1

Rings and Ideals

We shall begin by reviewing rapidly the definition and elementary properties of rings. This will indicate how much we are going to assume of the reader and it will also serve to fix notation and conventions. After this review we pass on to a discussion of prime and maximal ideals. The remainder of the chapter is devoted to explaining the various elementary operations which can be performed on ideals. The Grothendieck language of schemes is dealt with in the exercises at the end.

RINGS AND RING HOMOMORPHISMS

A *ring* A is a set with two binary operations (addition and multiplication) such that

1) A is an abelian group with respect to addition (so that A has a zero element, denoted by 0, and every $x \in A$ has an (additive) inverse, $-x$).
2) Multiplication is associative $((xy)z = x(yz))$ and distributive over addition $(x(y + z) = xy + xz, (y + z)x = yx + zx)$.

We shall consider only rings which are *commutative*:

3) $xy = yx$ for all $x, y \in A$,

and have an *identity element* (denoted by 1):

4) $\exists 1 \in A$ such that $x1 = 1x = x$ for all $x \in A$.

The identity element is then unique.

Throughout this book the word "ring" shall mean a commutative ring with an identity element, that is, a ring satisfying axioms (1) to (4) above.

Remark. We do not exclude the possibility in (4) that 1 might be equal to 0. If so, then for any $x \in A$ we have

$$x = x1 = x0 = 0$$

and so A has only one element, 0. In this case A is the *zero ring*, denoted by 0 (by abuse of notation).

A *ring homomorphism* is a mapping f of a ring A into a ring B such that

i) $f(x + y) = f(x) + f(y)$ (so that f is a homomorphism of abelian groups, and therefore also $f(x - y) = f(x) - f(y), f(-x) = -f(x), f(0) = 0$),

ii) $f(xy) = f(x)f(y)$,

iii) $f(1) = 1$.

In other words, f respects addition, multiplication and the identity element.

A subset S of a ring A is a *subring* of A if S is closed under addition and multiplication and contains the identity element of A. The identity mapping of S into A is then a ring homomorphism.

If $f: A \to B, g: B \to C$ are ring homomorphisms then so is their composition $g \circ f: A \to C$.

IDEALS. QUOTIENT RINGS

An *ideal* $\mathfrak{a}$ of a ring A is a subset of A which is an additive subgroup and is such that $A\mathfrak{a} \subseteq \mathfrak{a}$ (i.e., $x \in A$ and $y \in \mathfrak{a}$ imply $xy \in \mathfrak{a}$). The quotient group $A/\mathfrak{a}$ inherits a uniquely defined multiplication from A which makes it into a ring, called the *quotient ring* (or residue-class ring) $A/\mathfrak{a}$. The elements of $A/\mathfrak{a}$ are the cosets of $\mathfrak{a}$ in A, and the mapping $\phi: A \to A/\mathfrak{a}$ which maps each $x \in A$ to its coset $x + \mathfrak{a}$ is a surjective ring homomorphism.

We shall frequently use the following fact:

Proposition 1.1. *There is a one-to-one order-preserving correspondence between the ideals $\mathfrak{b}$ of A which contain $\mathfrak{a}$, and the ideals $\bar{\mathfrak{b}}$ of $A/\mathfrak{a}$, given by* $\mathfrak{b} = \phi^{-1}(\bar{\mathfrak{b}})$. ∎

If $f: A \to B$ is any ring homomorphism, the *kernel* of $f\,(=f^{-1}(0))$ is an ideal $\mathfrak{a}$ of A, and the *image* of $f\,(=f(A))$ is a subring C of B; and f induces a ring isomorphism $A/\mathfrak{a} \cong C$.

We shall sometimes use the notation $x \equiv y \pmod{\mathfrak{a}}$; this means that $x - y \in \mathfrak{a}$.

ZERO-DIVISORS. NILPOTENT ELEMENTS. UNITS

A *zero-divisor* in a ring A is an element x which "divides 0", i.e., for which there exists $y \neq 0$ in A such that $xy = 0$. A ring with no zero-divisors $\neq 0$ (and in which $1 \neq 0$) is called an *integral domain*. For example, $\mathbf{Z}$ and $k[x_1, \ldots, x_n]$ (k a field, x_i indeterminates) are integral domains.

An element $x \in A$ is *nilpotent* if $x^n = 0$ for some $n > 0$. A nilpotent element is a zero-divisor (unless $A = 0$), but not conversely (in general).

A *unit* in A is an element x which "divides 1", i.e., an element x such that $xy = 1$ for some $y \in A$. The element y is then uniquely determined by x, and is written x^{-1}. The units in A form a (multiplicative) abelian group.

The multiples ax of an element $x \in A$ form a *principal* ideal, denoted by (x) or Ax. x is a unit $\Leftrightarrow (x) = A = (1)$. The *zero* ideal (0) is usually denoted by 0.

A *field* is a ring A in which $1 \neq 0$ and every non-zero element is a unit. Every field is an integral domain (but not conversely: $\mathbf{Z}$ is not a field).

Proposition 1.2. *Let A be a ring $\neq 0$. Then the following are equivalent:*

i) *A is a field;*

ii) *the only ideals in A are 0 and (1);*

iii) *every homomorphism of A into a non-zero ring B is injective.*

Proof. i) $\Rightarrow$ ii). Let $\mathfrak{a} \neq 0$ be an ideal in A. Then $\mathfrak{a}$ contains a non-zero element x; x is a unit, hence $\mathfrak{a} \supseteq (x) = (1)$, hence $\mathfrak{a} = (1)$.

ii) $\Rightarrow$ iii). Let $\phi: A \to B$ be a ring homomorphism. Then $\operatorname{Ker}(\phi)$ is an ideal $\neq (1)$ in A, hence $\operatorname{Ker}(\phi) = 0$, hence ϕ is injective.

iii) $\Rightarrow$ i). Let x be an element of A which is not a unit. Then $(x) \neq (1)$, hence $B = A/(x)$ is not the zero ring. Let $\phi: A \to B$ be the natural homomorphism of A onto B, with kernel (x). By hypothesis, ϕ is injective, hence $(x) = 0$, hence $x = 0$. ∎

PRIME IDEALS AND MAXIMAL IDEALS

An ideal $\mathfrak{p}$ in A is *prime* if $\mathfrak{p} \neq (1)$ and if $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

An ideal $\mathfrak{m}$ in A is *maximal* if $\mathfrak{m} \neq (1)$ and if there is no ideal $\mathfrak{a}$ such that $\mathfrak{m} \subset \mathfrak{a} \subset (1)$ (*strict* inclusions). Equivalently:

$\mathfrak{p}$ is prime $\Leftrightarrow A/\mathfrak{p}$ is an integral domain;

$\mathfrak{m}$ is maximal $\Leftrightarrow A/\mathfrak{m}$ is a field (by (1.1) and (1.2)).

Hence a maximal ideal is prime (but not conversely, in general). The zero ideal is prime $\Leftrightarrow A$ is an integral domain.

If $f: A \to B$ is a ring homomorphism and $\mathfrak{q}$ is a prime ideal in B, then $f^{-1}(\mathfrak{q})$ is a prime ideal in A, for $A/f^{-1}(\mathfrak{q})$ is isomorphic to a subring of $B/\mathfrak{q}$ and hence has no zero-divisor $\neq 0$. But if $\mathfrak{n}$ is a maximal ideal of B it is not necessarily true that $f^{-1}(\mathfrak{n})$ is maximal in A; all we can say for sure is that it is prime. (Example: $A = \mathbf{Z}$, $B = \mathbf{Q}$, $\mathfrak{n} = 0$.)

Prime ideals are fundamental to the whole of commutative algebra. The following theorem and its corollaries ensure that there is always a sufficient supply of them.

Theorem 1.3. *Every ring $A \neq 0$ has at least one maximal ideal.* (Remember that "ring" means commutative ring with 1.)

Proof. This is a standard application of Zorn's lemma.* Let Σ be the set of all ideals $\neq (1)$ in A. Order Σ by inclusion. Σ is not empty, since $0 \in \Sigma$. To apply

---

* Let S be a non-empty partially ordered set (i.e., we are given a relation $x \leqslant y$ on S which is reflexive and transitive and such that $x \leqslant y$ and $y \leqslant x$ together imply

Zorn's lemma we must show that every chain in Σ has an upper bound in Σ; let then $(\mathfrak{a}_\alpha)$ be a chain of ideals in Σ, so that for each pair of indices α, β we have either $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$ or $\mathfrak{a}_\beta \subseteq \mathfrak{a}_\alpha$. Let $\mathfrak{a} = \bigcup_\alpha \mathfrak{a}_\alpha$. Then $\mathfrak{a}$ is an ideal (verify this) and $1 \notin \mathfrak{a}$ because $1 \notin \mathfrak{a}_\alpha$ for all α. Hence $\mathfrak{a} \in \Sigma$, and $\mathfrak{a}$ is an upper bound of the chain. Hence by Zorn's lemma Σ has a maximal element. ∎

Corollary 1.4. *If $\mathfrak{a} \neq (1)$ is an ideal of A, there exists a maximal ideal of A containing $\mathfrak{a}$.*

Proof. Apply (1.3) to $A/\mathfrak{a}$, bearing in mind (1.1). Alternatively, modify the proof of (1.3). ∎

Corollary 1.5. *Every non-unit of A is contained in a maximal ideal.* ∎

Remarks. 1) If A is Noetherian (Chapter 7) we can avoid the use of Zorn's lemma: the set of all ideals $\neq (1)$ has a maximal element.

2) There exist rings with exactly one maximal ideal, for example fields. A ring A with exactly one maximal ideal $\mathfrak{m}$ is called a *local ring*. The field $k = A/\mathfrak{m}$ is called the *residue field* of A.

Proposition 1.6. i) *Let A be a ring and $\mathfrak{m} \neq (1)$ an ideal of A such that every $x \in A - \mathfrak{m}$ is a unit in A. Then A is a local ring and $\mathfrak{m}$ its maximal ideal.*

ii) *Let A be a ring and $\mathfrak{m}$ a maximal ideal of A, such that every element of $1 + \mathfrak{m}$ (i.e., every $1 + x$, where $x \in \mathfrak{m}$) is a unit in A. Then A is a local ring.*

Proof. i) Every ideal $\neq (1)$ consists of non-units, hence is contained in $\mathfrak{m}$. Hence $\mathfrak{m}$ is the only maximal ideal of A.

ii) Let $x \in A - \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, the ideal generated by x and $\mathfrak{m}$ is (1), hence there exist $y \in A$ and $t \in \mathfrak{m}$ such that $xy + t = 1$; hence $xy = 1 - t$ belongs to $1 + \mathfrak{m}$ and therefore is a unit. Now use i). ∎

A ring with only a finite number of maximal ideals is called *semi-local.*

Examples. 1) $A = k[x_1, \ldots, x_n]$, k a field. Let $f \in A$ be an irreducible polynomial. By unique factorization, the ideal (f) is prime.

2) $A = \mathbf{Z}$. Every ideal in $\mathbf{Z}$ is of the form (m) for some $m \geqslant 0$. The ideal (m) is prime $\Leftrightarrow m = 0$ or a prime number. All the ideals (p), where p is a prime number, are maximal: $\mathbf{Z}/(p)$ is the field of p elements.

The same holds in Example 1) for $n = 1$, but not for $n > 1$. The ideal $\mathfrak{m}$ of all polynomials in $A = k[x_1, \ldots, x_n]$ with zero constant term is maximal (since

---

$x = y$). A subset T of S is a *chain* if either $x \leqslant y$ or $y \leqslant x$ for every pair of elements x, y in T. Then Zorn's lemma may be stated as follows: if every chain T of S has an upper bound in S (i.e., if there exists $x \in S$ such that $t \leqslant x$ for all $t \in T$) then S has at least one maximal element.

For a proof of the equivalence of Zorn's lemma with the axiom of choice, the well-ordering principle, etc., see for example P. R. Halmos, *Naïve Set Theory*, Van Nostrand (1960).