z}$ is a maximal ideal. Indeed, suppose $p\mathbf{Z}$ contained in some ideal $n\mathbf{Z}$. Then $p = nm$ for some integer m, whence $n = p$ or $n = 1$, thereby proving $p\mathbf{Z}$ maximal.

If n is an integer, the factor ring $\mathbf{Z}/n\mathbf{Z}$ is called the ring of **integers modulo** n. We also denote

$$\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}(n).$$

If n is a prime number p, then the ring of integers modulo p is in fact a field, denoted by $\mathbf{F}_p$. In particular, the multiplicative group of $\mathbf{F}_p$ is called the group of non-zero integers modulo p. From the elementary properties of groups, we get a standard fact of elementary number theory: If x is an integer $\not\equiv 0 \pmod{p}$, then $x^{p-1} \equiv 1 \pmod{p}$. (For simplicity, it is customary to write mod p instead of mod $p\mathbf{Z}$, and similarly to write mod n instead of mod $n\mathbf{Z}$ for any integer n.) Similarly, given an integer $n > 1$, the units in the ring $\mathbf{Z}/n\mathbf{Z}$ consist of those residue classes mod $n\mathbf{Z}$ which are represented by integers $m \neq 0$ and prime to n. The order of the group of units in $\mathbf{Z}/n\mathbf{Z}$ is called by definition $\varphi(n)$ (where φ is known as the **Euler phi-function**). Consequently, if x is an integer prime to n, then $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Theorem 2.1. (Chinese Remainder Theorem). *Let* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *be ideals of* A *such that* $\mathfrak{a}_i + \mathfrak{a}_j = A$ *for all* $i \neq j$. *Given elements* $x_1, \ldots, x_n \in A$, *there exists* $x \in A$ *such that* $x \equiv x_i \pmod{\mathfrak{a}_i}$ *for all* i.

Proof. If $n = 2$, we have an expression

$$1 = a_1 + a_2$$

for some elements $a_i \in \mathfrak{a}_i$, and we let $x = x_2 a_1 + x_1 a_2$.
For each $i \geqq 2$ we can find elements $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_i$ such that

$$a_i + b_i = 1, \qquad i \geqq 2.$$

The product $\prod_{i=2}^{n} (a_i + b_i)$ is equal to 1, and lies in

$$\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i,$$

i.e. in $\mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n$. Hence

$$\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i = A.$$

By the theorem for $n = 2$, we can find an element $y_1 \in A$ such that

$$y_1 \equiv 1 \pmod{\mathfrak{a}_1},$$

$$y_1 = 0 \left(\operatorname{mod} \prod_{i=2}^{n} \mathfrak{a}_i\right).$$

We find similarly elements $y_2, \ldots, y_n$ such that

$$y_j \equiv 1 \pmod{\mathfrak{a}_j} \qquad \text{and} \qquad y_j \equiv 0 \pmod{\mathfrak{a}_i} \qquad \text{for } i \neq j.$$

Then $x = x_1 y_1 + \cdots + x_n y_n$ satisfies our requirements.

In the same vein as above, we observe that if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals of a ring A such that

$$\mathfrak{a}_1 + \cdots + \mathfrak{a}_n = A,$$

and if $\nu_1, \ldots, \nu_n$ are positive integers, then

$$\mathfrak{a}_1^{\nu_1} + \cdots + \mathfrak{a}_n^{\nu_n} = A.$$

The proof is trivial, and is left as an exercise.

Corollary 2.2. *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of A. Assume that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for $i \neq j$. Let*

$$f\colon A \to \prod_{i=1}^{n} A/\mathfrak{a}_i = (A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$$

be the map of A into the product induced by the canonical map of A onto $A/\mathfrak{a}_i$ for each factor. Then the kernel of f is $\bigcap_{i=1}^{n} \mathfrak{a}_i$, and f is surjective, thus giving an isomorphism

$$A/\bigcap \mathfrak{a}_i \xrightarrow{\approx} \prod A/\mathfrak{a}_i.$$

Proof. That the kernel of f is what we said it is, is obvious. The surjectivity follows from the theorem.

The theorem and its corollary are frequently applied to the ring of integers $\mathbf{Z}$ and to distinct prime ideals $(p_1), \ldots, (p_n)$. These satisfy the hypothesis of the theorem since they are maximal. Similarly, one could take integers $m_1, \ldots, m_n$ which are relatively prime in pairs, and apply the theorem to the principal ideals $(m_1) = m_1\mathbf{Z}, \ldots, (m_n) = m_n\mathbf{Z}$. This is the ultraclassical case of the Chinese remainder theorem.

In particular, let m be an integer > 1, and let

$$m = \prod_i p_i^{r_i}$$

be a factorization of m into primes, with exponents $r_i \geqq 1$. Then we have a ring-isomorphism:

$$\mathbf{Z}/m\mathbf{Z} \approx \prod_i \mathbf{Z}/p_i^{r_i}\mathbf{Z}.$$

If A is a ring, we denote as usual by A^* the multiplicative group of invertible elements of A. We leave the following assertions as exercises:

The preceding ring-isomorphism of $\mathbf{Z}/m\mathbf{Z}$ onto the product induces a group-isomorphism

$$(\mathbf{Z}/m\mathbf{Z})^* \approx \prod_i (\mathbf{Z}/p_i^{r_i}\mathbf{Z})^*.$$

In view of our isomorphism, we have

$$\varphi(m) = \prod_i \varphi(p_i^{r_i}).$$

If p is a prime number and r an integer $\geqq 1$, then

$$\varphi(p^r) = (p-1)p^{r-1}.$$

One proves this last formula by induction. If $r = 1$, then $\mathbf{Z}/p\mathbf{Z}$ is a field, and the multiplicative group of that field has order $p - 1$. Let r be $\geqq 1$, and consider the canonical ring-homomorphism

$$\mathbf{Z}/p^{r+1}\mathbf{Z} \to \mathbf{Z}/p^r\mathbf{Z},$$

arising from the inclusion of ideals $(p^{r+1}) \subset (p^r)$. We get an induced group-homomorphism

$$\lambda\colon (\mathbf{Z}/p^{r+1}\mathbf{Z})^* \to (\mathbf{Z}/p^r\mathbf{Z})^*,$$

which is surjective because any integer a which represents an element of $\mathbf{Z}/p^r\mathbf{Z}$ and is prime to p will represent an element of $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$. Let a be an integer representing an element of $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$, such that $\lambda(a) = 1$. Then

$$a \equiv 1 \pmod{p^r\mathbf{Z}},$$

and hence we can write

$$a \equiv 1 + xp^r \pmod{p^{r+1}\mathbf{Z}}$$

for some $x \in \mathbf{Z}$. Letting $x = 0, 1, \ldots, p-1$ gives rise to p distinct elements of $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$, all of which are in the kernel of λ. Furthermore, the element x above can be selected to be one of these p integers because every integer is congruent to one of these p integers modulo (p). Hence the kernel of λ has order p, and our formula is proved.

Note that the kernel of λ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$. (Proof?)

Application: The ring of endomorphisms of a cyclic group. One of the first examples of a ring is the ring of endomorphisms of an abelian group. In the case of a cyclic group, we have the following complete determination.

Theorem 2.3. *Let A be a cyclic group of order n. For each $k \in \mathbf{Z}$ let $f_k\colon A \to A$ be the endomorphism $x \mapsto kx$ (writing A additively). Then $k \mapsto f_k$ induces a ring isomorphism $\mathbf{Z}/n\mathbf{Z} \approx \mathrm{End}(A)$, and a group isomorphism $(\mathbf{Z}/n\mathbf{Z})^* \approx \mathrm{Aut}(A)$.*

Proof. Recall that the additive group structure on End(A) is simply addition of mappings, and the multiplication is composition of mappings. The fact that $k \mapsto f_k$ is a ring-homomorphism is then a restatement of the formulas

$$1a = a, \qquad (k + k')a = ka + k'a, \qquad \text{and} \qquad (kk')a = k(k'a)$$

for $k, k' \in \mathbf{Z}$ and $a \in A$. If a is a generator of A, then $ka = 0$ if and only if $k \equiv 0 \bmod n$, so $\mathbf{Z}/n\mathbf{Z}$ is embedded in End(A). On the other hand, let $f\colon A \to A$ be an endomorphism. Again for a generator a, we have $f(a) = ka$

for some k, whence $f = f_k$ since every $x \in A$ is of the form ma for some $m \in Z$, and

$$f(x) = f(ma) = mf(a) = mka = kma = kx.$$

This proves the isomorphism $\mathbf{Z}/n\mathbf{Z} \approx \operatorname{End}(A)$. Furthermore, if $k \in (\mathbf{Z}/n\mathbf{Z})^*$ then there exists k' such that $kk' \equiv 1 \bmod n$, so f_k has the inverse $f_{k'}$ and f_k is an automorphism. Conversely, given any automorphism f with inverse g, we know from the first part of the proof that $f = f_k$, $g = g_{k'}$ for some k, k', and $f \circ g = \text{id}$ means that $kk' \equiv 1 \bmod n$, so k, $k' \in (\mathbf{Z}/n\mathbf{Z})^*$. This proves the isomorphism $(\mathbf{Z}/n\mathbf{Z})^* \approx \operatorname{Aut}(A)$.

Note that if A is written as a multiplicative group C, then the map f_k is given by $x \mapsto x^k$. For instance, let $\boldsymbol{\mu}_n$ be the group of n-th roots of unity in $\mathbf{C}$. Then all automorphisms of $\boldsymbol{\mu}_n$ are given by

$$\zeta \mapsto \zeta^k \qquad \text{with} \quad k \in (\mathbf{Z}/n\mathbf{Z})^*.$$

§3. POLYNOMIALS AND GROUP RINGS

Although all readers will have met polynomial functions, this section lays the ground work for polynomials in general. One needs polynomials over arbitrary rings in many contexts. For one thing, there are polynomials over a finite field which cannot be identified with polynomial functions in that field. One needs polynomials with integer coefficients, and one needs to reduce these polynomials mod p for primes p. One needs polynomials over arbitrary commutative rings, both in algebraic geometry and in analysis, for instance the ring of polynomial differential operators. We also have seen the example of a ring $B = A[S]$ generated by a set of elements over a ring A. We now give a systematic account of the basic definitions of polynomials over a commutative ring A.

We want to give a meaning to an expression such as

$$a_0 + a_1X + \cdots + a_nX^n,$$

where $a_i \in A$ and X is a "variable". There are several devices for doing so, and we pick one of them. (I picked another in my *Undergraduate Algebra*.) Consider an infinite cyclic group generated by an element X. We let S be the subset consisting of powers X^r with $r \geqq 0$. Then S is a monoid. We define the set of **polynomials** $A[X]$ to be the set of functions $S \to A$ which are equal to 0 except for a finite number of elements of S. For each element $a \in A$ we denote by aX^n the function which has the value a on X^n and the value 0 for all other elements of S. Then it is immediate that a polynomial can be written uniquely as a finite sum

$$a_0X^0 + \cdots + a_nX^n$$

for some integer $n \in \mathbf{N}$ and $a_i \in A$. Such a polynomial is denoted by $f(X)$. The elements $a_i \in A$ are called the **coefficients** of f. We define the product according to the convolution rule. Thus, given polynomials

$$f(X) = \sum_{i=0}^{n} a_iX^i \qquad \text{and} \qquad g(X) = \sum_{j=0}^{m} b_jX^j$$

we define the product to be

$$f(X)g(X) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_ib_j \right) X^k.$$

It is immediately verified that this product is associative and distributive. We shall give the details of associativity in the more general context of a monoid ring below. Observe that there is a unit element, namely $1X^0$. There is also an embedding

$$A \to A[X] \qquad \text{given by} \qquad a \mapsto aX^0.$$

One usually does not distinguish a from its image in $A[X]$, and one writes a instead of aX^0. Note that for $c \in A$ we have then $cf(x) = \sum ca_iX^i$.

Observe that by our definition, we have an equality of polynomials

$$\sum a_iX^i = \sum b_iX^i$$

if and only if $a_i = b_i$ for all i.

Let A be a subring of a commutative ring B. Let $x \in B$. If $f \in A[X]$ is a polynomial, we may then define the associated **polynomial function**

$$f_B \colon B \to B$$

by letting

$$f_B(x) = f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

Given an element $b \in B$, directly from the definition of multiplication of polynomials, we find:

The association

$$\mathrm{ev}_b \colon f \mapsto f(b)$$

is a ring homomorphism of $A[X]$ into B.

This homomorphism is called the **evaluation homomorphism**, and is also said to be obtained by **substituting** b for X in the polynomial. (Cf. Proposition 3.1 below.)

Let $x \in B$. We now see that the subring $A[x]$ of B generated by x over A is the ring of all polynomial values $f(x)$, for $f \in A[X]$. If the evaluation map $f \mapsto f(x)$ gives an isomorphism of $A[X]$ with $A[x]$, then we say that x is

transcendental over A, or that x is a **variable** over A. In particular, X is a variable over A.

Example. Let $\alpha = \sqrt{2}$. Then the set of all real numbers of the form $a + b\alpha$, with $a, b \in \mathbf{Z}$, is a subring of the real numbers, generated by $\sqrt{2}$. Note that α is not transcendental over $\mathbf{Z}$, because the polynomial $X^2 - 2$ lies in the kernel of the evaluation map $f \mapsto f(\sqrt{2})$. On the other hand, it can be shown that $e = 2.718\ldots$ and π are transcendental over $\mathbf{Q}$. See Appendix 1.

Example. Let p be a prime number and let $K = \mathbf{Z}/p\mathbf{Z}$. Then K is a field. Let $f(X) = X^p - X \in K[X]$. Then f is not the zero polynomial. But f_K is the zero function. Indeed, $f_K(0) = 0$. If $x \in K$, $x \neq 0$, then since the multiplicative group of K has order $p - 1$, it follows that $x^{p-1} = 1$, whence $x^p = x$, so $f(x) = 0$. Thus a non-zero polynomial gives rise to the zero function on K.

There is another homomorphism of the polynomial ring having to do with the coefficients. Let

$$\varphi\colon A \to B$$

be a homomorphism of commutative rings. Then there is an associated homomorphism of the polynomial rings $A[X] \to B[X]$, such that

$$f(X) = \sum a_i X^i \mapsto \sum \varphi(a_i) X^i = (\varphi f)(X).$$

The verification that this mapping is a homomorphism is immediate, and further details will be given below in Proposition 3.2, in a more general context. We call $f \mapsto \varphi f$ the **reduction map**.

Examples. In some applications the map φ may be an isomorphism. For instance, if $f(X)$ has complex coefficients, then its complex conjugate $\bar{f}(X) = \sum \bar{a}_i X^i$ is obtained by applying complex conjugation to its coefficients.

Let $\mathfrak{p}$ be a prime ideal of A. Let $\varphi\colon A \to A'$ be the canonical homomorphism of A onto $A/\mathfrak{p}$. If $f(X)$ is a polynomial in $A[X]$, then φf will sometimes be called the **reduction of f modulo $\mathfrak{p}$**.

For example, taking $A = \mathbf{Z}$ and $\mathfrak{p} = (p)$ where p is a prime number, we can speak of the polynomial $3X^4 - X + 2$ as a polynomial mod 5, viewing the coefficients $3, -1, 2$ as integers mod 5, i.e. elements of $\mathbf{Z}/5\mathbf{Z}$.

We may now combine the evaluation map and the reduction map to generalize the evaluation map.

Let $\varphi\colon A \to B$ be a homomorphism of commutative rings.
Let $x \in B$. There is a unique homomorphism extending φ

$$A[X] \to B \qquad \textit{such that} \qquad X \mapsto x,$$

and for this homomorphism, $\sum a_i X^i \mapsto \sum \varphi(a_i) x^i$.

The homomorphism of the above statement may be viewed as the composite

$$A[X] \longrightarrow B[X] \xrightarrow{\text{ev}_x} B$$

where the first map applies φ to the coefficients of a polynomial, and the second map is the evaluation at x previously discussed.

Example. In Chapter IX, §2 and §3, we shall discuss such a situation in several variables, when $(\varphi f)(x) = 0$, in which case x is called a **zero** of the polynomial f.

When writing a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i$, if $a_n \neq 0$ then we define n to be the **degree** of f. Thus the degree of f is the smallest integer n such that $a_r = 0$ for $r > n$. If $f = 0$ (i.e. f is the zero polynomial), then by convention we define the degree of f to be $-\infty$. We agree to the convention that

$$-\infty + -\infty = -\infty, \qquad -\infty + n = -\infty, \qquad -\infty < n,$$

for all $n \in \mathbf{Z}$, and no other operation with $-\infty$ is defined. A polynomial of degree 1 is also called a **linear** polynomial. If $f \neq 0$ and $\deg f = n$, then we call a_n the **leading coefficient** of f. We call a_0 its **constant term.**

Let

$$g(X) = b_0 + \cdots + b_m X^m$$

be a polynomial in $A[X]$, of degree m, and assume $g \neq 0$. Then

$$f(X)g(X) = a_0 b_0 + \cdots + a_n b_m X^{m+n}.$$

Therefore:

If we assume that at least one of the leading coefficients a_n or b_m is not a divisor of 0 *in A, then*

$$\deg(fg) = \deg f + \deg g$$

and the leading coefficient of fg is $a_n b_m$. This holds in particular when a_n or b_m is a unit in A, or when A is entire. Consequently, when A is entire, $A[X]$ is also entire.

If f or $g = 0$, then we still have

$$\deg(fg) = \deg f + \deg g$$

if we agree that $-\infty + m = -\infty$ for any integer m.

One verifies trivially that for any polynomials f, $g \in A[X]$ we have

$$\deg(f + g) \leqq \max(\deg f, \deg g),$$

again agreeing that $-\infty < m$ for every integer m.

Polynomials in several variables

We now go to polynomials in several variables. Let A be a subring of a commutative ring B. Let $x_1, \dots, x_n \in B$. For each n-tuple of integers $(\nu_1, \dots, \nu_n) = (\nu) \in \mathbf{N}^n$, we use vector notation, letting $(x) = (x_1, \dots, x_n)$, and

$$M_{(\nu)}(x) = x_1^{\nu_1} \cdots x_n^{\nu_n}.$$

The set of such elements forms a monoid under multiplication. Let $A[x] = A[x_1, \dots, x_n]$ be the subring of B generated by $x_1, \dots, x_n$ over A. Then every element of $A[x]$ can be written as a finite sum

$$\sum a_{(\nu)} M_{(\nu)}(x) \qquad \text{with} \quad a_{(\nu)} \in A.$$

Using the construction of polynomials in one variable repeatedly, we may form the ring

$$A[X_1, \dots, X_n] = A[X_1][X_2] \cdots [X_n],$$

selecting X_n to be a variable over $A[X_1, \dots, X_{n-1}]$. Then every element f of $A[X_1, \dots, X_n] = A[X]$ has a *unique* expression as a finite sum

$$f = \sum_{j=0}^{d_n} f_j(X_1, \dots, X_{n-1}) X_n^j \qquad \text{with} \quad f_j \in A[X_1, \dots, X_{n-1}].$$

Therefore by induction we can write f uniquely as a sum

$$f = \sum_{\nu_n = 0}^{d_n} \left(\sum_{\nu_1, \dots, \nu_{n-1}} a_{\nu_1 \cdots \nu_n} X_1^{\nu_1} \cdots X_{n-1}^{\nu_{n-1}} \right) X_n^{\nu_n}$$
$$= \sum a_{(\nu)} M_{(\nu)}(X) = \sum a_{(\nu)} X_1^{\nu_1} \cdots X_n^{\nu_n}$$

with elements $a_{(\nu)} \in A$, which are called the **coefficients** of f. The products

$$M_{(\nu)}(X) = X_1^{\nu_1} \cdots X_n^{\nu_n}$$

will be called **primitive monomials**. Elements of $A[X]$ are called **polynomials** (in n variables). We call $a_{(\nu)}$ its **coefficients**.

Just as in the one-variable case, we have an evaluation map. Given $(x) = (x_1, \dots, x_n)$ and f as above, we define

$$f(x) = \sum a_{(\nu)} M_{(\nu)}(x) = \sum a_{(\nu)} x_1^{\nu_1} \cdots x_n^{\nu_n}.$$

Then the **evaluation map**

$$\mathrm{ev}_{(x)}\colon A[X] \to B \qquad \text{such that} \qquad f \mapsto f(x)$$

is a ring-homomorphism. It may be viewed as the composite of the successive evaluation maps in one variable $X_i \mapsto x_i$ for $i = n, \dots, 1$, because $A[X] \subset B[X]$.

Just as for one variable, if $f(X) \in A[X]$ is a polynomial in n variables, then we obtain a function

$$f_B\colon B^n \to B \qquad \text{by} \qquad (x) \mapsto f(x).$$

We say that $f(x)$ is obtained by **substituting** (x) for (X) in f, or by **specializing** (X) to (x). As for one variable, if K is a finite field, and $f \in K[X]$ one may have $f \neq 0$ but $f_K = 0$. Cf. Chapter IV, Theorem 1.4 and its corollaries.

Next let $\varphi\colon A \to B$ be a homomorphism of commutative rings. Then we have the **reduction map** (generalized in Proposition 3.2 below)

$$f(X) = \sum a_{(\nu)} M_{(\nu)}(X) \mapsto \sum \varphi(a_{(\nu)}) M_{(\nu)}(X) = (\varphi f)(X).$$

We can also compose the evaluation and reduction. An element $(x) \in B^n$ is called a **zero** of f if $(\varphi f)(x) = 0$. Such zeros will be studied in Chapter IX.

Go back to A as a subring of B. Elements $x_1, \ldots, x_n \in B$ are called **algebraically independent** over A if the evaluation map

$$f \mapsto f(x)$$

is injective. Equivalently, we could say that if $f \in A[X]$ is a polynomial and $f(x) = 0$, then $f = 0$; in other words, there are no non-trivial polynomial relations among $x_1, \ldots, x_n$ over A.

Example. It is not known if e and π are algebraically independent over the rationals. It is not even known if $e + \pi$ is rational.

We now come to the notion of degree for several variables. By the **degree** of a primitive monomial

$$M_{(\nu)}(X) = X_1^{\nu_1} \cdots X_n^{\nu_n}$$

we shall mean the integer $|\nu| = \nu_1 + \cdots + \nu_n$ (which is $\geqq 0$).

A polynomial

$$aX_1^{\nu_1} \cdots X_n^{\nu_n} \qquad (a \in A)$$

will be called a **monomial** (not necessarily primitive).

If $f(X)$ is a polynomial in $A[X]$ written as

$$f(X) = \sum a_{(\nu)} X_1^{\nu_1} \cdots X_n^{\nu_n},$$

then either $f = 0$, in which case we say that its degree is $-\infty$, or $f \neq 0$, and then we define the **degree** of f to be the maximum of the degrees of the monomials $M_{(\nu)}(X)$ such that $a_{(\nu)} \neq 0$. (Such monomials are said to **occur** in the polynomial.) We note that the degree of f is 0 if and only if

$$f(X) = a_0 X_1^0 \cdots X_n^0$$

for some $a_0 \in A$, $a_0 \neq 0$. We also write this polynomial simply $f(X) = a_0$, i.e. writing 1 instead of

$$X_1^0 \cdots X_n^0,$$

in other words, we identify the polynomial with the constant a_0.

Note that a polynomial $f(X_1, \dots, X_n)$ in n variables can be viewed as a polynomial in X_n with coefficients in $A[X_1, \dots, X_{n-1}]$ (if $n \geqq 2$). Indeed, we can write

$$f(X) = \sum_{j=0}^{d_n} f_j(X_1, \dots, X_{n-1})X_n^j,$$

where f_j is an element of $A[X_1, \dots, X_{n-1}]$. By the **degree of f in X_n** we shall mean its degree when viewed as a polynomial in X_n with coefficients in $A[X_1, \dots, X_{n-1}]$. One sees easily that if this degree is d, then d is the largest integer occurring as an exponent of X_n in a monomial

$$a_{(v)}X_1^{v_1} \cdots X_n^{v_n}$$

with $a_{(v)} \neq 0$. Similarly, we define the degree of f in each variable X_i ($i = 1, \dots, n$).

The degree of f in each variable is of course usually different from its degree (which is sometimes called the **total degree** if there is need to prevent ambiguity). For instance,

$$X_1^3X_2 + X_2^2$$

has total degree 4, and has degree 3 in X_1 and 2 in X_2.

As a matter of notation, we shall often abbreviate "degree" by "deg."

For each integer $d \geqq 0$, given a polynomial f, let $f^{(d)}$ be the sum of all monomials occurring in f and having degree d. Then

$$f = \sum_d f^{(d)}.$$

Suppose $f \neq 0$. We say that f is **homogeneous** of degree d if $f = f^{(d)}$; thus f can be written in the form

$$f(X) = \sum a_{(v)}X_1^{v_1} \cdots X_n^{v_n} \qquad \text{with} \qquad v_1 + \cdots + v_n = d \qquad \text{if} \quad a_{(v)} \neq 0.$$

We shall leave it as an exercise to prove that *a non-zero polynomial f in n variables over A is homogeneous of degree d if and only if, for every set of $n + 1$ algebraically independent elements $u, t_1, \dots, t_n$ over A we have*

$$f(ut_1, \dots, ut_n) = u^d f(t_1, \dots, t_n).$$

We note that if f, g are homogeneous of degree d, e respectively, and $fg \neq 0$, then fg is homogeneous of degree $d + e$. If $d = e$ and $f + g \neq 0$, then $f + g$ is homogeneous of degree d.

Remark. In view of the isomorphism

$$A[X_1, \dots, X_n] \approx A[t_1, \dots, t_n]$$

between the polynomial ring in n variables and a ring generated over A by n

algebraically independent elements, we can apply all the terminology we have defined for polynomials, to elements of $A[t_1, \ldots, t_n]$. Thus we can speak of the degree of an element in $A[t]$, and the rules for the degree of a product or sum hold. In fact, we shall also call elements of $A[t]$ polynomials in (t). Algebraically independent elements will also be called **variables** (or independent variables), and any distinction which we make between $A[X]$ and $A[t]$ is more psychological than mathematical.

Suppose next that A is entire. By what we know of polynomials in one variable and induction, it follows that $A[X_1, \ldots, X_n]$ is entire. In particular, suppose f has degree d and g has degree e. Write

$$f = f^{(d)} + \text{terms of lower degree,}$$

$$g = g^{(e)} + \text{terms of lower degree.}$$

Then $fg = f^{(d)}g^{(e)} + \text{terms of lower degree}$, and if $fg \neq 0$ then $f^{(d)}g^{(e)} \neq 0$. Thus we find:

$$\deg(fg) = \deg f + \deg g,$$

$$\deg(f + g) \leqq \max(\deg f, \deg g).$$

We are now finished with the basic terminology of polynomials. We end this section by indicating how the construction of polynomials is actually a special case of another construction which is used in other contexts. Interested readers can skip immediately to Chapter IV, giving further important properties of polynomials. See also Exercise 33 of Chapter XIII for harmonic polynomials.

The group ring or monoid ring

Let A be a commutative ring. Let G be a monoid, written multiplicatively.

Let $A[G]$ be the set of all maps $\alpha: G \to A$ such that $\alpha(x) = 0$ for almost all $x \in G$. We define addition in $A[G]$ to be the ordinary addition of mappings into an abelian (additive) group. If α, $\beta \in A[G]$, we define their product $\alpha\beta$ by the rule

$$(\alpha\beta)(z) = \sum_{xy=z} \alpha(x)\beta(y).$$

The sum is taken over all pairs (x, y) with x, $y \in G$ such that $xy = z$. This sum is actually finite, because there is only a finite number of pairs of elements $(x, y) \in G \times G$ such that $\alpha(x)\beta(y) \neq 0$. We also see that $(\alpha\beta)(t) = 0$ for almost all t, and thus belongs to our set $A[G]$.

The axioms for a ring are trivially verified. We shall carry out the proof of associativity as an example. Let α, β, $\gamma \in A[G]$. Then

$$\begin{aligned}((\alpha\beta)\gamma)(z) &= \sum_{xy=z} (\alpha\beta)(x)\gamma(y)\\ &= \sum_{xy=z}\left[\sum_{uv=x} \alpha(u)\beta(v)\right]\gamma(y)\\ &= \sum_{xy=z}\left[\sum_{uv=x} \alpha(u)\beta(v)\gamma(y)\right]\\ &= \sum_{\substack{(u,v,y)\\ uvy=z}} \alpha(u)\beta(v)\gamma(y),\end{aligned}$$

this last sum being taken over all triples $(u\ v,\ y)$ whose product is z. This last sum is now symmetric, and if we had computed $(\alpha(\beta\gamma))(z)$, we would have found this sum also. This proves associativity.

The unit element of $A[G]$ is the function δ such that $\delta(e) = 1$ and $\delta(x) = 0$ for all $x \in G$, $x \neq e$. It is trivial to verify that $\alpha = \delta\alpha = \alpha\delta$ for all $\alpha \in A[G]$.

We shall now adopt a notation which will make the structure of $A[G]$ clearer. Let $a \in A$ and $x \in G$. We denote by $a \cdot x$ (and sometimes also by ax) the function whose value at x is a, and whose value at y is 0 if $y \neq x$. Then an element $\alpha \in A[G]$ can be written as a sum

$$\alpha = \sum_{x \in G} \alpha(x) \cdot x.$$

Indeed, if $\{a_x\}_{x \in G}$ is a set of elements of A almost all of which are 0, and we set

$$\beta = \sum_{x \in G} a_x \cdot x,$$

then for any $y \in G$ we have $\beta(y) = a_y$ (directly from the definitions). This also shows that a given element α admits a unique expression as a sum $\sum a_x \cdot x$.

With our present notation, multiplication can be written

$$\left(\sum_{x \in G} a_x \cdot x\right)\left(\sum_{y \in G} b_y \cdot y\right) = \sum_{x,y} a_x b_y \cdot xy$$

and addition can be written

$$\sum_{x \in G} a_x \cdot x + \sum_{x \in G} b_x \cdot x = \sum_{x \in G} (a_x + b_x) \cdot x,$$

which looks the way we want it to look. Note that the unit element of $A[G]$ is simply $1 \cdot e$.

We shall now see that we can embed both A and G in a natural way in $A[G]$.

Let $\varphi_0 \colon G \to A[G]$ be the map given by $\varphi_0(x) = 1 \cdot x$. It is immediately verified that φ_0 is a multiplicative monoid-homomorphism, and is in fact injective, i.e. an embedding.

Let $f_0 \colon A \to A[G]$ be the map given by

$$f_0(a) = a \cdot e.$$

It is immediately verified that f_0 is a ring-homomorphism, and is also an embedding. Thus we view A as a subring of $A[G]$. One calls $A[G]$ the **monoid ring** or **monoid algebra** of G over A, or the **group algebra** if G is a group.

Examples. When G is a finite group and $A = k$ is a field, then the group ring $k[G]$ will be studied in Chapter XVIII.

Polynomial rings are special cases of the above construction. In n variables, consider a multiplicative free abelian group of rank n. Let $X_1, \dots, X_n$ be generators. Let G be the multiplicative subset consisting of elements $X_1^{\nu_1} \cdots X_n^{\nu_n}$ with $\nu_i \geqq 0$ for all i. Then G is a monoid, and the reader can verify at once that $A[G]$ is just $A[X_1, \dots, X_n]$.

As a matter of notation we usually omit the dot in writing an element of the ring $A[G]$, so we write simply $\sum a_x x$ for such an element.

More generally, let $I = \{i\}$ be an infinite family of indices, and let S be the free abelian group with free generators X_i, written multiplicatively. Then we can form the polynomial ring $A[X]$ by taking the monoid to consist of products

$$M_{(\nu)}(X) = \prod_{i \in I} X_i^{\nu_i},$$

where of course all but a finite number of exponents ν_i are equal to 0. If A is a subring of the commutative ring B, and S is a subset of B, then we shall also use the following notation. Let $\nu: S \to \mathbf{N}$ be a mapping which is 0 except for a finite number of elements of S. We write

$$M_{(\nu)}(S) = \prod_{x \in S} x^{\nu(x)}.$$

Thus we get polynomials in infinitely many variables. One interesting example of the use of such polynomials will occur in Artin's proof of the existence of the algebraic closure of a field, cf. Chapter V, Theorem 2.5.

We now consider the evaluation and reduction homomorphisms in the present context of monoids.

Proposition 3.1. *Let $\varphi: G \to G'$ be a homomorphism of monoids. Then there exists a unique homomorphism $h: A[G] \to A[G']$ such that $h(x) = \varphi(x)$ for all $x \in G$ and $h(a) = a$ for all $a \in A$.*

Proof. In fact, let $\alpha = \sum a_x x \in A[G]$. Define

$$h(\alpha) = \sum a_x \varphi(x).$$

Then h is immediately verified to be a homomorphism of abelian groups, and $h(x) = \varphi(x)$. Let $\beta = \sum b_y y$. Then

$$h(\alpha\beta) = \sum_z \left(\sum_{xy=z} a_x b_y \right) \varphi(z).$$

We get $h(\alpha\beta) = h(\alpha)h(\beta)$ immediately from the hypothesis that $\varphi(xy) =$

$\varphi(x)\varphi(y)$. If e is the unit element of G, then by definition $\varphi(e) = e'$, so Proposition 3.1 follows.

Proposition 3.2. *Let G be a monoid and let $f\colon A \to B$ be a homomorphism of commutative rings. Then there is a unique homomorphism*

$$h\colon A[G] \to B[G]$$

such that

$$h\left(\sum_{x \in G} a_x x\right) = \sum_{x \in G} f(a_x)x.$$

Proof. Since every element of $A[G]$ has a unique expression as a sum $\sum a_x x$, the formula giving h gives a well-defined map from $A[G]$ into $B[G]$. This map is obviously a homomorphism of abelian groups. As for multiplication, let

$$\alpha = \sum a_x x \qquad \text{and} \qquad \beta = \sum b_y y.$$

Then

$$\begin{aligned} h(\alpha\beta) &= \sum_{z \in G} f\left(\sum_{xy=z} a_x b_y\right) z \\ &= \sum_{z \in G} \sum_{xy=z} f(a_x)f(b_y)z \\ &= h(\alpha)h(\beta). \end{aligned}$$

We have trivially $h(1) = 1$, so h is a ring-homomorphism, as was to be shown.

Observe that viewing A as a subring of $A[G]$, the restriction of h to A is the homomorphism f itself. In other words, if e is the unit element of G, then

$$h(ae) = f(a)e.$$

§4. LOCALIZATION

We continue to let A be a commutative ring.

By a **multiplicative subset** of A we shall mean a submonoid of A (viewed as a multiplicative monoid according to **RI 2**). In other words, it is a subset S containing 1, and such that, if $x, y \in S$, then $xy \in S$.

We shall now construct the **quotient ring of** A **by** S, also known as the **ring of fractions of** A **by** S.

We consider pairs (a, s) with $a \in A$ and $s \in S$. We define a relation

$$(a, s) \sim (a', s')$$

between such pairs, by the condition that there exists an element $s_1 \in S$ such that

$$s_1(s'a - sa') = 0.$$

It is then trivially verified that this is an equivalence relation, and the equivalence class containing a pair (a, s) is denoted by a/s. The set of equivalence classes is denoted by $S^{-1}A$.

Note that if $0 \in S$, then $S^{-1}A$ has precisely one element, namely $0/1$.

We define a multiplication in $S^{-1}A$ by the rule

$$(a/s)(a'/s') = aa'/ss'.$$

It is trivially verified that this is well defined. This multiplication has a unit element, namely $1/1$, and is clearly associative.

We define an addition in $S^{-1}A$ by the rule

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'}.$$

It is trivially verified that this is well defined. As an example, we give the proof in detail. Let $a_1/s_1 = a/s$, and let $a'_1/s'_1 = a'/s'$. We must show that

$$(s'_1 a_1 + s_1 a'_1)/s_1 s'_1 = (s'a + sa')/ss'.$$

There exist $s_2, s_3 \in S$ such that

$$s_2(sa_1 - s_1 a) = 0,$$
$$s_3(s'a'_1 - s'_1 a') = 0.$$

We multiply the first equation by $s_3 s' s'_1$ and the second by $s_2 s s_1$. We then add, and obtain

$$s_2 s_3[s's'_1(sa_1 - s_1 a) + ss_1(s'a'_1 - s'_1 a')] = 0.$$

By definition, this amounts to what we want to show, namely that there exists an element of S (e.g. $s_2 s_3$) which when multiplied with

$$ss'(s'_1 a_1 + s_1 a'_1) - s_1 s'_1(s'a + sa')$$

yields 0.

We observe that given $a \in A$ and $s, s' \in S$ we have

$$a/s = s'a/s's.$$

Thus this aspect of the elementary properties of fractions still remains true in our present general context.

Finally, it is also trivially verified that our two laws of composition on $S^{-1}A$ define a ring structure.

We let

$$\varphi_S \colon A \to S^{-1}A$$

be the map such that $\varphi_S(a) = a/1$. Then one sees at once that φ_S is a ring-homomorphism. Furthermore, every element of $\varphi_S(S)$ is invertible in $S^{-1}A$ (the inverse of $s/1$ is $1/s$).

Let $\mathcal{C}$ be the category whose objects are ring-homomorphisms

$$f\colon A \to B$$

such that for every $s \in S$, the element $f(s)$ is invertible in B. If $f\colon A \to B$ and $f'\colon A \to B'$ are two objects of $\mathcal{C}$, a morphism g of f into f' is a homomorphism

$$g\colon B \to B'$$

making the diagram commutative:

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "f'"'] & & B \arrow[dl, "g"] \\ & B' & \end{tikzcd}$$

We contend that φ_S is a universal object in this category $\mathcal{C}$.

Proof. Suppose that $a/s = a'/s'$, or in other words that the pairs (a, s) and (a', s') are equivalent. There exists $s_1 \in S$ such that

$$s_1(s'a - sa') = 0.$$

Let $f\colon A \to B$ be an object of $\mathcal{C}$. Then

$$f(s_1)[f(s')f(a) - f(s)f(a')] = 0.$$

Multiplying by $f(s_1)^{-1}$, and then by $f(s')^{-1}$ and $f(s)^{-1}$, we obtain

$$f(a)f(s)^{-1} = f(a')f(s')^{-1}.$$

Consequently, we can define a map

$$h\colon S^{-1}A \to B$$

such that $h(a/s) = f(a)f(s)^{-1}$, for all $a/s \in S^{-1}A$. It is trivially verified that h is a homomorphism, and makes the usual diagram commutative. It is also trivially verified that such a map h is unique, and hence that φ_S is the required universal object.

Let A be an entire ring, and let S be a multiplicative subset which does not contain 0. *Then*

$$\varphi_S\colon A \to S^{-1}A$$

is injective.

Indeed, by definition, if $a/1 = 0$ then there exists $s \in S$ such that $sa = 0$, and hence $a = 0$.

The most important cases of a multiplicative set S are the following:

1. Let A be a commutative ring, and let S be the set of invertible elements of A (i.e. the set of units). Then S is obviously multiplicative, and is denoted frequently by A^*. If A is a field, then A^* is the multiplicative group of non-zero elements of A. In that case, $S^{-1}A$ is simply A itself.

2. Let A be an entire ring, and let S be the set of non-zero elements of A. Then S is a multiplicative set, and $S^{-1}A$ is then a field, called the **quotient field** or the **field of fractions**, of A. It is then customary to identify A as a subset of $S^{-1}A$, and we can write

$$a/s = s^{-1}a$$

for $a \in A$ and $s \in S$.

We have seen in §3 that when A is an entire ring, then $A[X_1, \ldots, X_n]$ is also entire. If K is the quotient field of A, the quotient field of $A[X_1, \ldots, X_n]$ is denoted by $K(X_1, \ldots, X_n)$. An element of $K(X_1, \ldots, X_n)$ is called a **rational function**. A rational function can be written as a quotient $f(X)/g(X)$ where f, g are polynomials. If $(b_1, \ldots, b_n)$ is in $K^{(n)}$, and a rational function admits an expression as a quotient f/g such that $g(b) \neq 0$, then we say that the rational function is **defined** at (b). From general localization properties, we see that when this is the case, we can substitute (b) in the rational function to get a value $f(b)/g(b)$.

3. A ring A is called a **local ring** if it is commutative and has a unique maximal ideal. If A is a local ring and $\mathfrak{m}$ is its maximal ideal, and $x \in A$, $x \notin \mathfrak{m}$, then x is a unit (otherwise x generates a proper ideal, not contained in $\mathfrak{m}$, which is impossible). Let A be a ring and $\mathfrak{p}$ a prime ideal. Let S be the complement of $\mathfrak{p}$ in A. Then S is a multiplicative subset of A, and $S^{-1}A$ is denoted by $A_{\mathfrak{p}}$. It is a local ring (cf. Exercise 3) and is called **the local ring of A at** $\mathfrak{p}$. Cf. the examples of principal rings, and Exercises 15, 16.

Let S be a multiplicative subset of A. Denote by $J(A)$ the set of ideals of A. Then we can define a map

$$\psi_S : J(A) \to J(S^{-1}A);$$

namely we let $\psi_S(\mathfrak{a}) = S^{-1}\mathfrak{a}$ be the subset of $S^{-1}A$ consisting of all fractions a/s with $a \in \mathfrak{a}$ and $s \in S$. The reader will easily verify that $S^{-1}\mathfrak{a}$ is an $S^{-1}A$-ideal, and that ψ_S is a homomorphism for both the additive and multiplicative monoid structures on the set of ideals $J(A)$. Furthermore, ψ_S also preserves intersections and inclusions; in other words, for ideals $\mathfrak{a}$, $\mathfrak{b}$ of A we have:

$$S^{-1}(\mathfrak{a} + \mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b}, \qquad S^{-1}(\mathfrak{a}\mathfrak{b}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b}),$$

$$S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}.$$

As an example, we prove this last relation. Let $x \in \mathfrak{a} \cap \mathfrak{b}$. Then x/s is in $S^{-1}\mathfrak{a}$ and also in $S^{-1}\mathfrak{b}$, so the inclusion is trivial. Conversely, suppose we have an element of $S^{-1}A$ which can be written as $a/s = b/s'$ with $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, and $s, s' \in S$. Then there exists $s_1 \in S$ such that

$$s_1 s' a = s_1 s b,$$

and this element lies in both $\mathfrak{a}$ and $\mathfrak{b}$. Hence

$$a/s = s_1 s' a / s_1 s' s$$

lies in $S^{-1}(\mathfrak{a} \cap \mathfrak{b})$, as was to be shown.

§5. PRINCIPAL AND FACTORIAL RINGS

Let A be an entire ring. An element $a \neq 0$ is called **irreducible** if it is not a unit, and if whenever one can write $a = bc$ with $b \in A$ and $c \in A$ then b or c is a unit.

Let $a \neq 0$ be an element of A and assume that the principal ideal (a) is prime. Then a is irreducible. Indeed, if we write $a = bc$, then b or c lies in (a), say b. Then we can write $b = ad$ with some $d \in A$, and hence $a = acd$. Since A is entire, it follows that $cd = 1$, in other words, that c is a unit.

The converse of the preceding assertion is not always true. We shall discuss under which conditions it is true. An element $a \in A$, $a \neq 0$, is said to have a **unique factorization into irreducible elements** if there exists a unit u and there exist irreducible elements p_i $(i = 1, \ldots, r)$ in A such that

$$a = u \prod_{i=1}^{r} p_i,$$

and if given two factorizations into irreducible elements,

$$a = u \prod_{i=1}^{r} p_i = u' \prod_{j=1}^{s} q_j,$$

we have $r = s$, and after a permutation of the indices i, we have $p_i = u_i q_i$ for some unit u_i in A, $i = 1, \ldots, r$.

We note that if p is irreducible and u is a unit, then up is also irreducible, so we must allow multiplication by units in a factorization. In the ring of integers $\mathbf{Z}$, the ordering allows us to select a representative irreducible element (a prime number) out of two possible ones differing by a unit, namely $\pm p$, by selecting the positive one. This is, of course, impossible in more general rings.

Taking $r = 0$ above, we adopt the convention that a unit of A has a factorization into irreducible elements.

A ring is called **factorial** (or a **unique factorization ring**) if it is entire and if every element $\neq 0$ has a unique factorization into irreducible elements. We shall prove below that a principal entire ring is factorial.

Let A be an entire ring and $a, b \in A$, $ab \neq 0$. We say that a **divides** b and write $a | b$ if there exists $c \in A$ such that $ac = b$. We say that $d \in A$, $d \neq 0$, is a **greatest common divisor (g.c.d.)** of a and b if $d | a$, $d | b$, and if any element e of A, $e \neq 0$, which divides both a and b also divides d.

Proposition 5.1. *Let A be a principal entire ring and $a, b \in A$, $a, b \neq 0$. Let $(a) + (b) = (c)$. Then c is a greatest common divisor of a and b.*

Proof. Since b lies in the ideal (c), we can write $b = xc$ for some $x \in A$, so that $c|b$. Similarly, $c|a$. Let d divide both a and b, and write $a = dy$, $b = dz$ with $y, z \in A$. Since c lies in (a, b) we can write

$$c = wa + tb$$

with some $w, t \in A$. Then $c = w\,dy + t\,dz = d(wy + tz)$, whence $d|c$, and our proposition is proved.

Theorem 5.2. *Let A be a principal entire ring. Then A is factorial.*

Proof. We first prove that every non-zero element of A has a factorization into irreducible elements. Let S be the set of principal ideals $\neq 0$ whose generators do not have a factorization into irreducible elements, and suppose S is not empty. Let (a_1) be in S. Consider an ascending chain

$$(a_1) \subsetneqq (a_2) \subsetneqq \cdots \subsetneqq (a_n) \subsetneqq \cdots$$

of ideals in S. We contend that such a chain cannot be infinite. Indeed, the union of such a chain is an ideal of A, which is principal, say equal to (a). The generator a must already lie in some element of the chain, say (a_n), and then we see that $(a_n) \subset (a) \subset (a_n)$, whence the chain stops at (a_n). Hence S is inductively ordered, and has a maximal element (a). Therefore any ideal of A containing (a) and $\neq (a)$ has a generator admitting a factorization.

We note that a cannot be irreducible (otherwise it has a factorization), and hence we can write $a = bc$ with neither b nor c equal to a unit. But then $(b) \neq (a)$ and $(c) \neq (a)$ and hence both b, c admit factorizations into irreducible elements. The product of these factorizations is a factorization for a, contradicting the assumption that S is not empty.

To prove uniqueness, we first remark that if p is an irreducible element of A and $a, b \in A$, $p|ab$, then $p|a$ or $p|b$. *Proof*: If $p \nmid a$, then the g.c.d. of p, a is 1 and hence we can write

$$1 = xp + ya$$

with some $x, y \in A$. Then $b = bxp + yab$, and since $p|ab$ we conclude that $p|b$.

Suppose that a has two factorizations

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

into irreducible elements. Since p_1 divides the product farthest to the right, p_1 divides one of the factors, which we may assume to be q_1 after renumbering these factors. Then there exists a unit u_1 such that $q_1 = u_1 p_1$. We can now cancel p_1 from both factorizations and get

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

The argument is completed by induction.

We could call two elements a, $b \in A$ equivalent if there exists a unit u such that $a = bu$. Let us select one irreducible element p out of each equivalence class belonging to such an irreducible element, and let us denote by P the set of such representatives. Let $a \in A$, $a \neq 0$. Then there exists a unit u and integers $v(p) \geqq 0$, equal to 0 for almost all $p \in P$ such that

$$a = u \prod_{p \in P} p^{v(p)}.$$

Furthermore, the unit u and the integers $v(p)$ are uniquely determined by a. We call $v(p)$ the **order** of a at p, also written $\operatorname{ord}_p a$.

If A is a factorial ring, then an irreducible element p generates a prime ideal (p). Thus in a factorial ring, an irreducible element will also be called a **prime element**, or simply a **prime**.

We observe that one can define the notion of **least common multiple** (l.c.m.) of a finite number of non-zero elements of A in the usual manner: If

$$a_1, \ldots, a_n \in A$$

are such elements, we define a l.c.m. for these elements to be any $c \in A$ such that for all primes p of A we have

$$\operatorname{ord}_p c = \max_i \operatorname{ord}_p a_i.$$

This element c is well defined up to a unit.

If $a, b \in A$ are non-zero elements, we say that a, b are **relatively prime** if the g.c.d. of a and b is a unit.

Example. The ring of integers $\mathbf{Z}$ is factorial. Its group of units consists of 1 and -1. It is natural to take as representative prime element the positive prime element (what is called a prime number) p from the two possible choices p and $-p$. Similarly, we shall show later that the ring of polynomials in one variable over a field is factorial, and one selects representatives for the prime elements to be the irreducible polynomials with leading coefficient 1.

Examples. It will be proved in Chapter IV that if R is a factorial ring, then the polynomial ring $R[X_1, \ldots, X_n]$ in n variables is factorial. In particular, if k is a field, then the polynomial ring $k[X_1, \ldots, X_n]$ is factorial. Note that $k[X_1]$ is a principal ring, but for $n \geqq 2$, the ring $k[X_1, \ldots, X_n]$ is not principal.

In Exercise 5 you will prove that the localization of a factorial ring is factorial.

In Chapter IV, §9 we shall prove that the power series ring $k[[X_1, \ldots, X_n]]$ is factorial. This result is a special case of the more general statement that a regular local ring is factorial, but we do not define regular local rings in this book. You can look them up in books on commutative algebra. I recommend:

H. MATSUMURA, *Commutative Algebra*, second edition, Benjamin-Cummings, New York, 1980

H. MATSUMURA, *Commutative Rings*, Cambridge University Press, Cambridge, UK, 1986

Examples from algebraic and complex geometry. Roughly speaking, regular local rings arise in the following context of algebraic or complex geometry. Consider the ring of regular functions in the neighborhood of some point on a complex or algebraic manifold. This ring is regular. A typical example is the ring of convergent power series in a neighborhood of 0 in $\mathbf{C}^n$. In Chapter IV, we shall prove some results on power series which give some algebraic background for those analytic theories, and which are used in proving the factoriality of rings of power series, convergent or not.

Conversely to the above examples, singularities in geometric theories may give rise to examples of non-factoriality. We give examples using notions which are sufficiently basic so that readers should have encountered them in more elementary courses.

Examples of non-factorial rings. Let k be a field, and let x be a variable over k. Let $R = k[x^2, x^3]$. Then R is not factorial (proof?). The ring R may be viewed as the ring of regular functions on the curve $y^2 = x^3$, which has a singularity at the origin, as you can see by drawing its real graph.

Let R be the set of all numbers of the form $a + b\sqrt{-5}$, where $a, b \in \mathbf{Z}$. Then the only units of R are ± 1, and the elements 3, $2 + \sqrt{-5}$, $2 - \sqrt{-5}$ are irreducible elements, giving rise to a non-unique factorization

$$3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

(Do Exercise 10.) Here the non-factoriality is not due to singularities but due to a non-trivial ideal class group of R, which is a Dedekind ring. For a definition see the exercises of Chapter III, or go straight to my book *Algebraic Number Theory*, for instance.

As Trotter once pointed out (*Math. Monthly*, April 1988), the relation

$$\sin^2 x = (1 + \cos x)(1 - \cos x)$$

may be viewed as a non-unique factorization in the ring of trigonometric polynomials $\mathbf{R}[\sin x, \cos x]$, generated over $\mathbf{R}$ by the functions $\sin x$ and $\cos x$. This ring is a subring of the ring of all functions, or of all differentiable functions. See Exercise 11.

EXERCISES

We let A denote a commutative ring.

1. Suppose that $1 \neq 0$ in A. Let S be a multiplicative subset of A not containing 0. Let $\mathfrak{p}$ be a maximal element in the set of ideals of A whose intersection with S is empty. Show that $\mathfrak{p}$ is prime.

2. Let $f: A \to A'$ be a surjective homomorphism of rings, and assume that A is local, $A' \neq 0$. Show that A' is local.

3. Let $\mathfrak{p}$ be a prime ideal of A. Show that $A_{\mathfrak{p}}$ has a unique maximal ideal, consisting of all elements a/s with $a \in \mathfrak{p}$ and $s \notin \mathfrak{p}$.

4. Let A be a principal ring and S a multiplicative subset with $0 \notin S$. Show that $S^{-1}A$ is principal.

5. Let A be a factorial ring and S a multiplicative subset with $0 \notin S$. Show that $S^{-1}A$ is factorial, and that the prime elements of $S^{-1}A$ are of the form up with primes p of A such that $(p) \cap S$ is empty, and units u in $S^{-1}A$.

6. Let A be a factorial ring and p a prime element. Show that the local ring $A_{(p)}$ is principal.

7. Let A be a principal ring and $a_1, \ldots, a_n$ non-zero elements of A. Let $(a_1, \ldots, a_n) = (d)$. Show that d is a greatest common divisor for the a_i $(i = 1, \ldots, n)$.

8. Let p be a prime number, and let A be the ring $\mathbf{Z}/p^r\mathbf{Z}$ (r = integer $\geqq 1$). Let G be the group of units in A, i.e. the group of integers prime to p, modulo p^r. Show that G is cyclic, except in the case when

$$p = 2, \qquad r \geqq 3,$$

in which case it is of type $(2, 2^{r-2})$. [*Hint*: In the general case, show that G is the product of a cyclic group generated by $1 + p$, and a cyclic group of order $p - 1$. In the exceptional case, show that G is the product of the group $\{\pm 1\}$ with the cyclic group generated by the residue class of 5 mod 2^r.]

9. Let i be the complex number $\sqrt{-1}$. Show that the ring $\mathbf{Z}[i]$ is principal, and hence factorial. What are the units?

10. Let D be an integer $\geqq 1$, and let R be the set of all elements $a + b\sqrt{-D}$ with $a, b \in \mathbf{Z}$.
    (a) Show that R is a ring.
    (b) Using the fact that complex conjugation is an automorphism of $\mathbf{C}$, show that complex conjugation induces an automorphism of R.
    (c) Show that if $D \geqq 2$ then the only units in R are ± 1.
    (d) Show that $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ are irreducible elements in $\mathbf{Z}[\sqrt{-5}]$.

11. Let R be the ring of trigonometric polynomials as defined in the text. Show that R consists of all functions f on $\mathbf{R}$ which have an expression of the form

$$f(x) = a_0 + \sum_{m=1}^{n} (a_m \cos mx + b_m \sin mx),$$

where a_0, a_m, b_m are real numbers. Define the **trigonometric degree** $\deg_{\text{tr}}(f)$ to be the maximum of the integers r, s such that $a_r, b_s \neq 0$. Prove that

$$\deg_{\text{tr}}(fg) = \deg_{\text{tr}}(f) + \deg_{\text{tr}}(g).$$

Deduce from this that R has no divisors of 0, and also deduce that the functions $\sin x$ and $1 - \cos x$ are irreducible elements in that ring.

12. Let P be the set of positive integers and R the set of functions defined on P with values in a commutative ring K. Define the sum in R to be the ordinary addition of functions, and define the **convolution product** by the formula

$$(f * g)(m) = \sum_{xy=m} f(x)g(y),$$

where the sum is taken over all pairs (x, y) of positive integers such that $xy = m$.
(a) Show that R is a commutative ring, whose unit element is the function δ such that $\delta(1) = 1$ and $\delta(x) = 0$ if $x \neq 1$.
(b) A function f is said to be **multiplicative** if $f(mn) = f(m)f(n)$ whenever m, n are relatively prime. If f, g are multiplicative, show that $f * g$ is multiplicative.
(c) Let μ be the **Möbius function** such that $\mu(1) = 1$, $\mu(p_1 \cdots p_r) = (-1)^r$ if $p_1, \ldots, p_r$ are distinct primes, and $\mu(m) = 0$ if m is divisible by p^2 for some prime p. Show that $\mu * \varphi_1 = \delta$, where φ_1 denotes the constant function having value 1. [*Hint*: Show first that μ is multiplicative, and then prove the assertion for prime powers.] The Möbius inversion formula of elementary number theory is then nothing else but the relation $\mu * \varphi_1 * f = f$.

Dedekind rings

Prove the following statements about a Dedekind ring $\mathfrak{o}$. To simplify terminology, by an **ideal** we shall mean non-zero ideal unless otherwise specified. We let K denote the quotient field of $\mathfrak{o}$.

13. Every ideal is finitely generated. [*Hint*: Given an ideal $\mathfrak{a}$, let $\mathfrak{b}$ be the fractional ideal such that $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$. Write $1 = \sum a_i b_i$ with $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. Show that $\mathfrak{a} = (a_1, \ldots, a_n)$.]

14. Every ideal has a factorization as a product of prime ideals, uniquely determined up to permutation.

15. Suppose $\mathfrak{o}$ has only one prime ideal $\mathfrak{p}$. Let $t \in \mathfrak{p}$ and $t \notin \mathfrak{p}^2$. Then $\mathfrak{p} = (t)$ is principal.

16. Let $\mathfrak{o}$ be any Dedekind ring. Let $\mathfrak{p}$ be a prime ideal. Let $\mathfrak{o}_\mathfrak{p}$ be the local ring at $\mathfrak{p}$. Then $\mathfrak{o}_\mathfrak{p}$ is Dedekind and has only one prime ideal.

17. As for the integers, we say that $\mathfrak{a}|\mathfrak{b}$ ($\mathfrak{a}$ **divides** $\mathfrak{b}$) if there exists an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Prove:
(a) $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{b} \subset \mathfrak{a}$.
(b) Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals. Then $\mathfrak{a} + \mathfrak{b}$ is their greatest common divisor. In particular, $\mathfrak{a}$, $\mathfrak{b}$ are relatively prime if and only if $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$.

18. Every prime ideal $\mathfrak{p}$ is maximal. (Remember, $\mathfrak{p} \neq 0$ by convention.) In particular, if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct primes, then the Chinese remainder theorem applies to their powers $\mathfrak{p}_1^{r_1}, \ldots, \mathfrak{p}_n^{r_n}$. Use this to prove:

19. Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals. Show that there exists an element $c \in K$ (the quotient field of $\mathfrak{o}$) such that $c\mathfrak{a}$ is an ideal relatively prime to $\mathfrak{b}$. In particular, every ideal class in $\operatorname{Pic}(\mathfrak{o})$ contains representative ideals prime to a given ideal.

For a continuation, see Exercise 7 of Chapter VII; Chapter III, Exercise 11–13.