Chapter 3

Rings

Rings are additive abelian groups with a second operation called multiplication. The connection between the two operations is provided by the distributive law. Assuming the results of Chapter 2, this chapter flows smoothly. This is because ideals are also normal subgroups and ring homomorphisms are also group homomorphisms. We do not show that the polynomial ring $F[x]$ is a unique factorization domain, although with the material at hand, it would be easy to do. Also there is no mention of prime or maximal ideals, because these concepts are unnecessary for our development of linear algebra. These concepts are developed in the Appendix. A section on Boolean rings is included because of their importance in logic and computer science.

Suppose R is an additive abelian group, $R \neq \underline{0}$, and R has a second binary operation (i.e., map from $R \times R$ to R) which is denoted by multiplication. Consider the following properties.

1) If $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (The associative property of multiplication.)
2) If $a, b, c \in R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$. (The distributive law, which connects addition and multiplication.)
3) R has a multiplicative identity, i.e., there is an element $\underline{1} = \underline{1}_R \in R$ such that if $a \in R$, $a \cdot \underline{1} = \underline{1} \cdot a = a$.
4) If $a, b \in R$, $a \cdot b = b \cdot a$. (The commutative property for multiplication.)

Definition If 1), 2), and 3) are satisfied, R is said to be a *ring*. If in addition 4) is satisfied, R is said to be a *commutative ring*.

Examples The basic commutative rings in mathematics are the integers $\mathbf{Z}$, the rational numbers $\mathbf{Q}$, the real numbers $\mathbf{R}$, and the complex numbers $\mathbf{C}$. It will be shown later that $\mathbf{Z}_n$, the integers mod n, has a natural multiplication under which it is a commutative ring. Also if R is any commutative ring, we will define $R[x_1, x_2, \ldots, x_n]$, a polynomical ring in n variables. Now suppose R is any ring, $n \geq 1$, and R_n is the collection of all $n \times n$ matrices over R. In the next chapter, operations of addition and multiplication of matrices will be defined. Under these operations, R_n is a ring. This is a basic example of a non-commutative ring. If $n > 1$, R_n is never commutative, even if R is commutative.

The next two theorems show that ring multiplication behaves as you would wish it to. They should be worked as exercises.

Theorem Suppose R is a ring and $a,\ b \in R$.

1) $a \cdot \underline{0} = \underline{0} \cdot a = \underline{0}$. Since $R \neq \underline{0}$, it follows that $\underline{1} \neq \underline{0}$.
2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

Recall that, since R is an additive abelian group, it has a scalar multiplication over $\mathbf{Z}$ (page 20). This scalar multiplication can be written on the right or left, i.e., $na = an$, and the next theorem shows it relates nicely to the ring multiplication.

Theorem Suppose $a, b \in R$ and $n, m \in \mathbf{Z}$.

1) $(na) \cdot (mb) = (nm)(a \cdot b)$. (This follows from the distributive law and the previous theorem.)

2) Let $\underline{n} = n\underline{1}$. For example, $\underline{2} = \underline{1} + \underline{1}$. Then $na = \underline{n} \cdot a$, that is, scalar multiplication by n is the same as ring multiplication by $\underline{n}$. Of course, $\underline{n}$ may be $\underline{0}$ even though $n \neq 0$.

Units

Definition An element a of a ring R is a *unit* provided $\exists$ an element $a^{-1} \in R$ with $a \cdot a^{-1} = a^{-1} \cdot a = \underline{1}$.

Theorem $\underline{0}$ can never be a unit. $\underline{1}$ is always a unit. If a is a unit, a^{-1} is also a unit with $(a^{-1})^{-1} = a$. The product of units is a unit with $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. More generally, if $a_1, a_2, ..., a_n$ are units, then their product is a unit with $(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_1^{-1}$. The set of all units of R forms a multiplicative group denoted by R^*. Finally if a is a unit, $(-a)$ is a unit and $(-a)^{-1} = -(a^{-1})$.

In order for a to be a unit, it must have a two-sided inverse. It suffices to require a left inverse and a right inverse, as shown in the next theorem.

Theorem Suppose $a \in R$ and $\exists$ elements b and c with $b \cdot a = a \cdot c = \underline{1}$. Then $b = c$ and so a is a unit with $a^{-1} = b = c$.

Proof $b = b \cdot \underline{1} = b \cdot (a \cdot c) = (b \cdot a) \cdot c = \underline{1} \cdot c = c$.

Corollary Inverses are unique.

Domains and Fields In order to define these two types of rings, we first consider the concept of zero divisor.

Definition Suppose R is a commutative ring. An element $a \in R$ is called a *zero divisor* provided it is non-zero and $\exists$ a non-zero element b with $a \cdot b = \underline{0}$. Note that if a is a unit, it cannot be a zero divisor.

Theorem Suppose R is a commutative ring and $a \in (R - \underline{0})$ is not a zero divisor. Then $(a \cdot b = a \cdot c) \Rightarrow b = c$. In other words, multiplication by a is an injective map from R to R. It is surjective iff a is a unit.

Definition A *domain* (or *integral domain*) is a commutative ring such that, if $a \neq \underline{0}$, a is not a zero divisor. A *field* is a commutative ring such that, if $a \neq \underline{0}$, a is a unit. In other words, R is a field if it is commutative and its non-zero elements form a group under multiplication.

Theorem A field is a domain. A finite domain is a field.

Proof A field is a domain because a unit cannot be a zero divisor. Suppose R is a finite domain and $a \neq \underline{0}$. Then $f : R \to R$ defined by $f(b) = a \cdot b$ is injective and, by the pigeonhole principle, f is surjective. Thus a is a unit and so R is a field.

Exercise Let $\mathbf{C}$ be the additive abelian group $\mathbf{R}^2$. Define multiplication by $(a, b) \cdot (c, d) = (ac - bd,\ ad + bc)$. Show $\mathbf{C}$ is a commutative ring which is a field. Note that $\underline{1} = (1, 0)$ and if $i = (0, 1)$, then $i^2 = -\underline{1}$.

Examples $\mathbf{Z}$ is a domain. $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ are fields.

The Integers Mod n

The concept of integers mod n is fundamental in mathematics. It leads to a neat little theory, as seen by the theorems below. However, the basic theory cannot be completed until the product of rings is defined. (See the Chinese Remainder Theorem on page 50.) We know from page 27 that $\mathbf{Z}_n$ is an additive abelian group.

Theorem Suppose $n > 1$. Define a multiplication on $\mathbf{Z}_n$ by $[a] \cdot [b] = [ab]$. This is a well defined binary operation which makes $\mathbf{Z}_n$ into a commutative ring.

Proof Since $[a + kn] \cdot [b + ln] = [ab + n(al + bk + kln)] = [ab]$, the multiplication is well-defined. The ring axioms are easily verified.

Theorem Suppose $n > 1$ and $a \in \mathbf{Z}$. Then the following are equivalent.

1) $[a]$ is a generator of the additive group $\mathbf{Z}_n$.
2) $(a, n) = 1$.
3) $[a]$ is a unit of the ring $\mathbf{Z}_n$.

Proof We already know from page 27 that 1) and 2) are equivalent. Recall that if b is an integer, $[a]b = [a] \cdot [b] = [ab]$. Thus 1) and 3) are equivalent, because each says $\exists$ an integer b with $[a]b = [1]$.

Corollary If $n > 1$, the following are equivalent.

1) $\mathbf{Z}_n$ is a domain.
2) $\mathbf{Z}_n$ is a field.
3) n is a prime.

Proof We already know 1) and 2) are equivalent, because $\mathbf{Z}_n$ is finite. Suppose 3) is true. Then by the previous theorem, each of $[1]$, $[2]$,...,$[n-1]$ is a unit, and thus 2) is true. Now suppose 3) is false. Then $n = ab$ where $1 < a < n$, $1 < b < n$,

$[a][b] = [0]$, and thus $[a]$ is a zero divisor and 1) is false.

Exercise List the units and their inverses for $\mathbf{Z}_7$ and $\mathbf{Z}_{12}$. Show that $(\mathbf{Z}_7)^*$ is a cyclic group but $(\mathbf{Z}_{12})^*$ is not. Show that in $\mathbf{Z}_{12}$ the equation $x^2 = \underline{1}$ has four solutions. Finally show that if R is a domain, $x^2 = \underline{1}$ can have at most two solutions in R (see the first theorem on page 46).

Subrings Suppose S is a subset of a ring R. The statement that S is a *subring* of R means that S is a subgroup of the group R, $\underline{1} \in S$, and $(a, b \in S \Rightarrow a \cdot b \in S)$. Then clearly S is a ring and has the same multiplicative identity as R. Note that $\mathbf{Z}$ is a subring of $\mathbf{Q}$, $\mathbf{Q}$ is a subring of $\mathbf{R}$, and $\mathbf{R}$ is a subring of $\mathbf{C}$. Subrings do not play a role analogous to subgroups. That role is played by ideals, and an ideal is never a subring (unless it is the entire ring). Note that if S is a subring of R and $s \in S$, then s may be a unit in R but not in S. Note also that $\mathbf{Z}$ and $\mathbf{Z}_n$ have no proper subrings, and thus occupy a special place in ring theory, as well as in group theory.

Ideals and Quotient Rings

Ideals in ring theory play a role analagous to normal subgroups in group theory.

Definition A subset I of a ring R is a $\left\{\begin{array}{l}\text{left}\\ \text{right}\\ 2\text{−sided}\end{array}\right\}$ ideal provided it is a subgroup of the additive group R and if $a \in R$ and $b \in I$, then $\left\{\begin{array}{l}a \cdot b \in I\\ b \cdot a \in I\\ a \cdot b \text{ and } b \cdot a \in I\end{array}\right\}$. The word "ideal " means "2-sided ideal". Of course, if R is commutative, every right or left ideal is an ideal.

Theorem Suppose R is a ring.

1) R and $\underline{0}$ are ideals of R. These are called the *improper* ideals.

2) If $\{I_t\}_{t \in T}$ is a collection of right (left, 2-sided) ideals of R, then $\bigcap\limits_{t \in T} I_t$ is a right (left, 2-sided) ideal of R. (See page 22.)

3) Furthermore, if the collection is monotonic, then $\bigcup_{t \in T} I_t$ is a right (left, 2-sided) ideal of R.

4) If $a \in R$, $I = aR$ is a right ideal. Thus if R is commutative, aR is an ideal, called a *principal ideal*. Thus every subgroup of $\mathbf{Z}$ is a principal ideal, because it is of the form $n\mathbf{Z}$.

5) If R is a commutative ring and $I \subset R$ is an ideal, then the following are equivalent.
   i) $I = R$.
   ii) I contains some unit u.
   iii) I contains $\underline{1}$.

Exercise Suppose R is a commutative ring. Show that R is a field iff R contains no proper ideals.

The following theorem is just an observation, but it is in some sense the beginning of ring theory.

Theorem Suppose R is a ring and $I \subset R$ is an ideal, $I \neq R$. Since I is a normal subgroup of the additive group R, R/I is an additive abelian group. Multiplication of cosets defined by $(a + I) \cdot (b + I) = (ab + I)$ is well-defined and makes R/I a ring.

Proof $(a + I) \cdot (b + I) = a \cdot b + aI + Ib + II \ \subset \ a \cdot b + I$. Thus multiplication is well defined, and the ring axioms are easily verified. The multiplicative identity is $(\underline{1} + I)$.

Observation If $R = \mathbf{Z}$, $n > 1$, and $I = n\mathbf{Z}$, the ring structure on $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$ is the same as the one previously defined.

Homomorphisms

Definition Suppose R and $\bar{R}$ are rings. A function $f : R \to \bar{R}$ is a *ring homomorphism* provided

1) f is a group homomorphism
2) $f(\underline{1}_R) = \underline{1}_{\bar{R}}$ and
3) if $a, b \in R$ then $f(a \cdot b) = f(a) \cdot f(b)$. (On the left, multiplication

is in R, while on the right multiplication is in $\bar{R}$.)

The *kernel* of f is the kernel of f considered as a group homomorphism, namely $\ker(f) = f^{-1}(\underline{0})$.

Here is a list of the basic properties of ring homomorphisms. Much of this work has already been done by the theorem in group theory on page 28.

Theorem Suppose each of R and $\bar{R}$ is a ring.

1) The identity map $I_R : R \to R$ is a ring homomorphism.

2) The zero map from R to $\bar{R}$ is not a ring homomorphism (because it does not send $\underline{1}_R$ to $\underline{1}_{\bar{R}}$).

3) The composition of ring homomorphisms is a ring homomorphism.

4) If $f : R \to \bar{R}$ is a bijection which is a ring homomorphism, then $f^{-1} : \bar{R} \to R$ is a ring homomorphism. Such an f is called a *ring isomorphism*. In the case $R = \bar{R}$, f is also called a *ring automorphism*.

5) The image of a ring homomorphism is a subring of the range.

6) The kernel of a ring homomorphism is an ideal of the domain. In fact, if $f : R \to \bar{R}$ is a homomorphism and $I \subset \bar{R}$ is an ideal, then $f^{-1}(I)$ is an ideal of R.

7) Suppose I is an ideal of R, $I \neq R$, and $\pi : R \to R/I$ is the natural projection, $\pi(a) = (a + I)$. Then π is a surjective ring homomorphism with kernel I. Furthermore, if $f : R \to \bar{R}$ is a surjective ring homomorphism with kernel I, then $R/I \approx \bar{R}$ (see below).

8) From now on the word "homomorphism" means "ring homomorphism". Suppose $f : R \to \bar{R}$ is a homomorphism and I is an ideal of R, $I \neq R$. If $I \subset \ker(f)$, then $\bar{f} : R/I \to \bar{R}$ defined by $\bar{f}(a + I) = f(a)$

is a well-defined homomorphism making the following diagram commute.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & \bar{R} \\ R/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Thus defining a homomorphism on a quotient ring is the same as defining a homomorphism on the numerator which sends the denominator to zero. The image of $\bar{f}$ is the image of f, and the kernel of $\bar{f}$ is $\ker(f)/I$. Thus if $I = \ker(f)$, $\bar{f}$ is injective, and so $R/I \approx \text{image}\ (f)$.

Proof We know all this on the group level, and it is only necessary to check that $\bar{f}$ is a ring homomorphism, which is obvious.

9) Given any ring homomorphism f, $\text{domain}(f)/\ker(f) \approx \text{image}(f)$.

Exercise Find a ring R with a proper ideal I and an element b such that b is not a unit in R but $(b + I)$ is a unit in R/I.

Exercise Show that if u is a unit in a ring R, then conjugation by u is an automorphism on R. That is, show that $f : R \to R$ defined by $f(a) = u^{-1} \cdot a \cdot u$ is a ring homomorphism which is an isomorphism.

Exercise Suppose T is a non-void set, R is a ring, and R^T is the collection of all functions $f : T \to R$. Define addition and multiplication on R^T point-wise. This means if f and g are functions from T to R, then $(f + g)(t) = f(t) + g(t)$ and $(f \cdot g)(t) = f(t)g(t)$. Show that under these operations R^T is a ring. Suppose S is a non-void set and $\alpha : S \to T$ is a function. If $f : T \to R$ is a function, define a function $\alpha^*(f) : S \to R$ by $\alpha^*(f) = f \circ \alpha$. Show $\alpha^* : R^T \to R^S$ is a ring homomorphism.

Exercise Now consider the case $T = [0, 1]$ and $R = \mathbf{R}$. Let $A \subset \mathbf{R}^{[0,1]}$ be the collection of all C^∞ functions, i.e., $A = \{f : [0, 1] \to \mathbf{R} : f$ has an infinite number of derivatives$\}$. Show A is a ring. Notice that much of the work has been done in the previous exercise. It is only necessary to show that A is a subring of the ring $\mathbf{R}^{[0,1]}$.

Polynomial Rings

In calculus, we consider real functions f which are polynomials, $f(x) = a_0 + a_1 x + \cdot\cdot + a_n x^n$. The sum and product of polynomials are again polynomials, and it is easy to see that the collection of polynomial functions forms a commutative ring. We can do the same thing formally in a purely algebraic setting.

Definition Suppose R is a commutative ring and x is a "variable" or "symbol". The *polynomial ring* $R[x]$ is the collection of all polynomials $f = a_0 + a_1 x + \cdot\cdot + a_n x^n$ where $a_i \in R$. Under the obvious addition and multiplication, $R[x]$ is a commutative ring. The *degree* of a non-zero polynomial f is the largest integer n such that $a_n \neq \underline{0}$, and is denoted by $n = \deg(f)$. If the top term $a_n = \underline{1}$, then f is said to be *monic*.

To be more formal, think of a polynomial $a_0 + a_1 x + \cdots$ as an infinite sequence $(a_0, a_1, ...)$ such that each $a_i \in R$ and only a finite number are non-zero. Then
$(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$ and
$(a_0, a_1, ...) \cdot (b_0, b_1, ...) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, ...)$.
Note that on the right, the ring multiplication $a \cdot b$ is written simply as ab, as is often done for convenience.

Theorem If R is a domain, $R[x]$ is also a domain.

Proof Suppose f and g are non-zero polynomials. Then $\deg(f) + \deg(g) = \deg(fg)$ and thus fg is not $\underline{0}$. Another way to prove this theorem is to look at the bottom terms instead of the top terms. Let $a_i x^i$ and $b_j x^j$ be the first non-zero terms of f and g. Then $a_i b_j x^{i+j}$ is the first non-zero term of fg.

Theorem (The Division Algorithm) Suppose R is a commutative ring, $f \in R[x]$ has degree ≥ 1 and its top coefficient is a unit in R. (If R is a field, the top coefficient of f will always be a unit.) Then for any $g \in R[x]$, $\exists!\ h, r \in R[x]$ such that $g = fh + r$ with $r = \underline{0}$ or $\deg(r) < \deg(f)$.

Proof This theorem states the existence and uniqueness of polynomials h and r. We outline the proof of existence and leave uniqueness as an exercise. Suppose $f = a_0 + a_1 x + \cdot\cdot + a_m x^m$ where $m \geq 1$ and a_m is a unit in R. For any g with $\deg(g) < m$, set $h = \underline{0}$ and $r = g$. For the general case, the idea is to divide f into g until the remainder has degree less than m. The proof is by induction on the degree of g. Suppose $n \geq m$ and the result holds for any polynomial of degree less than

n. Suppose g is a polynomial of degree n. Now $\exists$ a monomial bx^t with $t = n - m$ and $\deg(g - fbx^t) < n$. By induction, $\exists$ h_1 and r with $fh_1 + r = (g - fbx^t)$ and $\deg(r) < m$. The result follows from the equation $f(h_1 + bx^t) + r = g$.

Note If $r = \underline{0}$ we say that f divides g. Note that $f = x - c$ divides g iff c is a *root* of g, i.e., $g(c) = \underline{0}$. More generally, $x - c$ divides g with remainder $g(c)$.

Theorem Suppose R is a domain, $n > 0$, and $g(x) = a_0 + a_1x + \cdots + a_nx^n$ is a polynomial of degree n with at least one root in R. Then g has at most n roots. Let $c_1, c_2, .., c_k$ be the distinct roots of g in the ring R. Then $\exists$ a unique sequence of positive integers $n_1, n_2, .., n_k$ and a unique polynomial h with no root in R so that $g(x) = (x - c_1)^{n_1} \cdots (x - c_k)^{n_k} h(x)$. (If h has degree 0, i.e., if $h = a_n$, then we say "all the roots of g belong to R". If $g = a_nx^n$, we say "all the roots of g are $\underline{0}$".)

Proof Uniqueness is easy so let's prove existence. The theorem is clearly true for $n = 1$. Suppose $n > 1$ and the theorem is true for any polynomial of degree less than n. Now suppose g is a polynomial of degree n and c_1 is a root of g. Then $\exists$ a polynomial h_1 with $g(x) = (x - c_1)h_1$. Since h_1 has degree less than n, the result follows by induction.

Note If g is any non-constant polynomial in $\mathbf{C}[x]$, all the roots of g belong to $\mathbf{C}$, i.e., $\mathbf{C}$ is an *algebraically closed field*. This is called The Fundamental Theorem of Algebra, and it is assumed without proof for this textbook.

Exercise Suppose g is a non-constant polynomial in $\mathbf{R}[x]$. Show that if g has odd degree then it has a real root. Also show that if $g(x) = x^2 + bx + c$, then it has a real root iff $b^2 \geq 4c$, and in that case both roots belong to $\mathbf{R}$.

Definition A domain T is a *principal ideal domain* (PID) if, given any ideal I, $\exists\ t \in T$ such that $I = tT$. Note that $\mathbf{Z}$ is a PID and any field is PID.

Theorem Suppose F is a field, I is a proper ideal of $F[x]$, and n is the smallest positive integer such that I contains a polynomial of degree n. Then I contains a unique polynomial of the form $f = a_0 + a_1x + \cdot\cdot + a_{n-1}x^{n-1} + x^n$ and it has the property that $I = fF[x]$. Thus $F[x]$ is a PID. Furthermore, each coset of I can be written uniquely in the form $(c_0 + c_1x + \cdot\cdot + c_{n-1}x^{n-1} + I)$.

Proof. This is a good exercise in the use of the division algorithm. Note this is similar to showing that a subgroup of $\mathbf{Z}$ is generated by one element (see page 15).

Theorem. Suppose R is a subring of a commutative ring C and $c \in C$. Then $\exists!$ homomorphism $h : R[x] \to C$ with $h(x) = c$ and $h(r) = r$ for all $r \in R$. It is defined by $h(a_0 + a_1 x + \cdot\cdot + a_n x^n) = a_0 + a_1 c + \cdot\cdot + a_n c^n$, i.e., h sends $f(x)$ to $f(c)$. The image of h is the smallest subring of C containing R and c.

This map h is called an *evaluation* map. The theorem says that adding two polynomials in $R[x]$ and evaluating is the same as evaluating and then adding in C. Also multiplying two polynomials in $R[x]$ and evaluating is the same as evaluating and then multiplying in C. In street language the theorem says you are free to send x wherever you wish and extend to a ring homomorphism on $R[x]$.

Exercise Let $\mathbf{C} = \{a + bi : a, b \in \mathbf{R}\}$. Since $\mathbf{R}$ is a subring of $\mathbf{C}$, there exists a homomorphism $h : \mathbf{R}[x] \to \mathbf{C}$ which sends x to i, and this h is surjective. Show $\ker(h) = (x^2 + 1)\mathbf{R}[x]$ and thus $\mathbf{R}[x]/(x^2 + 1) \approx \mathbf{C}$. This is a good way to look at the complex numbers, i.e., to obtain $\mathbf{C}$, adjoin x to $\mathbf{R}$ and set $x^2 = -1$.

Exercise $\mathbf{Z}_2[x]/(x^2 + x + 1)$ has 4 elements. Write out the multiplication table for this ring and show that it is a field.

Exercise Show that, if R is a domain, the units of $R[x]$ are just the units of R. Thus if F is a field, the units of $F[x]$ are the non-zero constants. Show that $[1] + [2]x$ is a unit in $\mathbf{Z}_4[x]$.

In this chapter we do not prove $F[x]$ is a unique factorization domain, nor do we even define unique factorization domain. The next definition and theorem are included merely for reference, and should not be studied at this stage.

Definition Suppose F is a field and $f \in F[x]$ has degree ≥ 1. The statement that g is an *associate* of f means $\exists$ a unit $u \in F[x]$ such that $g = uf$. The statement that f is *irreducible* means that if h is a non-constant polynomial which divides f, then h is an associate of f.

We do not develop the theory of $F[x]$ here. However, the development is easy because it corresponds to the development of $\mathbf{Z}$ in Chapter 1. The Division Algorithm corresponds to the Euclidean Algorithm. Irreducible polynomials correspond to prime integers. The degree function corresponds to the absolute value function. One difference is that the units of $F[x]$ are non-zero constants, while the units of $\mathbf{Z}$

are just ± 1. Thus the associates of f are all cf with $c \neq \underline{0}$ while the associates of an integer n are just $\pm n$. Here is the basic theorem. (This theory is developed in full in the Appendix under the topic of Euclidean domains.)

Theorem Suppose F is a field and $f \in F[x]$ has degree ≥ 1. Then f factors as the product of irreducibles, and this factorization is unique up to order and associates. Also the following are equivalent.

1) $F[x]/(f)$ is a domain.
2) $F[x]/(f)$ is a field.
3) f is irreducible.

Definition Now suppose x and y are "variables". If $a \in R$ and $n, m \geq 0$, then $ax^n y^m = ay^m x^n$ is called a *monomial*. Define an element of $R[x, y]$ to be any finite sum of monomials.

Theorem $R[x, y]$ is a commutative ring and $(R[x])[y] \approx R[x, y] \approx (R[y])[x]$. In other words, any polynomial in x and y with coefficients in R may be written as a polynomial in y with coefficients in $R[x]$, or as a polynomial in x with coefficients in $R[y]$.

Side Comment It is true that if F is a field, each $f \in F[x, y]$ factors as the product of irreducibles. However $F[x, y]$ is not a PID. For example, the ideal $I = xF[x, y] + yF[x, y] = \{f \in F[x, y] : f(\underline{0}, \underline{0}) = \underline{0}\}$ is not principal.

If R is a commutative ring and $n \geq 2$, the concept of a polynomial ring in n variables works fine without a hitch. If $a \in R$ and $v_1, v_2, ..., v_n$ are non-negative integers, then $ax_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$ is called a monomial. Order does not matter here. Define an element of $R[x_1, x_2, ..., x_n]$ to be any finite sum of monomials. This gives a commutative ring and there is canonical isomorphism $R[x_1, x_2, ..., x_n] \approx (R[x_1, x_2, ..., x_{n-1}])[x_n]$. Using this and induction on n, it is easy to prove the following theorem.

Theorem If R is a domain, $R[x_1, x_2, ..., x_n]$ is a domain and its units are just the units of R.

Exercise Suppose R is a commutative ring and $f : R[x,y] \to R[x]$ is the evaluation map which sends y to $\underline{0}$. This means $f(p(x,y)) = p(x,\underline{0})$. Show f is a ring homomorphism whose kernel is the ideal $(y) = yR[x,y]$. Use the fact that "the domain mod the kernel is isomorphic to the image" to show $R[x,y]/(y)$ is isomorphic to $R[x]$. That is, if you adjoin y to $R[x]$ and then factor it out, you get $R[x]$ back.

Product of Rings

The product of rings works fine, just as does the product of groups.

Theorem Suppose T is an index set and for each $t \in T$, R_t is a ring. On the additive abelian group $\prod\limits_{t\in T} R_t = \prod R_t$, define multiplication by $\{r_t\} \cdot \{s_t\} = \{r_t \cdot s_t\}$. Then $\prod R_t$ is a ring and each projection $\pi_s : \prod R_t \to R_s$ is a ring homomorphism. Suppose R is a ring. Under the natural bijection from $\{$functions $f : R \to \prod R_t\}$ to $\{$sequences of functions $\{f_t\}_{t\in T}$ where $f_t : R \to R_t\}$, f is a ring homomorphism iff each f_t is a ring homomorphism.

Proof We already know f is a group homomorphism iff each f_t is a group homomorphism (see page 36). Note that $\{\underline{1}_t\}$ is the multiplicative identity of $\prod R_t$, and $f(\underline{1}_R) = \{\underline{1}_t\}$ iff $f_t(\underline{1}_R) = \underline{1}_t$ for each $t \in T$. Finally, since multiplication is defined coordinatewise, f is a ring homomorphism iff each f_t is a ring homomorphism.

Exercise Suppose R and S are rings. Note that $R \times 0$ is not a subring of $R \times S$ because it does not contain $(\underline{1}_R, \underline{1}_S)$. Show $R \times \underline{0}$ is an ideal and $(R \times S/R \times \underline{0}) \approx S$. Suppose $I \subset R$ and $J \subset S$ are ideals. Show $I \times J$ is an ideal of $R \times S$ and every ideal of $R \times S$ is of this form.

Exercise Suppose R and S are commutative rings. Show $T = R \times S$ is not a domain. Let $e = (\underline{1}, \underline{0}) \in R \times S$ and show $e^2 = e$, $(\underline{1} - e)^2 = (\underline{1} - e)$, $R \times \underline{0} = eT$, and $\underline{0} \times S = (\underline{1} - e)T$.

Exercise If T is any ring, an element e of T is called an *idempotent* provided $e^2 = e$. The elements $\underline{0}$ and $\underline{1}$ are idempotents called the *trivial* idempotents. Suppose T is a commutative ring and $e \in T$ is an idempotent with $\underline{0} \neq e \neq \underline{1}$. Let $R = eT$ and $S = (\underline{1} - e)T$. Show each of the ideals R and S is a ring with identity, and $f : T \to R \times S$ defined by $f(t) = (et, (\underline{1} - e)t)$ is a ring isomorphism. This shows that a commutative ring T splits as the product of two rings iff it contains a non-trivial idempotent.

The Chinese Remainder Theorem

The natural map from $\mathbf{Z}$ to $\mathbf{Z}_m \times \mathbf{Z}_n$ is a group homomorphism and also a ring homomorphism. If m and n are relatively prime, this map is surjective with kernel $mn\mathbf{Z}$, and thus $\mathbf{Z}_{mn}$ and $\mathbf{Z}_m \times \mathbf{Z}_n$ are isomorphic as groups and as rings. The next theorem is a classical generalization of this. (See exercise three on page 35.)

Theorem Suppose $n_1, ..., n_t$ are integers, each $n_i > 1$, and $(n_i, n_j) = 1$ for all $i \neq j$. Let $f_i : \mathbf{Z} \to \mathbf{Z}_{n_i}$ be defined by $f_i(a) = [a]$. (Note that the bracket symbol is used ambiguously.) Then the ring homomorphism $f = (f_1, .., f_t) : \mathbf{Z} \to \mathbf{Z}_{n_1} \times \cdot\cdot \times \mathbf{Z}_{n_t}$ is surjective. Furthermore, the kernel of f is $n\mathbf{Z}$, where $n = n_1 n_2 \cdot\cdot n_t$. Thus $\mathbf{Z}_n$ and $\mathbf{Z}_{n_1} \times \cdot\cdot \times \mathbf{Z}_{n_t}$ are isomorphic as rings, and thus also as groups.

Proof We wish to show that the order of $f(1)$ is n, and thus $f(1)$ is a group generator, and thus f is surjective. The element $f(1)m = ([1], .., [1])m = ([m], .., [m])$ is zero iff m is a multiple of each of $n_1, .., n_t$. Since their least common multiple is n, the order of $f(1)$ is n. (See the fourth exercise on page 36 for the case $t = 3$.)

Exercise Show that if a is an integer and p is a prime, then $[a] = [a^p]$ in $\mathbf{Z}_p$ (Fermat's Little Theorem). Use this and the Chinese Remainder Theorem to show that if b is a positive integer, it has the same last digit as b^5.

Characteristic

The following theorem is just an observation, but it shows that in ring theory, the ring of integers is a "cornerstone".

Theorem If R is a ring, there is one and only one ring homomorphism $f : \mathbf{Z} \to R$. It is given by $f(m) = m\underline{1} = \underline{m}$. Thus the subgroup of R generated by $\underline{1}$ is a subring of R isomorphic to $\mathbf{Z}$ or isomorphic to $\mathbf{Z}_n$ for some positive integer n.

Definition Suppose R is a ring and $f : \mathbf{Z} \to R$ is the natural ring homomorphism $f(m) = m\underline{1} = \underline{m}$. The non-negative integer n with $\ker(f) = n\mathbf{Z}$ is called the *characteristic* of R. Thus f is injective iff R has characteristic 0 iff $\underline{1}$ has infinite order. If f is not injective, the characteristic of R is the order of $\underline{1}$.

It is an interesting fact that, if R is a domain, all the non-zero elements of R have the same order. (See page 23 for the definition of order.)

Theorem Suppose R is a domain. If R has characteristic 0, then each non-zero $a \in R$ has infinite order. If R has finite characteristic n, then n is a prime and each non-zero $a \in R$ has order n.

Proof Suppose R has characteristic 0, a is a non-zero element of R, and m is a positive integer. Then $ma = \underline{m} \cdot a$ cannot be $\underline{0}$ because $\underline{m}, a \neq \underline{0}$ and R is a domain. Thus $o(a) = \infty$. Now suppose R has characteristic n. Then R contains $\mathbf{Z}_n$ as a subring, and thus $\mathbf{Z}_n$ is a domain and n is a prime. If a is a non-zero element of R, $na = \underline{n} \cdot a = \underline{0} \cdot a = \underline{0}$ and thus $o(a)|n$ and thus $o(a) = n$.

Exercise Show that if F is a field of characteristic 0, F contains $\mathbf{Q}$ as a subring. That is, show that the injective homomorphism $f : \mathbf{Z} \to F$ extends to an injective homomorphism $\bar{f} : \mathbf{Q} \to F$.

Boolean Rings

This section is not used elsewhere in this book. However it fits easily here, and is included for reference.

Definition A ring R is a *Boolean ring* if for each $a \in R$, $a^2 = a$, i.e., each element of R is an idempotent.

Theorem Suppose R is a Boolean ring.

1) R has characteristic 2. If $a \in R$, $2a = a + a = \underline{0}$, and so $a = -a$.

Proof $(a + a) = (a + a)^2 = a^2 + 2a^2 + a^2 = 4a$. Thus $2a = \underline{0}$.

2) R is commutative.

Proof $(a + b) = (a + b)^2 = a^2 + (a \cdot b) + (b \cdot a) + b^2$
$= a + (a \cdot b) - (b \cdot a) + b$. Thus $a \cdot b = b \cdot a$.

3) If R is a domain, $R \approx \mathbf{Z}_2$.

Proof Suppose $a \neq \underline{0}$. Then $a \cdot (\underline{1} - a) = \underline{0}$ and so $a = \underline{1}$.

4) The image of a Boolean ring is a Boolean ring. That is, if I is an ideal of R with $I \neq R$, then every element of R/I is idempotent and thus R/I is a Boolean ring. It follows from 3) that R/I is a domain iff R/I is a field iff $R/I \approx \mathbf{Z}_2$. (In the language of Chapter 6, I is a prime ideal iff I is a maximal ideal iff $R/I \approx \mathbf{Z}_2$).

Suppose X is a non-void set. If a is a subset of X, let $a' = (X - a)$ be a complement of a in X. Now suppose R is a non-void collection of subsets of X. Consider the following properties which the collection R may possess.

1) $a \in R \;\Rightarrow\; a' \in R$.
2) $a, b \in R \;\Rightarrow\; (a \cap b) \in R$.
3) $a, b \in R \;\Rightarrow\; (a \cup b) \in R$.
4) $\emptyset \in R$ and $X \in R$.

Theorem If 1) and 2) are satisfied, then 3) and 4) are satisfied. In this case, R is called a *Boolean algebra of sets.*

Proof Suppose 1) and 2) are true, and $a, b \in R$. Then $a \cup b = (a' \cap b')'$ belongs to R and so 3) is true. Since R is non-void, it contains some element a. Then $\emptyset = a \cap a'$ and $X = a \cup a'$ belong to R, and so 4) is true.

Theorem Suppose R is a Boolean algebra of sets. Define an addition on R by $a + b = (a \cup b) - (a \cap b)$. Under this addition, R is an abelian group with $\underline{0} = \emptyset$ and $a = -a$. Define a multiplication on R by $a \cdot b = a \cap b$. Under this multiplication R becomes a Boolean ring with $\underline{1} = X$.

Exercise Let $X = \{1, 2, ..., n\}$ and let R be the Boolean ring of all subsets of X. Note that $o(R) = 2^n$. Define $f_i : R \to \mathbf{Z}_2$ by $f_i(a) = [1]$ iff $i \in a$. Show each f_i is a homomorphism and thus $f = (f_1, ..., f_n) : R \to \mathbf{Z}_2 \times \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2$ is a ring homomorphism. Show f is an isomorphism. (See exercises 1) and 4) on page 12.)

Exercise Use the last exercise on page 49 to show that any finite Boolean ring is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2$, and thus also to the Boolean ring of subsets above.

Note Suppose R is a Boolean ring. It is a classical theorem that $\exists$ a Boolean algebra of sets whose Boolean ring is isomorphic to R. So let's just suppose R is a Boolean algebra of sets which is a Boolean ring with addition and multiplication defined as above. Now define $a \vee b = a \cup b$ and $a \wedge b = a \cap b$. These operations cup and cap are associative, commutative, have identity elements, and each distributes over the other. With these two operations (along with complement), R is called a *Boolean algebra.* R is not a group under cup or cap. Anyway, it is a classical fact that, if you have a Boolean ring (algebra), you have a Boolean algebra (ring). The advantage of the algebra is that it is symmetric in cup and cap. The advantage of the ring viewpoint is that you can draw from the rich theory of commutative rings.