has more than one Sylow p-subgroup and that any two distinct Sylow p-subgroups of $N_G(P \cap Q)$ intersect in the subgroup $P \cap Q$. (Thus $|N_G(P \cap Q)|$ is divisible by $p \cdot |P \cap Q|$ and by some prime other than p. Note that Sylow p-subgroups of $N_G(P \cap Q)$ need not be Sylow in G.)

14. Prove that there are no simple groups of order 144, 525, 2025 or 3159.

General exercises:

15. Classify groups of order 105.

16. Prove that there are no non-abelian simple groups of odd order < 10000.

17. **(a)** Prove that there is no simple group of order 420.
(b) Prove that there are no simple groups of even order < 500 except for orders 2, 60, 168 and 360.

18. Prove that if G is a group of order 36 then G has either a normal Sylow 2-subgroup or a normal Sylow 3-subgroup.

19. Show that a group of order 12 with no subgroup of order 6 is isomorphic to A_4.

20. Show that a group of order 24 with no element of order 6 is isomorphic to S_4.

21. Generalize Lemma 13 by proving that if $n_p \not\equiv 1 (\text{mod } p^k)$ then there are distinct Sylow p-subgroups P and R of G such that $P \cap R$ is of index $\leq p^{k-1}$ in both P and R.

22. Suppose over all pairs of distinct Sylow p-subgroups of G, P and R are chosen with $|P \cap R|$ maximal. Prove that $N_G(P \cap R)$ is not a p-group.

23. Let A and B be normal subsets of a Sylow p-subgroup P of G. Prove that if A and B are conjugate in G then they are conjugate in $N_G(P)$.

24. Let G be a group of order pqr where p, q and r are primes with $p < q < r$. Prove that a Sylow r-subgroup of G is normal.

25. Let G be a simple group of order p^2qr where p, q and r are primes. Prove that $|G| = 60$.

26. Prove or construct a counterexample to the assertion: if G is a group of order 168 with more than one Sylow 7-subgroup then G is simple.

27. Show that if $\mathcal{F}$ is any set of points and lines satisfying properties (11) to (13) in the subsection on simple groups of order 168 then the graph of incidences for $\mathcal{F}$ is uniquely determined and is the same as Figure 1 (up to relabeling points and lines). [Take a line and any point not on this line. Depict the line as the base of an equilateral triangle and the point as the vertex of this triangle not on the base. Use the axioms to show that the incidences of the remaining points and lines are then uniquely determined as in Figure 1.]

28. Let G be a simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$. Compute all permissible values of n_p for each $p \in \{3, 7, 13, 409\}$ and reduce to the case where there is a unique possible value for each n_p.

29. Given the information on the Sylow numbers for a hypothetical simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$, prove that there is no such group. [Work with the permutation representation of degree 819.]

30. Suppose G is a simple group of order 720. Find as many properties of G as you can (Sylow numbers, isomorphism type of Sylow subgroups, conjugacy classes, etc.). Is there such a group?

6.3 A WORD ON FREE GROUPS

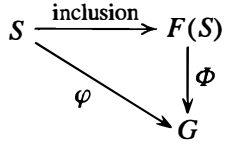
In this section we introduce the basic theory of so-called free groups. This will enable us to make precise the notions of generators and relations which were used in earlier chapters. The results of this section rely only on the basic theory of homomorphisms.

The basic idea of a free group $F(S)$ generated by a set S is that there are no relations satisfied by any of the elements in S (S is "free" of relations). For example, if S is the set $\{a, b\}$ then the elements of the free group on the two generators a and b are of the form a, aa, ab, $abab$, bab, etc., called *words* in a and b, together with the inverses of these elements, and all these elements are considered distinct. If we group like terms together, then we obtain elements of the familiar form a, b^{-3}, $aba^{-1}b^2$ etc. Such elements are multiplied by concatenating their words (for example, the product of aba and $b^{-1}a^3b$ would simply be $abab^{-1}a^3b$). It is natural at the outset (even before we know S is contained in some group) to simply *define* $F(S)$ to be the set of all words in S, where two such expressions are multiplied in $F(S)$ by concatenating them. Although in essence this is what we do, it is necessary to be more formal in order to prove that this concatenation operation is well defined and associative. After all, even the familiar notation a^n for the product $a \cdot a \cdots a$ (n terms) is permissible only because we know that this product is independent of the way it is bracketed (cf. the generalized associative law in Section 1.1). The formal construction of $F(S)$ is carried out below for an arbitrary set S.

One important property reflecting the fact that there are no relations that must be satisfied by the generators in S is that any *map* from the *set* S to a group G can be uniquely extended to a *homomorphism* from the *group* $F(S)$ to G (basically since we have specified where the generators must go and the images of all the other elements are uniquely determined by the homomorphism property — the fact that there are no relations to worry about means that we can specify the images of the generators *arbitrarily*). This is frequently referred to as the *universal* property of the free group and in fact characterizes the group $F(S)$.

The notion of "freeness" occurs in many algebraic systems and it may already be familiar (using a different terminology) from elementary vector space theory. When the algebraic systems are vector spaces, $F(S)$ is simply the vector space which has S as a basis. Every vector in this space is a unique linear combination of the elements of S (the analogue of a "word"). Any set map from the basis S to another vector space V extends uniquely to a linear transformation (i.e., vector space homomorphism) from $F(S)$ to V.

Before beginning the construction of $F(S)$ we mention that one often sees the universal property described in the language of commutative diagrams. In this form it reads (for groups) as follows: given any set map φ from the set S to a group G there is a unique homomorphism $\Phi : F(S) \to G$ such that $\Phi|_S = \varphi$ i.e., such that the following diagram commutes:



As mentioned above, the only difficulty with the construction of $F(S)$ is the verification that the concatenation operation on the words in $F(S)$ is well defined and associative. To prove the associative property for multiplication of words we return to the most basic level where all the exponents in the words of S are ± 1.

We first introduce inverses for elements of S and an identity.

Let S^{-1} be any set disjoint from S such that there is a bijection from S to S^{-1}. For each $s \in S$ denote its corresponding element in S^{-1} by s^{-1} and similarly for each $t \in S^{-1}$ let the corresponding element of S be denoted by t^{-1} (so $(s^{-1})^{-1} = s$). Take a singleton set not contained in $S \cup S^{-1}$ and call it $\{1\}$. Let $1^{-1} = 1$ and for any $x \in S \cup S^{-1} \cup \{1\}$ let $x^1 = x$.

Next we describe the elements of the free group on the set S. A *word* on S is by definition a sequence

$$(s_1, s_2, s_3, \dots) \quad \text{where } s_i \in S \cup S^{-1} \cup \{1\} \text{ and } s_i = 1 \text{ for all } i \text{ sufficiently large}$$

(that is, for each sequence there is an N such that $s_i = 1$ for all $i \geq N$). Thus we can think of a word as a finite product of elements of S and their inverses (where repetitions are allowed). Next, in order to assure uniqueness of expressions we consider only words which have no obvious "cancellations" between adjacent terms (such as $baa^{-1}b = bb$). The word $(s_1, s_2, s_3, \dots)$ is said to be *reduced* if

(1) $s_{i+1} \neq s_i^{-1}$ for all i with $s_i \neq 1$, and
(2) if $s_k = 1$ for some k, then $s_i = 1$ for all $i \geq k$.

The reduced word $(1, 1, 1, \dots)$ is called the *empty word* and is denoted by 1. We now simplify the notation by writing the reduced word $(s_1^{\epsilon_1}, s_2^{\epsilon_2}, \dots, s_n^{\epsilon_n}, 1, 1, 1, \dots)$, $s_i \in S$, $\epsilon_i = \pm 1$, as $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$. Note that by definition, reduced words $r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m}$ and $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$ are equal if and only if $n = m$ and $\delta_i = \epsilon_i$, $1 \leq i \leq n$. Let $F(S)$ be the set of reduced words on S and embed S into $F(S)$ by

$$s \mapsto (s, 1, 1, 1, \dots).$$

Under this set injection we identify S with its image and henceforth consider S as a subset of $F(S)$. Note that if $S = \emptyset$, $F(S) = \{1\}$.

We are now in a position to introduce the binary operation on $F(S)$. The principal technical difficulty is to ensure that the product of two reduced words is again a *reduced* word. Although the definition appears to be complicated it is simply the formal rule for "successive cancellation" of juxtaposed terms which are inverses of each other (e.g., $ab^{-1}a$ times $a^{-1}ba$ should reduce to aa). Let $r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m}$ and $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$ be reduced words and assume first that $m \leq n$. Let k be the smallest integer in the range $1 \leq k \leq m+1$ such that $s_k^{\epsilon_k} \neq r_{m-k+1}^{-\delta_{m-k+1}}$. Then the product of these reduced words is defined to be:

$$(r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m})(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = \begin{cases} r_1^{\delta_1} \dots r_{m-k+1}^{\delta_{m-k+1}} s_k^{\epsilon_k} \dots s_n^{\epsilon_n}, & \text{if } k \leq m \\ s_{m+1}^{\epsilon_{m+1}} \dots s_n^{\epsilon_n}, & \text{if } k = m+1 \leq n \\ 1, & \text{if } k = m+1 \text{ and } m = n. \end{cases}$$

The product is defined similarly when $m \geq n$, so in either case it results in a reduced word.

Theorem 16. $F(S)$ is a group under the binary operation defined above.

Proof: One easily checks that 1 is an identity and that the inverse of the reduced word $s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n}$ is the reduced word $s_n^{-\epsilon_n}s_{n-1}^{-\epsilon_{n-1}}\dots s_1^{-\epsilon_1}$. The difficult part of the proof is the verification of the associative law. This can be done by induction on the "length" of the words involved and considering various cases or one can proceed as follows: For each $s \in S \cup S^{-1} \cup \{1\}$ define $\sigma_s : F(S) \to F(S)$ by

$$\sigma_s(s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n}) = \begin{cases} s \cdot s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n}, & \text{if } s_1^{\epsilon_1} \neq s^{-1} \\ s_2^{\epsilon_2}s_3^{\epsilon_3}\dots s_n^{\epsilon_n}, & \text{if } s_1^{\epsilon_1} = s^{-1}. \end{cases}$$

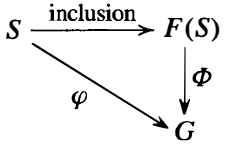
Since $\sigma_{s^{-1}} \circ \sigma_s$ is the identity map of $F(S) \to F(S)$, σ_s is a permutation of $F(S)$. Let $A(F)$ be the subgroup of the symmetric group on the set $F(S)$ which is generated by $\{\sigma_s \mid s \in S\}$. It is easy to see that the map

$$s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n} \mapsto \sigma_{s_1}^{\epsilon_1} \circ \sigma_{s_2}^{\epsilon_2} \circ \dots \circ \sigma_{s_n}^{\epsilon_n}$$

is a (set) bijection between $F(S)$ and $A(S)$ which respects their binary operations. Since $A(S)$ is a group, hence associative, so is $F(S)$.

The universal property of free groups now follows easily.

Theorem 17. Let G be a group, S a set and $\varphi : S \to G$ a set map. Then there is a unique group homomorphism $\Phi : F(S) \to G$ such that the following diagram commutes:



Proof: Such a map Φ must satisfy $\Phi(s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n}) = \varphi(s_1)^{\epsilon_1}\varphi(s_2)^{\epsilon_2}\dots\varphi(s_n)^{\epsilon_n}$ if it is to be a homomorphism (which proves uniqueness), and it is straightforward to check that this map is in fact a homomorphism (which proves existence).

Corollary 18. $F(S)$ is unique up to a unique isomorphism which is the identity map on the set S.

Proof: This follows from the universal property. Suppose $F(S)$ and $F'(S)$ are two free groups generated by S. Since S is contained in both $F(S)$ and $F'(S)$, we have natural injections $S \hookrightarrow F'(S)$ and $S \hookrightarrow F(S)$. By the universal property in the theorem, it follows that we have unique associated group homomorphisms $\Phi : F(S) \to F'(S)$ and $\Phi' : F'(S) \to F(S)$ which are both the identity on S. The composite $\Phi'\Phi$ is a homomorphism from $F(S)$ to $F(S)$ which is the identity on S, so by the uniqueness statement in the theorem, it must be the identity map. Similarly $\Phi\Phi'$ is the identity, so Φ is an isomorphism (with inverse Φ'), which proves the corollary.

Definition. The group $F(S)$ is called the *free group* on the set S. A group F is a *free group* if there is some set S such that $F = F(S)$ — in this case we call S a set of *free generators* (or a *free basis*) of F. The cardinality of S is called the *rank* of the free group.

One can now simplify expressions in a free group by using exponential notation, so we write a^3b^{-2} instead of the formal reduced word $aaab^{-1}b^{-1}$. Expressions like aba, however, cannot be simplified in the free group on $\{a, b\}$. We mention one important theorem in this area.

Theorem 19. (Schreier) Subgroups of a free group are free.

This is not trivial to prove and we do not include a proof. There is a nice proof of this result using covering spaces (cf. *Trees* by J.-P. Serre, Springer-Verlag, 1980).

Presentations

Let G be any group. Then G is a homomorphic image of a free group: take $S = G$ and φ as the identity map from G to G; then Theorem 16 produces a (surjective) homomorphism from $F(G)$ onto G. More generally, if S is any subset of G such that $G = \langle S \rangle$, then again there is a unique surjective homomorphism from $F(S)$ onto G which is the identity on S. (Note that we can now independently formulate the notion that a subset *generates* a group by noting that $G = \langle S \rangle$ if and only if the map $\pi : F(S) \to G$ which extends the identity map of S to G is surjective.)

Definition. Let S be a subset of a group G such that $G = \langle S \rangle$.

(1) A *presentation* for G is a pair (S, R), where R is a set of words in $F(S)$ such that the normal closure of $\langle R \rangle$ in $F(S)$ (the smallest normal subgroup containing $\langle R \rangle$) equals the kernel of the homomorphism $\pi : F(S) \to G$ (where π extends the identity map from S to S). The elements of S are called *generators* and those of R are called *relations* of G.

(2) We say G is *finitely generated* if there is a presentation (S, R) such that S is a finite set and we say G is *finitely presented* if there is a presentation (S, R) with both S and R finite sets.

Note that if (S, R) is a presentation, the kernel of the map $F(S) \to G$ is not $\langle R \rangle$ itself but rather the (much larger) group generated by R and *all conjugates* of elements in R. Note that even for a fixed set S a group will have many different presentations (we can always throw redundant relations into R, for example). If G is finitely presented with $S = \{s_1, s_2, \ldots, s_n\}$ and $R = \{w_1, w_2, \ldots, w_k\}$, we write (as we have in preceding chapters):

$$G = \langle s_1, s_2, \ldots, s_n \mid w_1 = w_2 = \cdots = w_k = 1 \rangle$$

and if w is the word $w_1 w_2^{-1}$, we shall write $w_1 = w_2$ instead of $w = 1$.

Examples

(1) Every finite group is finitely presented. To see this let $G = \{g_1, \ldots, g_n\}$ be a finite group. Let $S = G$ and let $\pi : F(S) \to G$ be the homomorphism extending the identity map of S. Let R_0 be the set of words $g_i g_j g_k^{-1}$, where $i, j = 1, \ldots, n$ and $g_i g_j = g_k$ in G. Clearly $R_0 \leq \ker \pi$. If N is the normal closure of R_0 in $F(S)$ and $\widetilde{G} = F(S)/N$, then G is a homomorphic image of $\widetilde{G}$ (i.e., π factors through N). Moreover, the set of elements $\{\widetilde{g}_i \mid i = 1, \ldots, n\}$ is closed under multiplication. Since this set generates $\widetilde{G}$, it must equal $\widetilde{G}$. Thus $|\widetilde{G}| = |G|$ and so $N = \ker \pi$ and (S, R_0) is a presentation of G.

This illustrates a sufficient condition for (S, R) to be a presentation for a given finite group G:

(i) S must be a generating set for G, and

(ii) any group generated by S satisfying the relations in R must have order $\leq |G|$.

(2) Abelian groups can be presented easily. For instance

$$\mathbb{Z} \cong F(\{a\}) = \langle a \rangle,$$
$$\mathbb{Z} \times \mathbb{Z} \cong \langle a, b \mid [a, b] = 1 \rangle,$$
$$Z_n \times Z_m \cong \langle a, b \mid a^n = b^m = [a, b] = 1 \rangle.$$

(Recall $[a, b] = a^{-1}b^{-1}ab$).

(3) Some familiar non-abelian groups introduced in earlier chapters have simple presentations:

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ s^{-1}rs = r^{-1} \rangle$$
$$Q_8 = \langle i, j \mid i^4 = 1,\ j^2 = i^2,\ j^{-1}ij = i^{-1} \rangle.$$

To check, for example, the presentation for D_{2n} note that the relations in the presentation $\langle r, s \mid r^n = s^2 = 1,\ s^{-1}rs = r^{-1} \rangle$ imply that this group has a normal subgroup (generated by r) of order $\leq n$ whose quotient is generated by s (which has order ≤ 2). Thus any group with these generators and relations has order at most $2n$. Since we already know of the existence of the group D_{2n} of order $2n$ satisfying these conditions, the abstract presentation must equal D_{2n}.

(4) As mentioned in Section 1.2, in general it is extremely difficult even to determine if a given set of generators and relations is or is not the identity group (let alone determine whether it is some other nontrivial finite group). For example, in the following two presentations the first group is an *infinite* group and the second is the *identity* group (cf. *Trees*, Chapter 1):

$$\langle x_1, x_2, x_3, x_4 \mid x_2x_1x_2^{-1} = x_1^2,\ x_3x_2x_3^{-1} = x_2^2,\ x_4x_3x_4^{-1} = x_3^2,\ x_1x_4x_1^{-1} = x_4^2 \rangle$$
$$\langle x_1, x_2, x_3, \mid x_2x_1x_2^{-1} = x_1^2,\ x_3x_2x_3^{-1} = x_2^2,\ x_1x_3x_1^{-1} = x_3^2 \rangle.$$

(5) It is easy to see that S_n is generated by the transpositions $(1\,2), (2\,3), \ldots, (n-1\,n)$, and that these satisfy the relations

$$((i\,i{+}1)(i{+}1\,i{+}2))^3 = 1 \quad \text{and} \quad [(i\,i{+}1), (j\,j{+}1)] = 1, \text{ whenever } |i - j| \geq 2$$

(here $|i-j|$ denotes the absolute value of the integer $i-j$). One can prove by induction on n that these form a presentation of S_n:

$$S_n \cong \langle t_1, \ldots, t_{n-1} \mid t_i^2 = 1,\ (t_it_{i+1})^3 = 1, \text{ and } [t_i, t_j] = 1 \text{ whenever } |i - j| \geq 2,\ 1 \leq i, j \leq n-1 \rangle.$$

As mentioned in Section 1.6 we can use presentations of a group to find homomorphisms between groups or to find automorphisms of a group. We did this in classifying groups of order 6, for example, when we proved that any non-abelian group of order 6 was generated by an element of order 3 and an element of order 2 inverting it; thus there is a homomorphism from S_3 onto any non-abelian group of order 6 (hence an isomorphism, by computing orders). More generally, suppose G is presented by, say, generators a, b with relations $r_1, \ldots, r_k$. If a', b' are any elements of a group H satisfying these relations, there is a homomorphism from G into H. Namely, if $\pi : F(\{a, b\}) \to G$ is the presentation homomorphism, we can define $\pi' : F(\{a, b\}) \to H$ by $\pi'(a) = a'$ and $\pi'(b) = b'$. Then $\ker \pi \leq \ker \pi'$ so π' factors through $\ker \pi$ and we obtain

$$G \cong F(\{a, b\})/\ker \pi \longrightarrow H.$$

In, particular, if $\langle a', b' \rangle = H = G$, this homomorphism is an automorphism of G. Conversely, any automorphism must send a set of generators to another set of generators satisfying the same relations. For example, $D_8 = \langle a, b \mid a^2 = b^4 = 1,\ aba = b^{-1} \rangle$ and any pair a', b' of elements, where a' is a noncentral element of order 2 and b' is of order 4, satisfies the same relations. Since there are four noncentral elements of order 2 and two elements of order 4, D_8 has 8 automorphisms.

Similarly, any pair of elements of order 4 in Q_8 which are not equal or inverses of each other necessarily generate Q_8 and satisfy the relations given in Example 3 above. It is easy to check that there are 24 such pairs, so

$$|\mathrm{Aut}(Q_8)| = 24.$$

Free objects can be constructed in (many, but not all) other categories. For instance, a *monoid* is a set together with a binary operation satisfying all of the group axioms except the axiom specifying the existence of inverses. Free objects in the category of monoids play a fundamental role in theoretical computer science where they model the behavior of machines (Turing machines, etc.). We shall encounter free algebras (i.e., polynomial algebras) and free modules in later chapters.

EXERCISES

1. Let F_1 and F_2 be free groups of finite rank. Prove that $F_1 \cong F_2$ if and only if they have the same rank. What facts do you need in order to extend your proof to infinite ranks (where the result is also true)?
2. Prove that if $|S| > 1$ then $F(S)$ is non-abelian.
3. Prove that the commutator subgroup of the free group on 2 generators is not finitely generated (in particular, subgroups of finitely generated groups need not be finitely generated).
4. Prove that every nonidentity element of a free group is of infinite order.
5. Establish a finite presentation for A_4 using 2 generators.
6. Establish a finite presentation for S_4 using 2 generators.
7. Prove that the following is a presentation for the quaternion group of order 8:
$$Q_8 = \langle a, b \mid a^2 = b^2,\ a^{-1}ba = b^{-1} \rangle.$$
8. Use presentations to find the orders of the automorphism groups of the groups $Z_2 \times Z_4$ and $Z_4 \times Z_4$.

9. Prove that $\mathrm{Aut}(Q_8) \cong S_4$.

10. This exercise exhibits an automorphism of S_6 that is not inner (hence, together with Exercise 19 in Section 4.4 it shows that $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$). Let $t_1' = (1\ 2)(3\ 4)(5\ 6)$, $t_2' = (1\ 4)(2\ 5)(3\ 6)$, $t_3' = (1\ 3)(2\ 4)(5\ 6)$, $t_4' = (1\ 2)(3\ 6)(4\ 5)$, and $t_5' = (1\ 4)(2\ 3)(5\ 6)$. Show that $t_1', \ldots, t_5'$ satisfy the following relations:

$(t_i')^2 = 1$ for all i,

$(t_i't_j')^2 = 1$ for all i and j with $|i - j| \geq 2$, and

$(t_i't_{i+1}')^3 = 1$ for all $i \in \{1, 2, 3, 4\}$.

Deduce that $S_6 = \langle t_1', \ldots, t_5' \rangle$ and that the map

$$(1\ 2) \mapsto t_1', \quad (2\ 3) \mapsto t_2', \quad (3\ 4) \mapsto t_3', \quad (4\ 5) \mapsto t_4', \quad (5\ 6) \mapsto t_5'$$

extends to an automorphism of S_6 (which is clearly not inner since it does not send transpositions to transpositions). [Use the presentation for S_6 described in Example 5.]

11. Let S be a set. The group with presentation (S, R), where $R = \{[s, t] \mid s, t \in S\}$ is called the *free abelian* group on S — denote it by $A(S)$. Prove that $A(S)$ has the following universal property: if G is any abelian group and $\varphi : S \to G$ is any set map, then there is a unique group homomorphism $\Phi : A(S) \to G$ such that $\Phi|_S = \varphi$. Deduce that if A is a free abelian group on a set of cardinality n then

$$A \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \quad (n \text{ factors}).$$

12. Let S be a set and let c be a positive integer. Formulate the notion of a *free nilpotent group* on S of nilpotence class c and prove it has the appropriate universal property with respect to nilpotent groups of class $\leq c$.

13. Prove that there cannot be a nilpotent group N generated by two elements with the property that *every* nilpotent group which is generated by two elements is a homomorphic image of N (i.e., the specification of the class c in the preceding problem was necessary).

Part II

RING THEORY

The theory of groups is concerned with general properties of certain objects having an algebraic structure defined by a single binary operation. The study of rings is concerned with objects possessing two binary operations (called addition and multiplication) related by the distributive laws. We first study analogues for the basic points of development in the structure theory of groups. In particular, we introduce subrings, quotient rings, ideals (which are the analogues of normal subgroups) and ring homomorphisms. We then focus on questions about general rings which arise naturally from the presence of two binary operations. Questions concerning multiplicative inverses lead to the notion of fields and eventually to the construction of some specific fields such as finite fields. The study of the arithmetic (divisibility, greatest common divisors, etc.) of rings such as the familiar ring of integers, $\mathbb{Z}$, leads to the notion of primes and unique factorizations in Chapter 8. The results of Chapters 7 and 8 are then applied to rings of polynomials in Chapter 9.

The basic theory of rings developed in Part II is the cornerstone for the remaining four parts of the book. The theory of ring actions (modules) comprises Part III of the book. There we shall see how the structure of rings is reflected in the structure of the objects on which they act and this will enable us to prove some powerful classification theorems. The structure theory of rings, in particular of polynomial rings, forms the basis in Part IV for the theory of fields and polynomial equations over fields. There the rich interplay among ring theory, field theory and group theory leads to many beautiful results on the structure of fields and the theory of roots of polynomials. Part V continues the study of rings and applications of ring theory to such topics as geometry and the theory of extensions. In Part VI the study of certain specific kinds of rings (group rings) and the objects (modules) on which they act again gives deep classification theorems whose consequences are then exploited to provide new results and insights into finite groups.

CHAPTER 7

Introduction to Rings

7.1 BASIC DEFINITIONS AND EXAMPLES

Definition.

(1) A *ring* R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

(i) $(R, +)$ is an *abelian* group,

(ii) $\times$ is associative : $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$,

(iii) the *distributive laws* hold in R : for all $a, b, c \in R$

$$(a+b)\times c = (a\times c)+(b\times c) \quad \text{and} \quad a\times(b+c) = (a\times b)+(a\times c).$$

(2) The ring R is *commutative* if multiplication is commutative.

(3) The ring R is said to have an *identity* (or *contain a* 1) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \qquad \text{for all } a \in R.$$

We shall usually write simply ab rather than $a \times b$ for $a, b \in R$. The additive identity of R will always be denoted by 0 and the additive inverse of the ring element a will be denoted by $-a$.

The condition that R be a group under addition is a fairly natural one, but it may seem artificial to require that this group be *abelian.* One motivation for this is that if the ring R has a 1, the commutativity under addition is *forced* by the distributive laws. To see this, compute the product $(1+1)(a+b)$ in two different ways, using the distributive laws (but not assuming that addition is commutative). One obtains

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

and

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

Since R is a group under addition, this implies $b+a = a+b$, i.e., that R under addition is necessarily commutative.

Fields are one of the most important examples of rings. Note that their definition below is just another formulation of the one given in Section 1.4.

Definition. A ring R with identity 1, where $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field*.

More examples of rings follow.

Examples

(1) The simplest examples of rings are the *trivial rings* obtained by taking R to be any commutative group (denoting the group operation by $+$) and defining the multiplication $\times$ on R by $a \times b = 0$ for all $a, b \in R$. It is easy to see that this multiplication defines a commutative ring. In particular, if $R = \{0\}$ is the trivial group, the resulting ring R is called the *zero ring*, denoted $R = 0$. Except for the zero ring, a trivial ring does not contain an identity ($R = 0$ is the only ring where $1 = 0$; we shall often exclude this ring by imposing the condition $1 \neq 0$). Although trivial rings have two binary operations, multiplication adds no new structure to the additive group and the theory of rings gives no information which could not already be obtained from (abelian) group theory.

(2) The ring of integers, $\mathbb{Z}$, under the usual operations of addition and multiplication is a commutative ring with identity (the integer 1). The ring axioms (as with the additive group axioms) follow from the basic axioms for the system of natural numbers. Note that under *multiplication* $\mathbb{Z} - \{0\}$ is *not* a group (in fact, there are very few multiplicative inverses to elements in this ring). We shall come back to the question of these inverses shortly.

(3) Similarly, the rational numbers, $\mathbb{Q}$, the real numbers, $\mathbb{R}$, and the complex numbers, $\mathbb{C}$, are commutative rings with identity (in fact they are fields). The ring axioms for each of these follow ultimately from the ring axioms for $\mathbb{Z}$. We shall verify this when we construct $\mathbb{Q}$ from $\mathbb{Z}$ (Section 7.5) and $\mathbb{C}$ from $\mathbb{R}$ (Example 1, Section 13.1); both of these constructions will be special cases of more general processes. The construction of $\mathbb{R}$ from $\mathbb{Q}$ (and subsequent verification of the ring axioms) is carried out in basic analysis texts.

(4) The quotient group $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity (the element $\bar{1}$) under the operations of addition and multiplication of residue classes (frequently referred to as "modular arithmetic"). We saw that the additive abelian group axioms followed from the general principles of the theory of quotient groups (indeed this was the prototypical quotient group). We shall shortly prove that the remaining ring axioms (in particular, the fact that multiplication of residue classes is well defined) follow analogously from the general theory of quotient rings.

In all of the examples so far the rings have been commutative. Historically, one of the first noncommutative rings was discovered in 1843 by Sir William Rowan Hamilton (1805–1865). This ring, which is a division ring, was extremely influential in the subsequent development of mathematics and it continues to play an important role in certain areas of mathematics and physics.

(5) (The *(real) Hamilton Quaternions*) Let $\mathbb{H}$ be the collection of elements of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ are real numbers (loosely, "polynomials in $1, i, j, k$ with real coefficients") where addition is defined "componentwise" by

$$(a+bi+cj+dk) + (a'+b'i+c'j+d'k) = (a+a') + (b+b')i + (c+c')j + (d+d')k$$

and multiplication is defined by expanding $(a + bi + cj + dk)(a' + b'i + c'j + d'k)$ using the distributive law (being careful about the order of terms) and simplifying

using the relations

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

(where the real number coefficients commute with i, j and k). For example,

$$\begin{aligned}(1+i+2j)(j+k) &= 1(j+k) + i(j+k) + 2j(j+k) = j + k + ij + ik + 2j^2 + 2jk \\ &= j + k + k + (-j) + 2(-1) + 2(i) = -2 + 2i + 2k.\end{aligned}$$

The fact that $\mathbb{H}$ is a ring may be proved by a straightforward, albeit lengthy, check of the axioms (associativity of multiplication is particularly tedious). The Hamilton Quaternions are a noncommutative ring with identity ($1 = 1+0i+0j+0k$). Similarly, one can define the ring of *rational* Hamilton Quaternions by taking a, b, c, d to be rational numbers above. Both the real and rational Hamilton Quaternions are *division rings*, where inverses of nonzero elements are given by

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

(6) One important class of rings is obtained by considering rings of functions. Let X be any nonempty set and let A be any ring. The collection, R, of all (set) functions $f : X \to A$ is a ring under the usual definition of pointwise addition and multiplication of functions: $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. Each ring axiom for R follows directly from the corresponding axiom for A. The ring R is commutative if and only if A is commutative and R has a 1 if and only if A has a 1 (in which case the 1 of R is necessarily the constant function 1 on X).

If X and A have more structure, we may form other rings of functions which respect those structures. For instance, if A is the ring of real numbers $\mathbb{R}$ and X is the closed interval $[0, 1]$ in $\mathbb{R}$ we may form the ring of all *continuous* functions from $[0, 1]$ to $\mathbb{R}$ (here we need basic limit theorems to guarantee that sums and products of continuous functions are continuous) — this is a commutative ring with 1.

(7) An example of a ring which does not have an identity is the ring $2\mathbb{Z}$ of even integers under usual addition and multiplication of integers (the sum and product of even integers is an even integer).

Another example which arises naturally in analysis is constructed as follows. A function $f : \mathbb{R} \to \mathbb{R}$ is said to have *compact support* if there are real numbers a, b (depending on f) such that $f(x) = 0$ for all $x \notin [a, b]$ (i.e., f is zero outside some bounded interval). The set of all functions $f : \mathbb{R} \to \mathbb{R}$ with compact support is a commutative ring without identity (since an identity could not have compact support). Similarly, the set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ with compact support is a commutative ring without identity.

In the next section we give three important ways of constructing "larger" rings from a given ring (analogous to Example 6 above) and thus greatly expand our list of examples. Before doing so we mention some basic properties of arbitrary rings. The ring $\mathbb{Z}$ is a good example to keep in mind, although this ring has a good deal more algebraic structure than a general ring (for example, it is commutative and has an identity). Nonetheless, its basic arithmetic holds for general rings as the following result shows.

Proposition 1. Let R be a ring. Then

(1) $0a = a0 = 0$ for all $a \in R$.

(2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$ (recall $-a$ is the additive inverse of a).

(3) $(-a)(-b) = ab$ for all $a, b \in R$.

(4) if R has an identity 1, then the identity is unique and $-a = (-1)a$.

Proof: These all follow from the distributive laws and cancellation in the additive group R. For example, (1) follows from $0a = (0 + 0)a = 0a + 0a$. The equality $(-a)b = -(ab)$ in (2) follows from $ab + (-a)b = (a + (-a))b = 0b = 0$. The rest follow similarly and are left to the reader.

This proposition shows that because of the distributive laws the additive and multiplicative structures of a ring behave well with respect to one another, just as in the familiar example of the integers.

Unlike the integers, however, general rings may possess many elements that have multiplicative inverses or may have nonzero elements a and b whose product is zero. These two properties of elements, which relate to the multiplicative structure of a ring, are given special names.

Definition. Let R be a ring.

(1) A nonzero element a of R is called a *zero divisor* if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.

(2) Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some v in R such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.

It is easy to see that the units in a ring R form a group under multiplication so $R^\times$ will be referred to as the *group of units* of R. In this terminology a *field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F - \{0\}$.*

Observe that *a zero divisor can never be a unit.* Suppose for example that a is a unit in R and that $ab = 0$ for some nonzero b in R. Then $va = 1$ for some $v \in R$, so $b = 1b = (va)b = v(ab) = v0 = 0$, a contradiction. Similarly, if $ba = 0$ for some nonzero b then a cannot be a unit.

This shows in particular that fields contain no zero divisors.

Examples

(1) The ring $\mathbb{Z}$ of integers has no zero divisors and its only units are ± 1, i.e., $\mathbb{Z}^\times = \{\pm 1\}$. Note that every nonzero integer has an inverse in the *larger ring* $\mathbb{Q}$, so the property of being a unit depends on the ring in which an element is viewed.

(2) Let n be an integer ≥ 2. In the ring $\mathbb{Z}/n\mathbb{Z}$ the elements $\bar{u}$ for which u and n are relatively prime are units (we shall prove this in the next chapter). Thus our use of the notation $(\mathbb{Z}/n\mathbb{Z})^\times$ is consistent with the definition of the group of units in an arbitrary ring.

If, on the other hand, a is a nonzero integer and a is not relatively prime to n then we show that $\bar{a}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$. To see this let d be the g.c.d. of a and n and let $b = \dfrac{n}{d}$. By assumption $d > 1$ so $0 < b < n$, i.e., $\bar{b} \neq \bar{0}$. But by construction n

divides ab, that is, $\overline{ab} = \bar{0}$ in $\mathbb{Z}/n\mathbb{Z}$. This shows that *every nonzero element of* $\mathbb{Z}/n\mathbb{Z}$ *is either a unit or a zero divisor.* Furthermore, every nonzero element is a unit if and only if every integer a in the range $0 < a < n$ is relatively prime to n. This happens if and only if n is a prime, i.e., $\mathbb{Z}/n\mathbb{Z}$ *is a field if and only if* n *is a prime.*

(3) If R is the ring of all functions from the closed interval $[0,1]$ to $\mathbb{R}$ then the units of R are the functions that are not zero at any point (for such f its inverse is the function $\frac{1}{f}$). If f is not a unit and not zero then f is a zero divisor because if we define

$$g(x) = \begin{cases} 0, & \text{if } f(x) \neq 0 \\ 1, & \text{if } f(x) = 0 \end{cases}$$

then g is not the zero function but $f(x)g(x) = 0$ for all x.

(4) If R is the ring of all *continuous* functions from the closed interval $[0,1]$ to $\mathbb{R}$ then the units of R are still the functions that are not zero at any point, but now there are functions that are neither units nor zero divisors. For instance, $f(x) = x - \frac{1}{2}$ has only one zero (at $x = \frac{1}{2}$) so f is not a unit. On the other hand, if $gf = 0$ then g must be zero for all $x \neq \frac{1}{2}$, and the only *continuous* function with this property is the zero function. Hence f is neither a unit nor a zero divisor. Similarly, no function with only a finite (or countable) number of zeros on $[0,1]$ is a zero divisor. This ring also contains many zero divisors. For instance let

$$f(x) = \begin{cases} 0, & 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2}, & \frac{1}{2} \leq x \leq 1 \end{cases}$$

and let $g(x) = f(1 - x)$. Then f and g are nonzero continuous functions whose product is the zero function.

(5) Let D be a rational number that is not a perfect square in $\mathbb{Q}$ and define

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$$

as a subset of $\mathbb{C}$. This set is clearly closed under subtraction, and the identity $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$ shows that it is also closed under multiplication. Hence $\mathbb{Q}(\sqrt{D})$ is a subring of $\mathbb{C}$ (even a subring of $\mathbb{R}$ if $D > 0$), so in particular is a commutative ring with identity. It is easy to show that the assumption that D is not a square implies that every element of $\mathbb{Q}(\sqrt{D})$ may be written uniquely in the form $a + b\sqrt{D}$. This assumption also implies that if a and b are not both 0 then $a^2 - Db^2$ is nonzero, and since $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$ it follows that if $a + b\sqrt{D} \neq 0$ (i.e., one of a or b is nonzero) then $\dfrac{a - b\sqrt{D}}{a^2 - Db^2}$ is the inverse of $a + b\sqrt{D}$ in $\mathbb{Q}(\sqrt{D})$. This shows that every nonzero element in this commutative ring is a unit, i.e., $\mathbb{Q}(\sqrt{D})$ is a field (called a *quadratic field*, cf. Section 13.2).

The rational number D may be written $D = f^2 D'$ for some rational number f and a unique integer D' where D' is not divisible by the square of any integer greater than 1, i.e., D' is either -1 or ± 1 times the product of distinct primes in $\mathbb{Z}$ (for example, $8/5 = (2/5)^2 \cdot 10$). Call D' the *squarefree part* of D. Then $\sqrt{D} = f\sqrt{D'}$, and so $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$. Thus *there is no loss in assuming that* D *is a squarefree integer* (i.e., $f = 1$) *in the definition of the quadratic field* $\mathbb{Q}(\sqrt{D})$.

Rings having some of the same characteristics as the integers $\mathbb{Z}$ are given a name:

Definition. A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

The absence of zero divisors in integral domains give these rings a cancellation property:

Proposition 2. Assume a, b and c are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a's). In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Proof: If $ab = ac$ then $a(b - c) = 0$ so either $a = 0$ or $b - c = 0$. The second statement follows from the first and the definition of an integral domain.

Corollary 3. Any finite integral domain is a field.

Proof: Let R be a finite integral domain and let a be a nonzero element of R. By the cancellation law the map $x \mapsto ax$ is an injective function. Since R is finite this map is also surjective. In particular, there is some $b \in R$ such that $ab = 1$, i.e., a is a unit in R. Since a was an arbitrary nonzero element, R is a field.

A remarkable result of Wedderburn is that a finite division ring is necessarily commutative, i.e., is a field. A proof of this theorem is outlined in the exercises at the end of Section 13.6.

In Section 5 we study the relation between zero divisors and units in greater detail. We shall see that every nonzero element of a commutative ring that is not a zero divisor has a multiplicative inverse in some larger ring. This gives another perspective on the cancellation law in Proposition 2.

Having defined the notion of a ring, there is a natural notion of a subring.

Definition. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

In other words, a subset S of a ring R is a subring if the operations of addition and multiplication in R when restricted to S give S the structure of a ring. To show that a subset of a ring R is a subring it suffices to check that it is *nonempty* and *closed under subtraction and under multiplication.*

Examples

A number of the examples above were also subrings.

(1) $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$. The property "is a subring of" is clearly transitive.

(2) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$, as is $n\mathbb{Z}$ for any integer n. The ring $\mathbb{Z}/n\mathbb{Z}$ is not a subring (or a subgroup) of $\mathbb{Z}$ for any $n \geq 2$.

(3) The ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ is a subring of the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$. The ring of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ is a subring of both of these.

(4) $S = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$, the *integral* Quaternions, form a subring of either the real or the rational Quaternions — it is easy to check that multiplying two such quaternions together gives another quaternion with integer coefficients. This ring (which is not a division ring) can be used to give proofs for a number of results in number theory.

(5) If R is a subring of a field F that contains the identity of F then R is an integral domain. The converse of this is also true, namely any integral domain is contained in a field (cf. Section 5).

Example: (Quadratic Integer Rings)

Let D be a squarefree integer. It is immediate from the addition and multiplication that the subset $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ forms a subring of the quadratic field $\mathbb{Q}(\sqrt{D})$ defined earlier. If $D \equiv 1 \bmod 4$ then the slightly larger subset

$$\mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{a + b\frac{1+\sqrt{D}}{2} \mid a, b \in \mathbb{Z}\}$$

is also a subring: closure under addition is immediate and $(a + b\frac{1+\sqrt{D}}{2})(c + d\frac{1+\sqrt{D}}{2}) = (ac + bd\frac{D-1}{4}) + (ad + bc + bd)\frac{1+\sqrt{D}}{2}$ together with the congruence on D shows closure under multiplication.

Define

$$\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

where

$$\omega = \begin{cases} \sqrt{D}, & \text{if } D \equiv 2, 3 \bmod 4 \\ \dfrac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \bmod 4, \end{cases}$$

called the *ring of integers* in the quadratic field $\mathbb{Q}(\sqrt{D})$. The terminology comes from the fact that the elements of the subring $\mathcal{O}$ of the field $\mathbb{Q}(\sqrt{D})$ have many properties analogous to those of the subring of integers $\mathbb{Z}$ in the field of rational numbers $\mathbb{Q}$ (and are the *integral closure* of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{D})$ as explained in Section 15.3).

In the special case when $D = -1$ we obtain the ring $\mathbb{Z}[i]$ of *Gaussian integers*, which are the complex numbers $a + bi \in \mathbb{C}$ with a and b both *integers*. These numbers were originally introduced by Gauss around 1800 in order to state the biquadratic reciprocity law which deals with the beautiful relations that exist among fourth powers modulo primes. We shall shortly see another useful application of the algebraic structure of this ring to number theoretic questions.

Define the *field norm* $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ by

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Q},$$

which, as previously mentioned, is nonzero if $a + b\sqrt{D} \neq 0$. This norm gives a measure of "size" in the field $\mathbb{Q}(\sqrt{D})$. For instance when $D = -1$ the norm of $a + bi$ is $a^2 + b^2$, which is the square of the length of this complex number considered as a vector in the complex plane. We shall use the field norm in this and subsequent examples to establish many properties of the rings $\mathcal{O}$.

It is easy to check that N is *multiplicative*, i.e., that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$. On the subring $\mathcal{O}$ it is also easy to see that the field norm is given by

$$N(a+b\omega) = (a+b\omega)(a+b\overline{\omega}) = \begin{cases} a^2 - Db^2, & \text{if } D \equiv 2, 3 \bmod 4 \\ a^2 + ab + \dfrac{1-D}{4}b^2, & \text{if } D \equiv 1 \bmod 4 \end{cases}$$

where

$$\overline{\omega} = \begin{cases} -\sqrt{D}, & \text{if } D \equiv 2, 3 \bmod 4 \\ \dfrac{1-\sqrt{D}}{2}, & \text{if } D \equiv 1 \bmod 4. \end{cases}$$

It follows that $N(\alpha)$ is in fact an *integer* for every $\alpha \in \mathcal{O}$.

We may use this norm to characterize the units in $\mathcal{O}$. If $\alpha \in \mathcal{O}$ has field norm $N(\alpha) = \pm 1$, the previous formula shows that $(a+b\omega)^{-1} = \pm(a+b\overline{\omega})$, which is again an element of $\mathcal{O}$ and so α is a unit in $\mathcal{O}$. Suppose conversely that α is a unit in $\mathcal{O}$, say $\alpha\beta = 1$ for some $\beta \in \mathcal{O}$. Then the multiplicative property of the field norm implies that $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Since both $N(\alpha)$ and $N(\beta)$ are integers, each must be ± 1. Hence,

the element α is a unit in $\mathcal{O}$ if and only if $N(\alpha) = \pm 1$.

In particular the determination of the integer solutions to the equation $x^2 - Dy^2 = \pm 1$ (called *Pell's equation* in elementary number theory) is essentially equivalent to the determination of the units in the ring $\mathcal{O}$.

When $D = -1$, the units in the Gaussian integers $\mathbb{Z}[i]$ are the elements $a + bi$ with $a^2 + b^2 = \pm 1$, $a, b \in \mathbb{Z}$, so the group of units consists of $\{\pm 1, \pm i\}$. When $D = -3$, the units in $\mathbb{Z}[(1+\sqrt{-3})/2]$ are determined by the integers a, b with $a^2 + ab + b^2 = \pm 1$, i.e., with $(2a+b)^2 + 3b^2 = \pm 4$, from which it is easy to see that the group of units is a group of order 6 given by $\{\pm 1, \pm\rho, \pm\rho^2\}$ where $\rho = (-1+\sqrt{-3})/2$. For any other $D < 0$ it is similarly straightforward to see that the only units are $\{\pm 1\}$.

By contrast, when $D > 0$ it can be shown that the group of units $\mathcal{O}^\times$ is always infinite. For example, it is easy to check that $1 + \sqrt{2}$ is a unit in the ring $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ (with field norm -1) and that $\{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$, is an infinite set of distinct units (in fact the full group of units in this case, but this is harder to prove).

EXERCISES

Let R be a ring with 1.

1. Show that $(-1)^2 = 1$ in R.

2. Prove that if u is a unit in R then so is $-u$.

3. Let R be a ring with identity and let S be a subring of R containing the identity. Prove that if u is a unit in S then u is a unit in R. Show by example that the converse is false.

4. Prove that the intersection of any nonempty collection of subrings of a ring is also a subring.

5. Decide which of the following (a) – (f) are subrings of $\mathbb{Q}$:
- **(a)** the set of all rational numbers with odd denominators (when written in lowest terms)
- **(b)** the set of all rational numbers with even denominators (when written in lowest terms)
- **(c)** the set of nonnegative rational numbers
- **(d)** the set of squares of rational numbers
- **(e)** the set of all rational numbers with odd numerators (when written in lowest terms)

(f) the set of all rational numbers with even numerators (when written in lowest terms).

6. Decide which of the following are subrings of the ring of all functions from the closed interval [0,1] to $\mathbb{R}$:
   (a) the set of all functions $f(x)$ such that $f(q) = 0$ for all $q \in \mathbb{Q} \cap [0, 1]$
   (b) the set of all polynomial functions
   (c) the set of all functions which have only a finite number of zeros, together with the zero function
   (d) the set of all functions which have an infinite number of zeros
   (e) the set of all functions f such that $\lim_{x \to 1^-} f(x) = 0$
   (f) the set of all rational linear combinations of the functions $\sin nx$ and $\cos mx$, where $m, n \in \{0, 1, 2, \ldots\}$.

7. The *center* of a ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e., is the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

8. Describe the center of the real Hamilton Quaternions $\mathbb{H}$. Prove that $\{a + bi \mid a, b \in \mathbb{R}\}$ is a subring of $\mathbb{H}$ which is a field but is not contained in the center of $\mathbb{H}$.

9. For a fixed element $a \in R$ define $C(a) = \{r \in R \mid ra = ar\}$. Prove that $C(a)$ is a subring of R containing a. Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.

10. Prove that if D is a division ring then $C(a)$ is a division ring for all $a \in D$ (cf. the preceding exercise).

11. Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

12. Prove that any subring of a field which contains the identity is an integral domain.

13. An element x in R is called *nilpotent* if $x^m = 0$ for some $m \in \mathbb{Z}^+$.
   (a) Show that if $n = a^k b$ for some integers a and b then $\overline{ab}$ is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.
   (b) If $a \in \mathbb{Z}$ is an integer, show that the element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.
   (c) Let R be the ring of functions from a nonempty set X to a field F. Prove that R contains no nonzero nilpotent elements.

14. Let x be a nilpotent element of the commutative ring R (cf. the preceding exercise).
   (a) Prove that x is either zero or a zero divisor.
   (b) Prove that rx is nilpotent for all $r \in R$.
   (c) Prove that $1 + x$ is a unit in R.
   (d) Deduce that the sum of a nilpotent element and a unit is a unit.

15. A ring R is called a *Boolean ring* if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

16. Prove that the only Boolean ring that is an integral domain is $\mathbb{Z}/2\mathbb{Z}$.

17. Let R and S be rings. Prove that the direct product $R \times S$ is a ring under componentwise addition and multiplication. Prove that $R \times S$ is commutative if and only if both R and S are commutative. Prove that $R \times S$ has an identity if and only if both R and S have identities.

18. Prove that $\{(r, r) \mid r \in R\}$ is a subring of $R \times R$.

19. Let I be any nonempty index set and let R_i be a ring for each $i \in I$. Prove that the direct

product $\prod_{i \in I} R_i$ is a ring under componentwise addition and multiplication.

20. Let R be the collection of sequences $(a_1, a_2, a_3, \ldots)$ of integers $a_1, a_2, a_3, \ldots$ where all but finitely many of the a_i are 0 (called the *direct sum* of infinitely many copies of $\mathbb{Z}$). Prove that R is a ring under componentwise addition and multiplication which does not have an identity.

21. Let X be any nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X (the *power set* of X). Define addition and multiplication on $\mathcal{P}(X)$ by

$$A + B = (A - B) \cup (B - A) \qquad \text{and} \qquad A \times B = A \cap B$$

i.e., addition is symmetric difference and multiplication is intersection.

(a) Prove that $\mathcal{P}(X)$ is a ring under these operations ($\mathcal{P}(X)$ and its subrings are often referred to as *rings of sets*).

(b) Prove that this ring is commutative, has an identity and is a Boolean ring.

22. Give an example of an infinite Boolean ring.

23. Let D be a squarefree integer, and let $\mathcal{O}$ be the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{D})$. For any positive integer f prove that the set $\mathcal{O}_f = \mathbb{Z}[f\omega] = \{a + bf\omega \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathcal{O}$ containing the identity. Prove that $[\mathcal{O} : \mathcal{O}_f] = f$ (index as additive abelian groups). Prove conversely that a subring of $\mathcal{O}$ containing the identity and having finite index f in $\mathcal{O}$ (as additive abelian group) is equal to $\mathcal{O}_f$. (The ring $\mathcal{O}_f$ is called the *order of conductor* f in the field $\mathbb{Q}(\sqrt{D})$. The ring of integers $\mathcal{O}$ is called the *maximal order* in $\mathbb{Q}(\sqrt{D})$.)

24. Show for $D = 3, 5, 6$, and 7 that the group of units $\mathcal{O}^\times$ of the quadratic integer ring $\mathcal{O}$ is infinite by exhibiting an explicit unit of infinite (multiplicative) order in each ring.

25. Let I be the ring of integral Hamilton Quaternions and define

$$N : I \to \mathbb{Z} \qquad \text{by} \qquad N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$$

(the map N is called a *norm*).

(a) Prove that $N(\alpha) = \alpha\overline{\alpha}$ for all $\alpha \in I$, where if $\alpha = a + bi + cj + dk$ then $\overline{\alpha} = a - bi - cj - dk$.

(b) Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in I$.

(c) Prove that an element of I is a unit if and only if it has norm $+1$. Show that $I^\times$ is isomorphic to the quaternion group of order 8. [The inverse in the ring of rational quaternions of a nonzero element α is $\dfrac{\overline{\alpha}}{N(\alpha)}$.]

26. Let K be a field. A *discrete valuation* on K is a function $v : K^\times \to \mathbb{Z}$ satisfying

(i) $v(ab) = v(a) + v(b)$ (i.e., v is a homomorphism from the multiplicative group of nonzero elements of K to $\mathbb{Z}$),

(ii) v is surjective, and

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

The set $R = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$ is called the *valuation ring* of v.

(a) Prove that R is a subring of K which contains the identity. (In general, a ring R is called a *discrete valuation ring* if there is some field K and some discrete valuation v on K such that R is the valuation ring of v.)

(b) Prove that for each nonzero element $x \in K$ either x or x^{-1} is in R.

(c) Prove that an element x is a unit of R if and only if $v(x) = 0$.

27. A specific example of a discrete valuation ring (cf. the preceding exercise) is obtained

when p is a prime, $K = \mathbb{Q}$ and

$$v_p : \mathbb{Q}^\times \to \mathbb{Z} \qquad \text{by} \qquad v_p(\frac{a}{b}) = \alpha \quad \text{where } \frac{a}{b} = p^\alpha \frac{c}{d}, \quad p \nmid c \text{ and } p \nmid d.$$

Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p. Describe the units of this valuation ring.

28. Let R be a ring with $1 \neq 0$. A nonzero element a is called a *left zero divisor* in R if there is a nonzero element $x \in R$ such that $ax = 0$. Symmetrically, $b \neq 0$ is a *right zero divisor* if there is a nonzero $y \in R$ such that $yb = 0$ (so a zero divisor is an element which is either a left or a right zero divisor). An element $u \in R$ has a *left inverse* in R if there is some $s \in R$ such that $su = 1$. Symmetrically, v has a *right inverse* if $vt = 1$ for some $t \in R$.

(a) Prove that u is a unit if and only if it has both a right and a left inverse (i.e., u must have a two-sided inverse).

(b) Prove that if u has a right inverse then u is not a right zero divisor.

(c) Prove that if u has more than one right inverse then u is a left zero divisor.

(d) Prove that if R is a finite ring then every element that has a right inverse is a unit (i.e., has a two-sided inverse).

29. Let A be any commutative ring with identity $1 \neq 0$. Let R be the set of all group homomorphisms of the additive group A to itself with addition defined as pointwise addition of functions and multiplication defined as function composition. Prove that these operations make R into a ring with identity. Prove that the units of R are the group automorphisms of A (cf. Exercise 20, Section 1.6).

30. Let $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$ be the direct product of copies of $\mathbb{Z}$ indexed by the positive integers (so A is a ring under componentwise addition and multiplication) and let R be the ring of all group homomorphisms from A to itself as described in the preceding exercise. Let φ be the element of R defined by $\varphi(a_1, a_2, a_3, \dots) = (a_2, a_3, \dots)$. Let ψ be the element of R defined by $\psi(a_1, a_2, a_3, \dots) = (0, a_1, a_2, a_3, \dots)$.

(a) Prove that $\varphi\psi$ is the identity of R but $\psi\varphi$ is not the identity of R (i.e., ψ is a *right inverse* for φ but not a left inverse).

(b) Exhibit infinitely many right inverses for φ.

(c) Find a nonzero element π in R such that $\varphi\pi = 0$ but $\pi\varphi \neq 0$.

(d) Prove that there is no nonzero element $\lambda \in R$ such that $\lambda\varphi = 0$ (i.e., φ is a left zero divisor but not a right zero divisor).

7.2 EXAMPLES: POLYNOMIAL RINGS, MATRIX RINGS, AND GROUP RINGS

We introduce here three important types of rings: polynomial rings, matrix rings, and group rings. We shall see in the course of the text that these three classes of rings are often related. For example, we shall see in Part VI that the group ring of a group G over the complex numbers $\mathbb{C}$ is a direct product of matrix rings over $\mathbb{C}$.

These rings also have many important applications, in addition to being interesting in their own right. In Part III we shall use polynomial rings to prove some classification theorems for matrices which, in particular, determine when a matrix is similar to a diagonal matrix. In Part VI we shall use group rings to study group actions and to prove some additional important classification theorems.

Polynomial Rings

Fix a commutative ring R with identity. We define the ring of polynomials in a form which may already be familiar, at least for polynomials with real coefficients. A definition in terms of Cartesian products is given in Appendix I. Let x be an indeterminate. The formal sum

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $n \geq 0$ and each $a_i \in R$ is called a *polynomial* in x with coefficients a_i in R. If $a_n \neq 0$, then the polynomial is said to be of *degree* n, $a_n x^n$ is called the *leading term*, and a_n is called the *leading coefficient* (where the leading coefficient of the zero polynomial is taken to be 0). The polynomial is *monic* if $a_n = 1$. The set of all such polynomials is called the ring of *polynomials in the variable* x *with coefficients in* R and will be denoted $R[x]$.

The operations of addition and multiplication which make $R[x]$ into a ring are the same operations familiar from elementary algebra: addition is "componentwise"

$$\begin{aligned}(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)\\ = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)\end{aligned}$$

(here a_n or b_n may be zero in order for addition of polynomials of different degrees to be defined). Multiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ for polynomials with only one nonzero term and then extending to all polynomials by the distributive laws (usually referred to as "expanding out and collecting like terms"):

$$\begin{aligned}&(a_0 + a_1 x + a_2 x^2 + \ldots) \times (b_0 + b_1 x + b_2 x^2 + \ldots)\\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots\end{aligned}$$

(in general, the coefficient of x^k in the product will be $\sum_{i=0}^{k} a_i b_{k-i}$). These operations make sense since R is a ring so the sums and products of the coefficients are defined. An easy verification proves that $R[x]$ is indeed a ring with these definitions of addition and multiplication.

The ring R appears in $R[x]$ as the *constant polynomials*. Note that by definition of the multiplication, $R[x]$ is a *commutative ring with identity* (the identity 1 from R).

The coefficient ring R above was assumed to be a commutative ring since that is the situation we shall be primarily interested in, but note that the definition of the addition and multiplication in $R[x]$ above would be valid even if R were not commutative or did not have an identity. If the coefficient ring R is the integers $\mathbb{Z}$ (respectively, the rationals $\mathbb{Q}$) the polynomial ring $\mathbb{Z}[x]$ (respectively, $\mathbb{Q}[x]$) is the ring of polynomials with integer (rational) coefficients familiar from elementary algebra.

Another example is the polynomial ring $\mathbb{Z}/3\mathbb{Z}[x]$ of polynomials in x with coefficients in $\mathbb{Z}/3\mathbb{Z}$. This ring consists of nonnegative powers of x with coefficients 0, 1, and 2 with calculations on the coefficients performed modulo 3. For example, if

$$p(x) = x^2 + 2x + 1 \qquad \text{and} \qquad q(x) = x^3 + x + 2$$

then

$$p(x) + q(x) = x^3 + x^2$$

and

$$p(x)q(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2.$$

The ring in which the coefficients are taken makes a substantial difference in the behavior of polynomials. For example, the polynomial $x^2 + 1$ is not a perfect square in the polynomial ring $\mathbb{Z}[x]$, but *is* a perfect square in the polynomial ring $\mathbb{Z}/2\mathbb{Z}[x]$, since $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ in this ring.

Proposition 4. Let R be an integral domain and let $p(x)$, $q(x)$ be nonzero elements of $R[x]$. Then

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$,
(2) the units of $R[x]$ are just the units of R,
(3) $R[x]$ is an integral domain.

Proof: If R has no zero divisors then neither does $R[x]$; if $p(x)$ and $q(x)$ are polynomials with leading terms $a_n x^n$ and $b_m x^m$, respectively, then the leading term of $p(x)q(x)$ is $a_n b_m x^{n+m}$, and $a_n b_m \neq 0$. This proves (3) and also verifies (1). If $p(x)$ is a unit, say $p(x)q(x) = 1$ in $R[x]$, then degree $p(x)$ + degree $q(x) = 0$, so both $p(x)$ and $q(x)$ are elements of R, hence are units in R since their product is 1. This proves (2).

If the ring R has zero divisors then so does $R[x]$, because $R \subset R[x]$. Also, if $f(x)$ is a zero divisor in $R[x]$ (i.e., $f(x)g(x) = 0$ for some nonzero $g(x) \in R[x]$) then in fact $cf(x) = 0$ for some nonzero $c \in R$ (cf. Exercise 2).

If S is a subring of R then $S[x]$ is a subring of $R[x]$. For instance, $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$. Some other examples of subrings of $R[x]$ are the set of all polynomials in x^2 (i.e., in which only even powers of x appear) and the set of all polynomials with zero constant term (the latter subring does not have an identity).

Polynomial rings, particularly those over fields, will be studied extensively in Chapter 9.

Matrix Rings

Fix an arbitrary ring R and let n be a positive integer. Let $M_n(R)$ be the set of all $n \times n$ *matrices with entries from* R. The element (a_{ij}) of $M_n(R)$ is an $n \times n$ square array of elements of R whose entry in row i and column j is $a_{ij} \in R$. The set of matrices becomes a ring under the usual rules by which matrices of real numbers are added and multiplied. Addition is componentwise: the i, j entry of the matrix $(a_{ij}) + (b_{ij})$ is $a_{ij} + b_{ij}$. The i, j entry of the matrix product $(a_{ij}) \times (b_{ij})$ is $\sum_{k=1}^{n} a_{ik} b_{kj}$ (note that these matrices need to be square in order that multiplication of any two elements be defined). It is a straightforward calculation to check that these operations make $M_n(R)$ into a ring. When R is a field we shall prove that $M_n(R)$ is a ring by less computational means in Part III.

Note that if R is any nontrivial ring (even a commutative one) and $n \geq 2$ then $M_n(R)$ is *not commutative*: if $ab \neq 0$ in R let A be the matrix with a in position 1,1 and zeros elsewhere and let B be the matrix with b in position 1,2 and zeros elsewhere; then ab is the (nonzero) entry in position 1,2 of AB whereas BA is the zero matrix.

These two matrices also show that $M_n(R)$ has zero divisors for all nonzero rings R whenever $n \geq 2$.

An element (a_{ij}) of $M_n(R)$ is called a *scalar matrix* if for some $a \in R$, $a_{ii} = a$ for all $i \in \{1, \ldots, n\}$ and $a_{ij} = 0$ for all $i \neq j$ (i.e., all diagonal entries equal a and all off-diagonal entries are 0). The set of scalar matrices is a subring of $M_n(R)$. This subring is a copy of R (i.e., is "isomorphic" to R): if the matrix A has the element a along the main diagonal and the matrix B has the element b along the main diagonal then the matrix $A + B$ has $a + b$ along the diagonal and AB has ab along the diagonal (and all other entries 0). If R is commutative, the scalar matrices commute with all elements of $M_n(R)$. If R has a 1, then the scalar matrix with 1's down the diagonal (the $n \times n$ *identity matrix*) is the 1 of $M_n(R)$. In this case the units in $M_n(R)$ are the invertible $n \times n$ matrices and the group of units is denoted $GL_n(R)$, the *general linear group* of degree n over R.

If S is a subring of R then $M_n(S)$ is a subring of $M_n(R)$. For instance $M_n(\mathbb{Z})$ is a subring of $M_n(\mathbb{Q})$ and $M_n(2\mathbb{Z})$ is a subring of both of these. Another example of a subring of $M_n(R)$ is the set of *upper triangular* matrices: $\{(a_{ij}) \mid a_{pq} = 0 \text{ whenever } p > q\}$ (the set of matrices all of whose entries below the main diagonal are zero) — one easily checks that the sum and product of upper triangular matrices is upper triangular.

Group Rings

Fix a commutative ring R with identity $1 \neq 0$ and let $G = \{g_1, g_2, \ldots, g_n\}$ be any finite group with group operation written multiplicatively. Define the *group ring*, RG, of G with coefficients in R to be the set of all formal sums

$$a_1g_1 + a_2g_2 + \cdots + a_ng_n \qquad a_i \in R, \quad 1 \leq i \leq n.$$

If g_1 is the identity of G we shall write a_1g_1 simply as a_1. Similarly, we shall write the element $1g$ for $g \in G$ simply as g.

Addition is defined "componentwise"

$$\begin{aligned}(a_1g_1 + a_2g_2 + \cdots + a_ng_n) + (b_1g_1 + b_2g_2 + \cdots + b_ng_n)\\ = (a_1 + b_1)g_1 + (a_2 + b_2)g_2 + \cdots + (a_n + b_n)g_n.\end{aligned}$$

Multiplication is performed by first defining $(ag_i)(bg_j) = (ab)g_k$, where the product ab is taken in R and $g_ig_j = g_k$ is the product in the group G. This product is then extended to all formal sums by the distributive laws so that the coefficient of g_k in the product $(a_1g_1 + \cdots + a_ng_n) \times (b_1g_1 + \cdots + b_ng_n)$ is $\sum_{g_ig_j = g_k} a_ib_j$. It is straightforward to check that these operations make RG into a ring (again, commutativity of R is not needed). The associativity of multiplication follows from the associativity of the group operation in G. The ring RG is commutative if and only if G is a commutative group.

Example

Let $G = D_8$ be the dihedral group of order 8 with the usual generators r, s ($r^4 = s^2 = 1$ and $rs = sr^{-1}$) and let $R = \mathbb{Z}$. The elements $\alpha = r + r^2 - 2s$ and $\beta = -3r^2 + rs$ are

typical members of $\mathbb{Z}D_8$. Their sum and product are then

$$\begin{aligned}\alpha + \beta &= r - 2r^2 - 2s + rs \\ \alpha\beta &= (r + r^2 - 2s)(-3r^2 + rs) \\ &= r(-3r^2 + rs) + r^2(-3r^2 + rs) - 2s(-3r^2 + rs) \\ &= -3r^3 + r^2s - 3 + r^3s + 6r^2s - 2r^3 \\ &= -3 - 5r^3 + 7r^2s + r^3s.\end{aligned}$$

The ring R appears in RG as the "constant" formal sums i.e., the R-multiples of the identity of G (note that the definition of the addition and multiplication in RG restricted to these elements is just the addition and multiplication in R). These elements of R commute with all elements of RG. The identity of R is the identity of RG.

The group G also appears in RG (the element g_i appears as $1g_i$ — for example, $r, s \in D_8$ are also elements of the group ring $\mathbb{Z}D_8$ above) — multiplication in the ring RG restricted to G is just the group operation. In particular, each element of G has a multiplicative inverse in the ring RG (namely, its inverse in G). This says that G is a *subgroup of the group of units of* RG.

If $|G| > 1$ then RG always has zero divisors. For example, let g be any element of G of order $m > 1$. Then

$$(1 - g)(1 + g + \cdots + g^{m-1}) = 1 - g^m = 1 - 1 = 0$$

so $1 - g$ is a zero divisor (note that by definition of RG neither of the formal sums in the above product is zero).

If S is a subring of R then SG is a subring of RG. For instance, $\mathbb{Z}G$ (called the *integral group ring* of G) is a subring of $\mathbb{Q}G$ (the *rational group ring* of G). Furthermore, if H is a subgroup of G then RH is a subring of RG. The set of all elements of RG whose coefficients sum to zero is a subring (without identity). If $|G| > 1$, the set of elements with zero "constant term" (i.e., the coefficient of the identity of G is zero) is *not* a subring (it is not closed under multiplication).

Note that the group ring $\mathbb{R}Q_8$ is *not* the same ring as the Hamilton Quaternions $\mathbb{H}$ even though the latter contains a copy of the quaternion group Q_8 (under multiplication). One difference is that the unique element of order 2 in Q_8 (usually denoted by -1) is not the additive inverse of 1 in $\mathbb{R}Q_8$. In other words, if we temporarily denote the identity of the group Q_8 by g_1 and the unique element of order 2 by g_2, then $g_1 + g_2$ is not zero in $\mathbb{R}Q_8$, whereas $1 + (-1)$ is zero in $\mathbb{H}$. Furthermore, as noted above, the group ring $\mathbb{R}Q_8$ contains zero divisors hence is not a division ring.

Group rings over fields will be studied extensively in Chapter 18.

EXERCISES

Let R be a commutative ring with 1.

1. Let $p(x) = 2x^3 - 3x^2 + 4x - 5$ and let $q(x) = 7x^3 + 33x - 4$. In each of parts (a), (b) and (c) compute $p(x) + q(x)$ and $p(x)q(x)$ under the assumption that the coefficients of the two given polynomials are taken from the specified ring (where the integer coefficients are taken mod n in parts (b) and (c)):
(a) $R = \mathbb{Z}$, **(b)** $R = \mathbb{Z}/2\mathbb{Z}$, **(c)** $R = \mathbb{Z}/3\mathbb{Z}$.

2. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$. Prove that $p(x)$ is a zero divisor in $R[x]$ if and only if there is a nonzero $b \in R$ such that $bp(x) = 0$. [Let $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ be a nonzero polynomial of minimal degree such that $g(x)p(x) = 0$. Show that $b_m a_n = 0$ and so $a_n g(x)$ is a polynomial of degree less than m that also gives 0 when multiplied by $p(x)$. Conclude that $a_n g(x) = 0$. Apply a similar argument to show by induction on i that $a_{n-i}g(x) = 0$ for $i = 0, 1, \ldots, n$, and show that this implies $b_m p(x) = 0$.]

3. Define the set $R[[x]]$ of *formal power series* in the indeterminate x with coefficients from R to be all formal infinite sums

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots.$$

Define addition and multiplication of power series in the same way as for power series with real or complex coefficients i.e., extend polynomial addition and multiplication to power series as though they were "polynomials of infinite degree":

$$\sum_{n=0}^{\infty} a_n x^n \quad + \quad \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

$$\sum_{n=0}^{\infty} a_n x^n \quad \times \quad \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) x^n.$$

(The term "formal" is used here to indicate that convergence is not considered, so that formal power series need not represent functions on R.)

(a) Prove that $R[[x]]$ is a commutative ring with 1.

(b) Show that $1 - x$ is a unit in $R[[x]]$ with inverse $1 + x + x^2 + \cdots$.

(c) Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

4. Prove that if R is an integral domain then the ring of formal power series $R[[x]]$ is also an integral domain.

5. Let F be a field and define the ring $F((x))$ of *formal Laurent series* with coefficients from F by

$$F((x)) = \{ \sum_{n \geq N}^{\infty} a_n x^n \mid a_n \in F \text{ and } N \in \mathbb{Z} \}.$$

(Every element of $F((x))$ is a power series in x plus a polynomial in $1/x$, i.e., each element of $F((x))$ has only a finite number of terms with negative powers of x.)

(a) Prove that $F((x))$ is a field.

(b) Define the map

$$v : F((x))^{\times} \to \mathbb{Z} \qquad \text{by} \qquad v\Big(\sum_{n \geq N}^{\infty} a_n x^n \Big) = N$$

where a_N is the first nonzero coefficient of the series (i.e., N is the "order of zero or pole of the series at 0"). Prove that v is a discrete valuation on $F((x))$ whose discrete valuation ring is $F[[x]]$, the ring of formal power series (cf. Exercise 26, Section 1).

6. Let S be a ring with identity $1 \neq 0$. Let $n \in \mathbb{Z}^+$ and let A be an $n \times n$ matrix with entries from S whose i, j entry is a_{ij}. Let E_{ij} be the element of $M_n(S)$ whose i, j entry is 1 and whose other entries are all 0.

(a) Prove that $E_{ij}A$ is the matrix whose i^{th} row equals the j^{th} row of A and all other rows are zero.

(b) Prove that AE_{ij} is the matrix whose j^{th} column equals the i^{th} column of A and all other columns are zero.

(c) Deduce that $E_{pq}AE_{rs}$ is the matrix whose p, s entry is a_{qr} and all other entries are zero.

7. Prove that the center of the ring $M_n(R)$ is the set of scalar matrices (cf. Exercise 7, Section 1). [Use the preceding exercise.]

8. Let S be any ring and let $n \geq 2$ be an integer. Prove that if A is any strictly upper triangular matrix in $M_n(S)$ then $A^n = 0$ (a strictly upper triangular matrix is one whose entries on and below the main diagonal are all zero).

9. Let $\alpha = r + r^2 - 2s$ and $\beta = -3r^2 + rs$ be the two elements of the integral group ring $\mathbb{Z}D_8$ described in this section. Compute the following elements of $\mathbb{Z}D_8$:
(a) $\beta\alpha$, **(b)** α^2, **(c)** $\alpha\beta - \beta\alpha$, **(d)** $\beta\alpha\beta$.

10. Consider the following elements of the integral group ring $\mathbb{Z}S_3$:

$$\alpha = 3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3) \qquad \text{and} \qquad \beta = 6(1) + 2(2\ 3) - 7(1\ 3\ 2)$$

(where (1) is the identity of S_3). Compute the following elements:
(a) $\alpha + \beta$, **(b)** $2\alpha - 3\beta$, **(c)** $\alpha\beta$, **(d)** $\beta\alpha$, **(e)** α^2.

11. Repeat the preceding exercise under the assumption that the coefficients of α and β are in $\mathbb{Z}/3\mathbb{Z}$ (i.e., $\alpha, \beta \in \mathbb{Z}/3\mathbb{Z}S_3$).

12. Let $G = \{g_1, \ldots, g_n\}$ be a finite group. Prove that the element $N = g_1 + g_2 + \ldots + g_n$ is in the center of the group ring RG (cf. Exercise 7, Section 1).

13. Let $\mathcal{K} = \{k_1, \ldots, k_m\}$ be a conjugacy class in the finite group G.
(a) Prove that the element $K = k_1 + \ldots + k_m$ is in the center of the group ring RG (cf. Exercise 7, Section 1). [Check that $g^{-1}Kg = K$ for all $g \in G$.]
(b) Let $\mathcal{K}_1, \ldots, \mathcal{K}_r$ be the conjugacy classes of G and for each $\mathcal{K}_i$ let K_i be the element of RG that is the sum of the members of $\mathcal{K}_i$. Prove that an element $\alpha \in RG$ is in the center of RG if and only if $\alpha = a_1K_1 + a_2K_2 + \cdots + a_rK_r$ for some $a_1, a_2, \ldots, a_r \in R$.

7.3 RING HOMOMORPHISMS AND QUOTIENT RINGS

A ring homomorphism is a map from one ring to another that respects the additive and multiplicative structures:

Definition. Let R and S be rings.

(1) A *ring homomorphism* is a map $\varphi : R \to S$ satisfying
  (i) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$ (so φ is a group homomorphism on the additive groups) and
  (ii) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

(2) The *kernel* of the ring homomorphism φ, denoted $\ker\varphi$, is the set of elements of R that map to 0 in S (i.e., the kernel of φ viewed as a homomorphism of additive groups).

(3) A bijective ring homomorphism is called an *isomorphism.*

If the context is clear we shall simply use the term "homomorphism" instead of "ring homomorphism." Similarly, if A and B are rings, $A \cong B$ will always mean an isomorphism of rings unless otherwise stated.

Examples

(1) The map $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by sending an even integer to 0 and an odd integer to 1 is a ring homomorphism. The map is additive since the sum of two even or odd integers is even and the sum of an even integer and an odd integer is odd. The map is multiplicative since the product of two odd integers is odd and the product of an even integer with any integer is even. The kernel of φ (the fiber of φ above $0 \in \mathbb{Z}/2\mathbb{Z}$) is the set of even integers. The fiber of φ above $1 \in \mathbb{Z}/2\mathbb{Z}$ is the set of odd integers.

(2) For $n \in \mathbb{Z}$ the maps $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi_n(x) = nx$ are *not* in general ring homomorphisms because $\varphi_n(xy) = nxy$ whereas $\varphi_n(x)\varphi_n(y) = nxny = n^2xy$. Hence φ_n is a ring homomorphism only when $n^2 = n$, i.e., $n = 0, 1$. Note however that φ_n is always a *group homomorphism* on the additive groups. Thus care should be exercised when dealing with rings to be sure to check that *both* ring operations are preserved. Note that φ_0 is the zero homomorphism and φ_1 is the identity homomorphism.

(3) Let $\varphi : \mathbb{Q}[x] \to \mathbb{Q}$ be the map from the ring of polynomials in x with rational coefficients to the rationals defined by $\varphi(p(x)) = p(0)$ (i.e., mapping the polynomial to its constant term). Then φ is a ring homomorphism since the constant term of the sum of two polynomials is the sum of their constant terms and the constant term of the product of two polynomials is the product of their constant terms. The fiber above $a \in \mathbb{Q}$ consists of the set of polynomials with a as constant term. In particular, the kernel of φ consists of the polynomials with constant term 0.

Proposition 5. Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

(1) The image of φ is a subring of S.

(2) The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker\varphi$ then $r\alpha$ and $\alpha r \in \ker\varphi$ for every $r \in R$, i.e., $\ker\varphi$ is closed under multiplication by elements from R.

Proof: (1) If $s_1, s_2 \in \operatorname{im}\varphi$ then $s_1 = \varphi(r_1)$ and $s_2 = \varphi(r_2)$ for some $r_1, r_2 \in R$. Then $\varphi(r_1 - r_2) = s_1 - s_2$ and $\varphi(r_1r_2) = s_1s_2$. This shows $s_1 - s_2, s_1s_2 \in \operatorname{im}\varphi$, so the image of φ is closed under subtraction and under multiplication, hence is a subring of S.

(2) If $\alpha, \beta \in \ker\varphi$ then $\varphi(\alpha) = \varphi(\beta) = 0$. Hence $\varphi(\alpha - \beta) = 0$ and $\varphi(\alpha\beta) = 0$, so $\ker\varphi$ is closed under subtraction and under multiplication, so is a subring of R. Similarly, for any $r \in R$ we have $\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = \varphi(r)\ 0 = 0$, and also $\varphi(\alpha r) = \varphi(\alpha)\varphi(r) = 0\ \varphi(r) = 0$, so $r\alpha, \alpha r \in \ker\varphi$.

In the case of a homomorphism φ of groups we saw that the fibers of the homomorphism have the structure of a group naturally isomorphic to the image of φ, which led to the notion of a quotient group by a normal subgroup. An analogous result is true for a homomorphism of rings.

Let $\varphi : R \to S$ be a ring homomorphism with kernel I. Since R and S are in particular additive abelian groups, φ is in particular a homomorphism of abelian groups

and the fibers of φ are the additive cosets $r + I$ of the kernel I (more precisely, if r is any element of R mapping to $a \in S$, $\varphi(r) = a$, then the fiber of φ over a is the coset $r + I$ of the kernel I). These fibers have the structure of a ring naturally isomorphic to the image of φ: if X is the fiber over $a \in S$ and Y is the fiber over $b \in S$, then $X + Y$ is the fiber over $a + b$ and XY is the fiber over ab. In terms of cosets of the kernel I this addition and multiplication is

$$(r + I) + (s + I) = (r + s) + I \tag{7.1}$$

$$(r + I) \times (s + I) = (rs) + I. \tag{7.2}$$

As in the case for groups, the verification that these operations define a ring structure on the collection of cosets of the kernel I ultimately rests on the corresponding ring properties of S. This ring of cosets is called the *quotient ring* of R by $I = \ker \varphi$ and is denoted R/I. Note that the additive structure of the ring R/I is just the additive quotient group of the additive abelian group R by the (necessarily normal) subgroup I. When I is the kernel of some homomorphism φ this additive abelian quotient group also has a multiplicative structure, defined by (7.2), which makes R/I into a ring.

As in the case for groups, we can also consider whether (1) and (2) can be used to define a ring structure on the collection of cosets of an *arbitrary* subgroup I of R. Note that since R is an abelian additive group, the subgroup I is necessarily normal so that the quotient R/I of cosets of I is automatically an additive abelian group. The question then is whether this quotient group also has a *multiplicative* structure induced from the multiplication in R, defined by (2). The answer is no in general (just as the answer is no in trying to form the quotient by an arbitrary subgroup of a group), which leads to the notion of an *ideal* in R (the analogue for rings of a normal subgroup of a group). We shall then see that the ideals of R are exactly the kernels of the ring homomorphisms of R (the analogue for rings of the characterization of normal subgroups as the kernels of group homomorphisms).

Let I be an arbitrary subgroup of the additive group R. We consider when the multiplication of cosets in (2) is well defined and makes the additive abelian group R/I into a ring. The statement that the multiplication in (2) is well defined is the statement that the multiplication is independent of the particular representatives r and s chosen, i.e., that we obtain the same coset on the right if instead we use the representatives $r + \alpha$ and $s + \beta$ for any $\alpha, \beta \in I$. In other words, we must have

$$(r + \alpha)(s + \beta) + I = rs + I \tag{$*$}$$

for all $r, s \in R$ and all $\alpha, \beta \in I$.

Letting $r = s = 0$, we see that I must be closed under multiplication, i.e., I must be a *subring* of R.

Next, by letting $s = 0$ and letting r be arbitrary, we see that we must have $r\beta \in I$ for every $r \in R$ and every $\beta \in I$, i.e., that I must be closed under multiplication on the left by elements from R. Letting $r = 0$ and letting s be arbitrary, we see similarly that I must be closed under multiplication on the right by elements from R.

Conversely, if I is closed under multiplication on the left and on the right by elements from R then the relation $(*)$ is satisfied for all $\alpha, \beta \in I$. Hence this is a necessary and sufficient condition for the multiplication in (2) to be well defined.

Finally, if the multiplication of cosets defined by (2) is well defined, then this multiplication makes the additive quotient group R/I into a ring. Each ring axiom in the quotient follows directly from the corresponding axiom in R. For example, one of the distributive laws is verified as follows:

$$\begin{aligned}(r+I)[(s+I)+(t+I)] &= (r+I)[(s+t)+I] \\ &= r(s+t)+I = (rs+rt)+I \\ &= (rs+I)+(rt+I) \\ &= [(r+I)(s+I)]+[(r+I)(t+I)].\end{aligned}$$

This shows that the quotient R/I of the ring R by a subgroup I has a natural ring structure if and only if I is also closed under multiplication on the left and on the right by elements from R (so in particular must be a subring of R since it is closed under multiplication). As mentioned, such subrings I are called the *ideals* of R:

Definition. Let R be a ring, let I be a subset of R and let $r \in R$.

(1) $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.

(2) A subset I of R is a *left ideal* of R if

(i) I is a subring of R, and

(ii) I is closed under left multiplication by elements from R, i.e., $rI \subseteq I$ for all $r \in R$.

Similarly I is a *right ideal* if (i) holds and in place of (ii) one has

(ii)′ I is closed under right multiplication by elements from R, i.e., $Ir \subseteq I$ for all $r \in R$.

(3) A subset I that is both a left ideal and a right ideal is called an *ideal* (or, for added emphasis, a *two-sided ideal*) of R.

For commutative rings the notions of left, right and two-sided ideal coincide. We emphasize that to prove a subset I of a ring R is an ideal it is necessary to prove that I is nonempty, closed under subtraction and closed under multiplication by all the elements of R (and not just by elements of I). If R has a 1 then $(-1)a = -a$ so in this case I is an ideal if it is nonempty, closed under addition and closed under multiplication by all the elements of R.

Note also that the last part of Proposition 5 proves that the kernel of any ring homomorphism is an ideal.

We summarize the preceding discussion in the following proposition.

Proposition 6. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I) = (r+s)+I \qquad \text{and} \qquad (r+I)\times(s+I) = (rs)+I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition. When I is an ideal of R the ring R/I with the operations in the previous proposition is called the *quotient ring* of R by I.

Theorem 7.

(1) *(The First Isomorphism Theorem for Rings)* If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.

(2) If I is any ideal of R, then the map

$$R \to R/I \qquad \text{defined by} \qquad r \mapsto r + I$$

is a surjective ring homomorphism with kernel I (this homomorphism is called the *natural projection* of R onto R/I). Thus every ideal is the kernel of a ring homomorphism and vice versa.

Proof: This is just a matter of collecting previous calculations. If I is the kernel of φ, then the cosets (under addition) of I are precisely the fibers of φ. In particular, the cosets $r+I$, $s+I$ and $rs+I$ are the fibers of φ over $\varphi(r)$, $\varphi(s)$ and $\varphi(rs)$, respectively. Since φ is a ring homomorphism $\varphi(r)\varphi(s) = \varphi(rs)$, hence $(r+I)(s+I) = rs+I$. Multiplication of cosets is well defined and so I is an ideal and R/I is a ring. The correspondence $r + I \mapsto \varphi(r)$ is a bijection between the rings R/I and $\varphi(R)$ which respects addition and multiplication, hence is a ring isomorphism.

If I is any ideal, then R/I is a ring (in particular is an abelian group) and the map $\pi : r \mapsto r + I$ is a group homomorphism with kernel I. It remains to check that π is a ring homomorphism. This is immediate from the definition of multiplication in R/I:

$$\pi : rs \mapsto rs + I = (r + I)(s + I) = \pi(r)\pi(s).$$

As with groups we shall often use the bar notation for reduction mod I: $\bar{r} = r + I$. With this notation the addition and multiplication in the quotient ring R/I become simply $\bar{r} + \bar{s} = \overline{r+s}$ and $\bar{r}\,\bar{s} = \overline{rs}$.

Examples

Let R be a ring.

(1) The subrings R and $\{0\}$ are ideals. An ideal I is *proper* if $I \neq R$. The ideal $\{0\}$ is called the *trivial ideal* and is denoted by 0.

(2) It is immediate that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for any $n \in \mathbb{Z}$ and these are the only ideals of $\mathbb{Z}$ since in particular these are the only subgroups of $\mathbb{Z}$. The associated quotient ring is $\mathbb{Z}/n\mathbb{Z}$ (which explains the choice of notation and which we have now proved is a ring), introduced in Chapter 0. For example, if $n = 15$ then the elements of $\mathbb{Z}/15\mathbb{Z}$ are the cosets $\bar{0}, \bar{1}, \ldots, \overline{13}, \overline{14}$. To add (or multiply) in the quotient, simply choose any representatives for the two cosets, add (multiply, respectively) these representatives in the integers $\mathbb{Z}$, and take the corresponding coset containing this sum (product, respectively). For example, $\bar{7} + \overline{11} = \overline{18}$ and $\overline{18} = \bar{3}$, so $\bar{7} + \overline{11} = \bar{3}$ in $\mathbb{Z}/15\mathbb{Z}$. Similarly, $\bar{7}\,\overline{11} = \overline{77} = \bar{2}$ in $\mathbb{Z}/15\mathbb{Z}$. We could also express this by writing $7 + 11 \equiv 3 \bmod 15$, $7(11) \equiv 2 \bmod 15$.

The natural projection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is called *reduction mod n* and will be discussed further at the end of these examples.

(3) Let $R = \mathbb{Z}[x]$ be the ring of polynomials in x with integer coefficients. Let I be the collection of polynomials whose terms are of degree at least 2 (i.e., having no terms of degree 0 or degree 1) together with the zero polynomial. Then I is an ideal: the sum of two such polynomials again has terms of degree at least 2 and the product of a polynomial whose terms are of degree at least 2 with *any* polynomial again only has terms of degree at least 2. Two polynomials $p(x), q(x)$ are in the same coset of I if and only if they differ by a polynomial whose terms are of degree at least 2, i.e., if and only if $p(x)$ and $q(x)$ have the same constant and first degree terms. For example, the polynomials $3 + 5x + x^3 + x^5$ and $3 + 5x - x^4$ are in the same coset of I. It follows easily that a complete set of representatives for the quotient R/I is given by the polynomials $a + bx$ of degree at most 1.

Addition and multiplication in the quotient are again performed by representatives. For example,

$$(\overline{1 + 3x}) + (\overline{-4 + 5x}) = \overline{-3 + 8x}$$

and

$$(\overline{1 + 3x})(\overline{-4 + 5x}) = \overline{(-4 - 7x + 15x^2)} = \overline{-4 - 7x}\,.$$

Note that in this quotient ring R/I we have $\bar{x}\,\bar{x} = \overline{x^2} = \bar{0}$, for example, so that R/I has zero divisors, even though $R = \mathbb{Z}[x]$ does not.

(4) Let A be a ring, let X be any nonempty set and let R be the ring of all functions from X to A. For each fixed $c \in X$ the map

$$E_c : R \to A \quad \text{defined by} \quad E_c(f) = f(c)$$

(called *evaluation at c*) is a ring homomorphism because the operations in R are pointwise addition and multiplication of functions. The kernel of E_c is given by $\{f \in R \mid f(c) = 0\}$ (the set of functions from X to A that vanish at c). Also, E_c is surjective: given any $a \in A$ the constant function $f(x) = a$ maps to a under evaluation at c. Thus $R/\ker E_c \cong A$.

Similarly, let X be the closed interval $[0,1]$ in $\mathbb{R}$ and let R be the ring of all continuous real valued functions on $[0,1]$. For each $c \in [0, 1]$, evaluation at c is a surjective ring homomorphism (since R contains the constant functions) and so $R/\ker E_c \cong \mathbb{R}$. The kernel of E_c is the ideal of all continuous functions whose graph crosses the x-axis at c. More generally, the fiber of E_c above the real number y_0 is the set of all continuous functions that pass through the point (c, y_0).

(5) The map from the polynomial ring $R[x]$ to R defined by $p(x) \mapsto p(0)$ (evaluation at 0) is a ring homomorphism whose kernel is the set of all polynomials whose constant term is zero, i.e., $p(0) = 0$. We can compose this homomorphism with any homomorphism from R to another ring S to obtain a ring homomorphism from $R[x]$ to S. For example, let $R = \mathbb{Z}$ and consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ defined by the composition $p(x) \mapsto p(0) \mapsto p(0) \bmod 2 \in \mathbb{Z}/2\mathbb{Z}$. The kernel of this composite map is given by $\{p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\}$, i.e., the set of all polynomials with integer coefficients whose constant term is even. The other fiber of this homomorphism is the coset of polynomials whose constant term is odd, as we determined earlier. Since the homomorphism is clearly surjective, the quotient ring is $\mathbb{Z}/2\mathbb{Z}$.

(6) Fix some $n \in \mathbb{Z}$ with $n \geq 2$ and consider the noncommutative ring $M_n(R)$. If J is any ideal of R then $M_n(J)$, the $n \times n$ matrices whose entries come from J, is a two-sided ideal of $M_n(R)$. This ideal is the kernel of the surjective homomorphism $M_n(R) \to M_n(R/J)$ which reduces each entry of a matrix mod J, i.e., which maps each entry a_{ij} to $\overline{a_{ij}}$ (here bar denotes passage to R/J). For instance, when $n = 3$ and $R = \mathbb{Z}$, the 3×3 matrices whose entries are all even is the two-sided ideal $M_3(2\mathbb{Z})$

of $M_3(\mathbb{Z})$ and the quotient $M_3(\mathbb{Z})/M_3(2\mathbb{Z})$ is isomorphic to $M_3(\mathbb{Z}/2\mathbb{Z})$. If the ring R has an identity then the exercises below show that every two-sided ideal of $M_n(R)$ is of the form $M_n(J)$ for some two-sided ideal J of R.

(7) Let R be a commutative ring with 1 and let $G = \{g_1, \ldots, g_n\}$ be a finite group. The map from the group ring RG to R defined by $\sum_{i=1}^n a_i g_i \mapsto \sum_{i=1}^n a_i$ is easily seen to be a homomorphism, called the *augmentation map* . The kernel of the augmentation map, the *augmentation ideal*, is the set of elements of RG whose coefficients sum to 0. For example, $g_i - g_j$ is an element of the augmentation ideal for all i, j. Since the augmentation map is surjective, the quotient ring is isomorphic to R.

Another ideal in RG is $\{\sum_{i=1}^n a g_i \mid a \in R\}$, i.e., the formal sums whose coefficients are all equal (equivalently, all R-multiples of the element $g_1 + \cdots + g_n$).

(8) Let R be a commutative ring with identity $1 \neq 0$ and let $n \in \mathbb{Z}$ with $n \geq 2$. We exhibit some one-sided ideals in the ring $M_n(R)$. For each $j \in \{1, 2, \ldots, n\}$ let L_j be the set of all $n \times n$ matrices in $M_n(R)$ with arbitrary entries in the j^{th} column and zeros in all other columns. It is clear that L_j is closed under subtraction. It follows directly from the definition of matrix multiplication that for any matrix $T \in M_n(R)$ and any $A \in L_j$ the product TA has zero entries in the i^{th} column for all $i \neq j$. This shows L_j is a *left ideal* of $M_n(R)$. Moreover, L_j is *not* a *right* ideal (hence is not a two-sided ideal). To see this, let E_{pq} be the matrix with 1 in the p^{th} row and q^{th} column and zeros elsewhere $(p, q \in \{1, \ldots, n\})$. Then $E_{1j} \in L_j$ but $E_{1j}E_{ji} = E_{1i} \notin L_j$ if $i \neq j$, so L_j is not closed under right multiplication by arbitrary ring elements. An analogous argument shows that if R_j is the set of all $n \times n$ matrices in $M_n(R)$ with arbitrary entries in the j^{th} row and zeros in all other rows, then R_j is a *right* ideal which is not a *left* ideal. These one-sided ideals will play an important role in Part VI.

Example: (The Reduction Homomorphism)

The canonical projection map from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ obtained by factoring out by the ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is usually referred to as "reducing modulo n." The fact that this is a *ring homomorphism* has important consequences for elementary number theory. For example, suppose we are trying to solve the equation

$$x^2 + y^2 = 3z^2$$

in *integers* x, y and z (such problems are frequently referred to as *Diophantine equations* after Diophantus, who was one of the first to systematically examine the existence of *integer* solutions of equations). Suppose such integers exist. Observe first that we may assume x, y and z have no factors in common, since otherwise we could divide through this equation by the square of this common factor and obtain another set of integer solutions smaller than the initial ones. This equation simply states a relation between these elements in the *ring* $\mathbb{Z}$. As such, the same relation must also hold in any *quotient* ring as well. In particular, this relation must hold in $\mathbb{Z}/n\mathbb{Z}$ for any integer n. The choice $n = 4$ is particularly efficacious, for the following reason: the squares mod 4 are just $0^2, 1^2, 2^2, 3^2$, i.e., 0, 1 (mod 4). Reading the above equation mod 4 (that is, considering this equation in the quotient ring $\mathbb{Z}/4\mathbb{Z}$), we must have

$$\begin{Bmatrix} 0 \\ 1 \end{Bmatrix} + \begin{Bmatrix} 0 \\ 1 \end{Bmatrix} \equiv 3 \begin{Bmatrix} 0 \\ 1 \end{Bmatrix} \equiv \begin{Bmatrix} 0 \\ 3 \end{Bmatrix} \pmod 4$$

where the $\begin{Bmatrix} 0 \\ 1 \end{Bmatrix}$, for example, indicates that either a 0 or a 1 may be taken. Checking the few possibilities shows that we must take the 0 each time. This means that each

of x, y and z must be even integers (squares of the odd integers gave us 1 mod 4). But this contradicts the assumption of no common factors for these integers, and shows that this equation has *no solutions in nonzero integers.*

Note that even had solutions existed, this technique gives information about the possible residues of the solutions mod n (since we could just as well have examined the possibilities mod n as mod 4) and note that for each choice of n we have only a *finite* problem to solve because there are only finitely many residue classes mod n. Together with the Chinese Remainder Theorem (described in Section 6), we can then determine the possible solutions modulo very large integers, which greatly assists in finding them numerically (when they exist). We also observe that this technique has a number of limitations — for example, there are equations which have solutions modulo every integer, but which do not have integer solutions. An easy example (but extremely hard to verify that it does indeed have this property) is the equation

$$3x^3 + 4y^3 + 5z^3 = 0.$$

As a final example of this technique, we mention that the map from the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients to the ring $\mathbb{Z}/p\mathbb{Z}[x]$ of polynomials with coefficients in $\mathbb{Z}/p\mathbb{Z}$ for a prime p given by *reducing the coefficients modulo p* is a ring homomorphism. This example of reduction will be used in Chapter 9 in trying to determine whether polynomials can be factored.

The following theorem gives the remaining Isomorphism Theorems for rings. Each of these may be proved as follows: first use the corresponding theorem from group theory to obtain an isomorphism of *additive groups* (or correspondence of groups, in the case of the Fourth Isomorphism Theorem) and then check that this group isomorphism (or correspondence, respectively) is a multiplicative map, and so defines a *ring* isomorphism. In each case the verification is immediate from the definition of multiplication in quotient rings. For example, the map that gives the isomorphism in (2) below is defined by $\varphi : r + I \mapsto r + J$. This map is multiplicative since $(r_1 + I)(r_2 + I) = r_1r_2 + I$ by the definition of the multiplication in the quotient ring R/I, and $r_1r_2 + I \mapsto r_1r_2 + J = (r_1 + J)(r_2 + J)$ by the definition of the multiplication in the quotient ring R/J, i.e., $\varphi(r_1r_2) = \varphi(r_1)\varphi(r_2)$. The proofs for the other parts of the theorem are similar.

Theorem 8. Let R be a ring.

(1) *(The Second Isomorphism Theorem for Rings)* Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b \mid a \in A,\ b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.

(2) *(The Third Isomorphism Theorem for Rings)* Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

(3) *(The Fourth or Lattice Isomorphism Theorem for Rings)* Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

Let $R = \mathbb{Z}$ and let I be the ideal $12\mathbb{Z}$. The quotient ring $\overline{R} = R/I = \mathbb{Z}/12\mathbb{Z}$ has ideals $\overline{R}$, $2\mathbb{Z}/12\mathbb{Z}$, $3\mathbb{Z}/12\mathbb{Z}$, $4\mathbb{Z}/12\mathbb{Z}$, $6\mathbb{Z}/12\mathbb{Z}$, and $\overline{0} = 12\mathbb{Z}/12\mathbb{Z}$ corresponding to the ideals $R = \mathbb{Z}$, $2\mathbb{Z}$, $3\mathbb{Z}$, $4\mathbb{Z}$, $6\mathbb{Z}$ and $12\mathbb{Z} = I$ of R containing I, respectively.

If I and J are ideals in the ring R then the set of sums $a + b$ with $a \in I$ and $b \in J$ is not only a subring of R (as in the Second Isomorphism Theorem for Rings), but is an *ideal* in R (the set is clearly closed under sums and $r(a + b) = ra + rb \in I + J$ since $ra \in I$ and $rb \in J$). We can also define the product of two ideals:

Definition. Let I and J be ideals of R.

(1) Define the *sum* of I and J by $I + J = \{a + b \mid a \in I,\ b \in J\}$.

(2) Define the *product* of I and J, denoted by IJ, to be the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$.

(3) For any $n \geq 1$, define the n^{th} *power* of I, denoted by I^n, to be the set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in I$ for all i. Equivalently, I^n is defined inductively by defining $I^1 = I$, and $I^n = II^{n-1}$ for $n = 2, 3, \ldots$.

It is easy to see that the sum $I + J$ of the ideals I and J is the smallest ideal of R containing both I and J and that the product IJ is an ideal contained in $I \cap J$ (but may be strictly smaller, cf. the exercises). Note also that the elements of the product ideal IJ are *finite sums* of products of elements ab from I and J. The set $\{ab \mid a \in I,\ b \in J\}$ consisting just of products of elements from I and J is in general not closed under addition, hence is not in general an ideal.

Examples

(1) Let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$ in $\mathbb{Z}$. Then $I + J$ consists of all integers of the form $6x + 10y$ with $x, y \in \mathbb{Z}$. Since every such integer is divisible by 2, the ideal $I + J$ is contained in $2\mathbb{Z}$. On the other hand, $2 = 6(2) + 10(-1)$ shows that the ideal $I + J$ contains the ideal $2\mathbb{Z}$, so that $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$. In general, $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, where d is the greatest common divisor of m and n. The product IJ consists of all finite sums of elements of the form $(6x)(10y)$ with $x, y \in \mathbb{Z}$, which clearly gives the ideal $60\mathbb{Z}$.

(2) Let I be the ideal in $\mathbb{Z}[x]$ consisting of the polynomials with integer coefficients whose constant term is even (cf. Example 5). The two polynomials 2 and x are contained in I, so both $4 = 2 \cdot 2$ and $x^2 = x \cdot x$ are elements of the product ideal $I^2 = II$, as is their sum $x^2 + 4$. It is easy to check, however, that $x^2 + 4$ cannot be written as a single product $p(x)q(x)$ of two elements of I.

EXERCISES

Let R be a ring with identity $1 \neq 0$.

1. Prove that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

2. Prove that the rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

3. Find all homomorphic images of $\mathbb{Z}$.

4. Find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$. In each case describe the kernel and the image.
5. Describe all ring homomorphisms from the ring $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. In each case describe the kernel and the image.
6. Decide which of the following are ring homomorphisms from $M_2(\mathbb{Z})$ to $\mathbb{Z}$:
   (a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$ (projection onto the 1,1 entry)
   (b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$ (the *trace* of the matrix)
   (c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$ (the *determinant* of the matrix).
7. Let $R = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{Z}\}$ be the subring of $M_2(\mathbb{Z})$ of upper triangular matrices. Prove that the map
$$\varphi : R \to \mathbb{Z} \times \mathbb{Z} \quad \text{defined by} \quad \varphi : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a, d)$$
is a surjective homomorphism and describe its kernel.
8. Decide which of the following are ideals of the ring $\mathbb{Z} \times \mathbb{Z}$:
   (a) $\{(a, a) \mid a \in \mathbb{Z}\}$
   (b) $\{(2a, 2b) \mid a, b \in \mathbb{Z}\}$
   (c) $\{(2a, 0) \mid a \in \mathbb{Z}\}$
   (d) $\{(a, -a) \mid a \in \mathbb{Z}\}$.
9. Decide which of the sets in Exercise 6 of Section 1 are ideals of the ring of all functions from [0,1] to $\mathbb{R}$.
10. Decide which of the following are ideals of the ring $\mathbb{Z}[x]$:
    (a) the set of all polynomials whose constant term is a multiple of 3
    (b) the set of all polynomials whose coefficient of x^2 is a multiple of 3
    (c) the set of all polynomials whose constant term, coefficient of x and coefficient of x^2 are zero
    (d) $\mathbb{Z}[x^2]$ (i.e., the polynomials in which only even powers of x appear)
    (e) the set of polynomials whose coefficients sum to zero
    (f) the set of polynomials $p(x)$ such that $p'(0) = 0$, where $p'(x)$ is the usual first derivative of $p(x)$ with respect to x.
11. Let R be the ring of all continuous real valued functions on the closed interval $[0, 1]$. Prove that the map $\varphi : R \to \mathbb{R}$ defined by $\varphi(f) = \int_0^1 f(t)dt$ is a homomorphism of additive groups but not a ring homomorphism.
12. Let D be an integer that is not a perfect square in $\mathbb{Z}$ and let $S = \{\begin{pmatrix} a & b \\ Db & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$.
    (a) Prove that S is a subring of $M_2(\mathbb{Z})$.
    (b) If D is not a perfect square in $\mathbb{Z}$ prove that the map $\varphi : \mathbb{Z}[\sqrt{D}] \to S$ defined by $\varphi(a + b\sqrt{D}) = \begin{pmatrix} a & b \\ Db & a \end{pmatrix}$ is a ring isomorphism.
    (c) If $D \equiv 1 \bmod 4$ is squarefree, prove that the set $\{\begin{pmatrix} a & b \\ (D-1)b/4 & a+b \end{pmatrix} \mid a, b \in \mathbb{Z}\}$
    is a subring of $M_2(\mathbb{Z})$ and is isomorphic to the quadratic integer ring $\mathcal{O}$.

13. Prove that the ring $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\mathbb{C}$.

14. Prove that the ring $M_4(\mathbb{R})$ contains a subring that is isomorphic to the real Hamilton Quaternions, $\mathbb{H}$.

15. Let X be a nonempty set and let $\mathcal{P}(X)$ be the Boolean ring of all subsets of X defined in Exercise 21 of Section 1. Let R be the ring of all functions from X into $\mathbb{Z}/2\mathbb{Z}$. For each $A \in \mathcal{P}(X)$ define the function

$$\chi_A : X \to \mathbb{Z}/2\mathbb{Z} \qquad \text{by} \qquad \chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

(χ_A is called the *characteristic function of* A with values in $\mathbb{Z}/2\mathbb{Z}$). Prove that the map $\mathcal{P}(X) \to R$ defined by $A \mapsto \chi_A$ is a ring isomorphism.

16. Let $\varphi : R \to S$ be a surjective homomorphism of rings. Prove that the image of the center of R is contained in the center of S (cf. Exercise 7 of Section 1).

17. Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\varphi : R \to S$ be a nonzero homomorphism of rings.

(a) Prove that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

(b) Prove that if $\varphi(1_R) = 1_S$ then $\varphi(u)$ is a unit in S and that $\varphi(u^{-1}) = \varphi(u)^{-1}$ for each unit u of R.

18. **(a)** If I and J are ideals of R prove that their intersection $I \cap J$ is also an ideal of R.

(b) Prove that the intersection of an arbitrary nonempty collection of ideals is again an ideal (do not assume the collection is countable).

19. Prove that if $I_1 \subseteq I_2 \subseteq \cdots$ are ideals of R then $\cup_{n=1}^{\infty} I_n$ is an ideal of R.

20. Let I be an ideal of R and let S be a subring of R. Prove that $I \cap S$ is an ideal of S. Show by example that not every ideal of a subring S of a ring R need be of the form $I \cap S$ for some ideal I of R.

21. Prove that every (two-sided) ideal of $M_n(R)$ is equal to $M_n(J)$ for some (two-sided) ideal J of R. [Use Exercise 6(c) of Section 2 to show first that the set of entries of matrices in an ideal of $M_n(R)$ form an ideal in R.]

22. Let a be an element of the ring R.

(a) Prove that $\{x \in R \mid ax = 0\}$ is a right ideal and $\{y \in R \mid ya = 0\}$ is a left ideal (called respectively the right and left *annihilators* of a in R).

(b) Prove that if L is a left ideal of R then $\{x \in R \mid xa = 0 \text{ for all } a \in L\}$ is a two-sided ideal (called the left *annihilator* of L in R).

23. Let S be a subring of R and let I be an ideal of R. Prove that if $S \cap I = 0$ then $\overline{S} \cong S$, where the bar denotes passage to R/I.

24. Let $\varphi : R \to S$ be a ring homomorphism.

(a) Prove that if J is an ideal of S then $\varphi^{-1}(J)$ is an ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if J is an ideal of S then $J \cap R$ is an ideal of R.

(b) Prove that if φ is surjective and I is an ideal of R then $\varphi(I)$ is an ideal of S. Give an example where this fails if φ is not surjective.

25. Assume R is a commutative ring with 1. Prove that the Binomial Theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

holds in R, where the binomial coefficient $\binom{n}{k}$ is interpreted in R as the sum $1+1+\cdots+1$ of the identity 1 in R taken $\binom{n}{k}$ times.

26. The *characteristic* of a ring R is the smallest positive integer n such that $1+1+\cdots+1=0$ (n times) in R; if no such integer exists the characteristic of R is said to be 0. For example, $\mathbb{Z}/n\mathbb{Z}$ is a ring of characteristic n for each positive integer n and $\mathbb{Z}$ is a ring of characteristic 0.

(a) Prove that the map $\mathbb{Z} \to R$ defined by

$$k \mapsto \begin{cases} 1+1+\cdots+1 \ (k \text{ times}) & \text{if } k > 0 \\ 0 & \text{if } k = 0 \\ -1-1-\cdots-1 \ (-k \text{ times}) & \text{if } k < 0 \end{cases}$$

is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R (this explains the use of the terminology "characteristic 0" instead of the archaic phrase "characteristic ∞" for rings in which no sum of 1's is zero).

(b) Determine the characteristics of the rings $\mathbb{Q}$, $\mathbb{Z}[x]$, $\mathbb{Z}/n\mathbb{Z}[x]$.

(c) Prove that if p is a prime and if R is a commutative ring of characteristic p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

27. Prove that a nonzero Boolean ring has characteristic 2 (cf. Exercise 15, Section 1).

28. Prove that an integral domain has characteristic p, where p is either a prime or 0 (cf. Exercise 26).

29. Let R be a commutative ring. Recall (cf. Exercise 13, Section 1) that an element $x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of nilpotent elements form an ideal — called the *nilradical* of R and denoted by $\mathfrak{N}(R)$. [Use the Binomial Theorem to show $\mathfrak{N}(R)$ is closed under addition.]

30. Prove that if R is a commutative ring and $\mathfrak{N}(R)$ is its nilradical (cf. the preceding exercise) then zero is the only nilpotent element of $R/\mathfrak{N}(R)$ i.e., prove that $\mathfrak{N}(R/\mathfrak{N}(R)) = 0$.

31. Prove that the elements $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are nilpotent elements of $M_2(\mathbb{Z})$ whose sum is not nilpotent (note that these two matrices do not commute). Deduce that the set of nilpotent elements in the noncommutative ring $M_2(\mathbb{Z})$ is not an ideal.

32. Let $\varphi : R \to S$ be a homomorphism of rings. Prove that if x is a nilpotent element of R then $\varphi(x)$ is nilpotent in S.

33. Assume R is commutative. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$.

(a) Prove that $p(x)$ is a unit in $R[x]$ if and only if a_0 is a unit and $a_1, a_2, \ldots, a_n$ are nilpotent in R. [See Exercise 14 of Section 1.]

(b) Prove that $p(x)$ is nilpotent in $R[x]$ if and only if $a_0, a_1, \ldots, a_n$ are nilpotent elements of R.

34. Let I and J be ideals of R.

(a) Prove that $I + J$ is the smallest ideal of R containing both I and J.

(b) Prove that IJ is an ideal contained in $I \cap J$.

(c) Give an example where $IJ \neq I \cap J$.

(d) Prove that if R is commutative and if $I + J = R$ then $IJ = I \cap J$.

35. Let I, J, K be ideals of R.

(a) Prove that $I(J+K) = IJ + IK$ and $(I+J)K = IK + JK$.

(b) Prove that if $J \subseteq I$ then $I \cap (J+K) = J + (I \cap K)$.

36. Show that if I is the ideal of all polynomials in $\mathbb{Z}[x]$ with zero constant term then $I^n = \{a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{n+m}x^{n+m} \mid a_i \in \mathbb{Z},\ m \geq 0\}$ is the set of polynomials whose first nonzero term has degree at least n.

37. An ideal N is called *nilpotent* if N^n is the zero ideal for some $n \geq 1$. Prove that the ideal $p\mathbb{Z}/p^m\mathbb{Z}$ is a nilpotent ideal in the ring $\mathbb{Z}/p^m\mathbb{Z}$.

7.4 PROPERTIES OF IDEALS

Throughout this section R is a ring with identity $1 \neq 0$.

Definition. Let A be any subset of the ring R.

(1) Let (A) denote the smallest ideal of R containing A, called *the ideal generated by* A.

(2) Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$ i.e., $RA = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$ (where the convention is $RA = 0$ if $A = \emptyset$).
Similarly, $AR = \{a_1r_1 + a_2r_2 + \cdots + a_nr_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$ and $RAR = \{r_1a_1r_1' + r_2a_2r_2' + \cdots + r_na_nr_n' \mid r_i, r_i' \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$.

(3) An ideal generated by a single element is called a *principal ideal.*

(4) An ideal generated by a finite set is called a *finitely generated ideal.*

When $A = \{a\}$ or $\{a_1, a_2, \ldots\}$, etc., we shall drop the set brackets and simply write (a), $(a_1, a_2, \ldots)$ for (A), respectively.

The notion of ideals generated by subsets of a ring is analogous to that of subgroups generated by subsets of a group (Section 2.4). Since the intersection of any nonempty collection of ideals of R is also an ideal (cf. Exercise 18, Section 3) and A is always contained in at least one ideal (namely R), we have

$$(A) = \bigcap_{\substack{I \text{ an ideal} \\ A \subseteq I}} I\ ,$$

i.e., (A) is the intersection of all ideals of R that contain the set A.

The *left ideal generated by* A is the intersection of all left ideals of R that contain A. This left ideal is obtained from A by closing A under all the operations that define a left ideal. It is immediate from the definition that RA is closed under addition and under left multiplication by any ring element. Since R has an identity, RA contains A. Thus RA is a left ideal of R which contains A. Conversely, any left ideal which contains A must contain all finite sums of elements of the form ra, $r \in R$ and $a \in A$ and so must contain RA. Thus *RA is precisely the left ideal generated by A.* Similarly, *AR is the right ideal generated by A* and *RAR is the (two-sided) ideal generated by A.* In particular,

$$\textit{if } R \textit{ is commutative then } RA = AR = RAR = (A).$$

When R is a commutative ring and $a \in R$, the principal ideal (a) generated by a is just the set of all R-multiples of a. If R is not commutative, however, the set

$\{ras \mid r, s \in R\}$ is not necessarily the two-sided ideal generated by a since it need not be closed under addition (in this case the ideal generated by a is the ideal RaR, which consists of all *finite sums* of elements of the form ras, $r, s \in R$).

The formation of principal ideals in a commutative ring is a particularly simple way of creating ideals, similar to generating cyclic subgroups of a group. Notice that the element $b \in R$ belongs to the ideal (a) if and only if $b = ra$ for some $r \in R$, i.e., if and only if *b is a multiple of a* or, put another way, *a divides b in R*. Also, $b \in (a)$ if and only if $(b) \subseteq (a)$. Thus containment relations between ideals, in particular between principal ideals, is seen to capture some of the arithmetic of general commutative rings. Commutative rings in which all ideals are principal are among the easiest to study and these will play an important role in Chapters 8 and 9.

Examples

(1) The trivial ideal 0 and the ideal R are both principal: $0 = (0)$ and $R = (1)$.

(2) In $\mathbb{Z}$ we have $n\mathbb{Z} = \mathbb{Z}n = (n) = (-n)$ for all integers n. Thus our notation for aR is consistent with the definition of $n\mathbb{Z}$ we have been using. As noted in the preceding section, these are all the ideals of $\mathbb{Z}$ so *every* ideal of $\mathbb{Z}$ is principal. For positive integers n and m, $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if m divides n in $\mathbb{Z}$, so the lattice of ideals containing $n\mathbb{Z}$ is the same as the lattice of divisors of n. Furthermore, the ideal generated by two nonzero integers n and m is the principal ideal generated by their greatest common divisor, d: $(n, m) = (d)$. The notation for (n, m) as the greatest common divisor of n and m is thus consistent with the same notation for the ideal generated by n and m (although a principal generator for the ideal generated by n and m is determined only up to a $\pm$ sign — we could make it unique by choosing a nonnegative generator). In particular, n and m are relatively prime if and only if $(n, m) = (1)$.

(3) We show that the ideal $(2, x)$ generated by 2 and x in $\mathbb{Z}[x]$ is *not* a principal ideal. Observe that $(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$ and so this ideal consists precisely of the polynomials with integer coefficients whose constant term is even (as discussed in Example 5 in the preceding section) — in particular, this is a proper ideal. Assume by way of contradiction that $(2, x) = (a(x))$ for some $a(x) \in \mathbb{Z}[x]$. Since $2 \in (a(x))$ there must be some $p(x)$ such that $2 = p(x)a(x)$. The degree of $p(x)a(x)$ equals degree $p(x)$ + degree $a(x)$, hence both $p(x)$ and $a(x)$ must be constant polynomials, i.e., integers. Since 2 is a prime number, $a(x)$, $p(x) \in \{\pm 1, \pm 2\}$. If $a(x)$ were ± 1 then every polynomial would be a multiple of $a(x)$, contrary to $(a(x))$ being a proper ideal. The only possibility is $a(x) = \pm 2$. But now $x \in (a(x)) = (2) = (-2)$ and so $x = 2q(x)$ for some polynomial $q(x)$ with integer coefficients, clearly impossible. This contradiction proves that $(2, x)$ is not principal.

Note that the symbol (A) is ambiguous if the ring is not specified: the ideal generated by 2 and x in $\mathbb{Q}[x]$ is the entire ring (1) since it contains the element $\frac{1}{2}2 = 1$.

We shall see in Chapter 9 that for any *field* F, all ideals of $F[x]$ *are* principal.

(4) If R is the ring of all functions from the closed interval $[0,1]$ into $\mathbb{R}$ let M be the ideal $\{f \mid f(\frac{1}{2}) = 0\}$ (the kernel of evaluation at $\frac{1}{2}$). Let $g(x)$ be the function which is zero at $x = \frac{1}{2}$ and 1 at all other points. Then $f = fg$ for all $f \in M$ so M is a principal ideal with generator g. In fact, *any* function which is zero at $\frac{1}{2}$ and nonzero at all other points is another generator for the same ideal M.

On the other hand, if R is the ring of all *continuous* functions from $[0,1]$ to $\mathbb{R}$ then $\{f \mid f(\frac{1}{2}) = 0\}$ is *not* principal nor is it even finitely generated (cf. the exercises).

(5) If G is a finite group and R is a commutative ring with 1 then the augmentation ideal is generated by the set $\{g - 1 \mid g \in G\}$, although this need not be a minimal set of generators. For example, if G is a cyclic group with generator σ, then the augmentation ideal is a principal ideal with generator $\sigma - 1$.

Proposition 9. Let I be an ideal of R.

(1) $I = R$ if and only if I contains a unit.

(2) Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Proof: (1) If $I = R$ then I contains the unit 1. Conversely, if u is a unit in I with inverse v, then for any $r \in R$

$$r = r \cdot 1 = r(vu) = (rv)u \in I$$

hence $R = I$.

(2) The ring R is a field if and only if every nonzero element is a unit. If R is a field every nonzero ideal contains a unit, so by the first part R is the only nonzero ideal. Conversely, if 0 and R are the only ideals of R let u be any nonzero element of R. By hypothesis $(u) = R$ and so $1 \in (u)$. Thus there is some $v \in R$ such that $1 = vu$, i.e., u is a unit. Every nonzero element of R is therefore a unit and so R is a field.

Corollary 10. If R is a field then any nonzero ring homomorphism from R into another ring is an injection.

Proof: The kernel of a ring homomorphism is an ideal. The kernel of a nonzero homomorphism is a proper ideal hence is 0 by the proposition.

These results show that the ideal structure of fields is trivial. Our approach to studying an algebraic structure through its homomorphisms will still play a fundamental role in field theory (Part IV) when we study injective homomorphisms (embeddings) of one field into another and automorphisms of fields (isomorphisms of a field to itself).

If D is a ring with identity $1 \neq 0$ in which the only left ideals and the only right ideals are 0 and D, then D is a division ring. Conversely, the only (left, right or two-sided) ideals in a division ring D are 0 and D, which gives an analogue of Proposition 9(2) if R is not commutative (see the exercises). However, if F is a field, then for any $n \geq 2$ the only two-sided ideals in the matrix ring $M_n(F)$ are 0 and $M_n(F)$, even though this is not a division ring (it does have proper, nontrivial, left and right ideals: cf. Section 3), which shows that Proposition 9(2) does not hold for noncommutative rings. Rings whose only two-sided ideals are 0 and the whole ring (which are called *simple rings*) will be studied in Chapter 18.

One important class of ideals are those which are not contained in any other proper ideal:

Definition. An ideal M in an arbitrary ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S.

A general ring need not have maximal ideals. For example, take any abelian group which has no maximal subgroups (for example, $\mathbb{Q}$ — cf. Exercise 16, Section 6.1) and make it into a trivial ring by defining $ab = 0$ for all a, b. In such a ring the ideals are simply the subgroups and so there are no maximal ideals. The zero ring has no maximal ideals, hence any result involving maximal ideals forces a ring to be nonzero. The next proposition shows that rings with an identity $1 \neq 0$ always possess maximal ideals. Like many such general existence theorems (e.g., the result that a finitely generated group has maximal subgroups or that every vector space has a basis) the proof relies on Zorn's Lemma (see Appendix I). In many specific rings, however, the presence of maximal ideals is often obvious, independent of Zorn's Lemma.

Proposition 11. In a ring with identity every proper ideal is contained in a maximal ideal.

Proof: Let R be a ring with identity and let I be a proper ideal (so R cannot be the zero ring, i.e., $1 \neq 0$). Let $\mathcal{S}$ be the set of all proper ideals of R which contain I. Then $\mathcal{S}$ is nonempty ($I \in \mathcal{S}$) and is partially ordered by inclusion. If $\mathcal{C}$ is a chain in $\mathcal{S}$, define J to be the union of all ideals in $\mathcal{C}$:

$$J = \bigcup_{A \in \mathcal{C}} A.$$

We first show that J is an ideal. Certainly J is nonempty because $\mathcal{C}$ is nonempty — specifically, $0 \in J$ since 0 is in every ideal A. If $a, b \in J$, then there are ideals $A, B \in \mathcal{C}$ such that $a \in A$ and $b \in B$. By definition of a chain either $A \subseteq B$ or $B \subseteq A$. In either case $a - b \in J$, so J is closed under subtraction. Since each $A \in \mathcal{C}$ is closed under left and right multiplication by elements of R, so is J. This proves J is an ideal.

If J is not a proper ideal then $1 \in J$. In this case, by definition of J we must have $1 \in A$ for some $A \in \mathcal{C}$. This is a contradiction because each A is a proper ideal ($A \in \mathcal{C} \subseteq \mathcal{S}$). This proves that each chain has an upper bound in $\mathcal{S}$. By Zorn's Lemma $\mathcal{S}$ has a maximal element which is therefore a maximal (proper) ideal containing I.

For commutative rings the next result characterizes maximal ideals by the structure of their quotient rings.

Proposition 12. Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Proof: This follows from the Lattice Isomorphism Theorem together with Proposition 9(2). The ideal M is maximal if and only if there are no ideals I with $M \subset I \subset R$. By the Lattice Isomorphism Theorem the ideals of R containing M correspond bijectively with the ideals of R/M, so M is maximal if and only if the only ideals of R/M are 0 and R/M. By Proposition 9(2) we see that M is maximal if and only if R/M is a field.

The proposition above indicates how to *construct* some fields: take the quotient of any commutative ring R with identity by a maximal ideal in R. We shall use this in Part IV to construct all finite fields by taking quotients of the ring $\mathbb{Z}[x]$ by maximal ideals.

Examples

(1) Let n be a nonnegative integer. The ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is a maximal ideal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field. We saw in Section 3 that this is the case if and only if n is a prime number. This also follows directly from the containment of ideals of $\mathbb{Z}$ described in Example 2 above.

(2) The ideal $(2, x)$ is a maximal ideal in $\mathbb{Z}[x]$ because its quotient ring is the field $\mathbb{Z}/2\mathbb{Z}$ — cf. Example 3 above and Example 5 at the end of Section 3.

(3) The ideal (x) in $\mathbb{Z}[x]$ is not a maximal ideal because $(x) \subset (2, x) \subset \mathbb{Z}[x]$. The quotient ring $\mathbb{Z}[x]/(x)$ is isomorphic to $\mathbb{Z}$ (the ideal (x) in $\mathbb{Z}[x]$ is the kernel of the surjective ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}$ given by evaluation at 0). Since $\mathbb{Z}$ is not a field, we see again that (x) is not a maximal ideal in $\mathbb{Z}[x]$.

(4) Let R be the ring of all functions from [0,1] to $\mathbb{R}$ and for each $a \in [0, 1]$ let M_a be the kernel of evaluation at a. Since evaluation is a surjective homomorphism from R to $\mathbb{R}$, we see that $R/M_a \cong \mathbb{R}$ and hence M_a is a maximal ideal. Similarly, the kernel of evaluation at any fixed point is a maximal ideal in the ring of continuous real valued functions on [0, 1].

(5) If F is a field and G is a finite group, then the augmentation ideal I is a maximal ideal of the group ring FG (cf. Example 7 at the end of the preceding section). The augmentation ideal is the kernel of the augmentation map which is a surjective homomorphism onto the field F (i.e., $FG/I \cong F$, a field). Note that Proposition 12 does not apply directly since FG need not be commutative, however, the implication in Proposition 12 that I is a maximal ideal if R/I is a field holds for arbitrary rings.

Definition. Assume R is commutative. An ideal P is called a *prime ideal* if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

The notion of a maximal ideal is fairly intuitive but the definition of a prime ideal may seem a little strange. It is, however, a natural generalization of the notion of a "prime" in the integers $\mathbb{Z}$. Let n be a nonnegative integer. According to the above definition the ideal $n\mathbb{Z}$ is a *prime* ideal provided $n \neq 1$ (to ensure that the ideal is proper) and provided every time the product ab of two integers is an element of $n\mathbb{Z}$, at least one of a, b is an element of $n\mathbb{Z}$. Put another way, if $n \neq 0$, it must have the property that whenever n divides ab, n must divide a or divide b. This is equivalent to the usual definition that n is a prime number. Thus *the prime ideals of $\mathbb{Z}$ are just the ideals $p\mathbb{Z}$ of $\mathbb{Z}$ generated by prime numbers p together with the ideal 0.*

For the integers $\mathbb{Z}$ there is no difference between the maximal ideals and the nonzero prime ideals. This is not true in general, but we shall see shortly that every maximal ideal is a prime ideal. First we translate the notion of prime ideals into properties of quotient rings as we did for maximal ideals in Proposition 12. Recall that an integral domain is a commutative ring with identity $1 \neq 0$ that has no zero divisors.

Proposition 13. Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Proof: This proof is simply a matter of translating the definition of a prime ideal into the language of quotients. The ideal P is prime if and only if $P \neq R$ and whenever

$ab \in P$, then either $a \in P$ or $b \in P$. Use the bar notation for elements of R/P: $\bar{r} = r + P$. Note that $r \in P$ if and only if the element $\bar{r}$ is zero in the quotient ring R/P. Thus in the terminology of quotients P is a prime ideal if and only if $\bar{R} \neq \bar{0}$ and whenever $\overline{ab} = \bar{a}\bar{b} = \bar{0}$, then either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, i.e., R/P is an integral domain.

It follows in particular that a commutative ring with identity is an integral domain if and only if 0 is a prime ideal.

Corollary 14. Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof: If M is a maximal ideal then R/M is a field by Proposition 12. A field is an integral domain so the corollary follows from Proposition 13.

Examples

(1) The principal ideals generated by primes in $\mathbb{Z}$ are both prime and maximal ideals. The zero ideal in $\mathbb{Z}$ is prime but not maximal.

(2) The ideal (x) is a prime ideal in $\mathbb{Z}[x]$ since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. This ideal is not a maximal ideal. The ideal 0 is a prime ideal in $\mathbb{Z}[x]$, but is not a maximal ideal.

EXERCISES

Let R be a ring with identity $1 \neq 0$.

1. Let L_j be the left ideal of $M_n(R)$ consisting of arbitrary entries in the j^{th} column and zero in all other entries and let E_{ij} be the element of $M_n(R)$ whose i, j entry is 1 and whose other entries are all 0. Prove that $L_j = M_n(R)E_{ij}$ for any i. [See Exercise 6, Section 2.]

2. Assume R is commutative. Prove that the augmentation ideal in the group ring RG is generated by $\{g - 1 \mid g \in G\}$. Prove that if $G = \langle \sigma \rangle$ is cyclic then the augmentation ideal is generated by $\sigma - 1$.

3. **(a)** Let p be a prime and let G be an abelian group of order p^n. Prove that the nilradical of the group ring $\mathbb{F}_p G$ is the augmentation ideal (cf. Exercise 29, Section 3). [Use the preceding exercise.]

(b) Let $G = \{g_1, \ldots, g_n\}$ be a finite group and assume R is commutative. Prove that if r is any element of the augmentation ideal of RG then $r(g_1 + \cdots + g_n) = 0$. [Use the preceding exercise.]

4. Assume R is commutative. Prove that R is a field if and only if 0 is a maximal ideal.

5. Prove that if M is an ideal such that R/M is a field then M is a maximal ideal (do not assume R is commutative).

6. Prove that R is a division ring if and only if its only left ideals are (0) and R. (The analogous result holds when "left" is replaced by "right.")

7. Let R be a commutative ring with 1. Prove that the principal ideal generated by x in the polynomial ring $R[x]$ is a prime ideal if and only if R is an integral domain. Prove that (x) is a maximal ideal if and only if R is a field.

8. Let R be an integral domain. Prove that $(a) = (b)$ for some elements $a, b \in R$, if and only if $a = ub$ for some unit u of R.

9. Let R be the ring of all continuous functions on $[0, 1]$ and let I be the collection of functions $f(x)$ in R with $f(1/3) = f(1/2) = 0$. Prove that I is an ideal of R but is not a prime ideal.

10. Assume R is commutative. Prove that if P is a prime ideal of R and P contains no zero divisors then R is an integral domain.

11. Assume R is commutative. Let I and J be ideals of R and assume P is a prime ideal of R that contains IJ (for example, if P contains $I \cap J$). Prove either I or J is contained in P.

12. Assume R is commutative and suppose $I = (a_1, a_2, \ldots, a_n)$ and $J = (b_1, b_2, \ldots, b_m)$ are two finitely generated ideals in R. Prove that the product ideal IJ is finitely generated by the elements $a_i b_j$ for $i = 1, 2, \ldots, n$, and $j = 1, 2, \ldots, m$.

13. Let $\varphi : R \to S$ be a homomorphism of commutative rings.

(a) Prove that if P is a prime ideal of S then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime ideal of S then $P \cap R$ is either R or a prime ideal of R.

(b) Prove that if M is a maximal ideal of S and φ is surjective then $\varphi^{-1}(M)$ is a maximal ideal of R. Give an example to show that this need not be the case if φ is not surjective.

14. Assume R is commutative. Let x be an indeterminate, let $f(x)$ be a monic polynomial in $R[x]$ of degree $n \geq 1$ and use the bar notation to denote passage to the quotient ring $R[x]/(f(x))$.

(a) Show that every element of $R[x]/(f(x))$ is of the form $\overline{p(x)}$ for some polynomial $p(x) \in R[x]$ of degree less than n, i.e.,

$$R[x]/(f(x)) = \{\overline{a_0} + \overline{a_1}\overline{x} + \cdots + \overline{a_{n-1}x^{n-1}} \mid a_0, a_1, \ldots, a_{n-1} \in R\}.$$

[If $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ then $\overline{x^n} = \overline{-(b_{n-1}x^{n-1} + \cdots + b_0)}$. Use this to reduce powers of $\overline{x}$ in the quotient ring.]

(b) Prove that if $p(x)$ and $q(x)$ are distinct polynomials in $R[x]$ which are both of degree less than n, then $\overline{p(x)} \neq \overline{q(x)}$. [Otherwise $p(x) - q(x)$ is an $R[x]$-multiple of the monic polynomial $f(x)$.]

(c) If $f(x) = a(x)b(x)$ where both $a(x)$ and $b(x)$ have degree less than n, prove that $\overline{a(x)}$ is a zero divisor in $R[x]/(f(x))$.

(d) If $f(x) = x^n - a$ for some nilpotent element $a \in R$, prove that $\overline{x}$ is nilpotent in $R[x]/(f(x))$.

(e) Let p be a prime, assume $R = \mathbb{F}_p$ and $f(x) = x^p - a$ for some $a \in \mathbb{F}_p$. Prove that $\overline{x - a}$ is nilpotent in $R[x]/(f(x))$. [Use Exercise 26(c) of Section 3.]

15. Let $x^2 + x + 1$ be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{F}_2[x]/(x^2 + x + 1)$.

(a) Prove that $\overline{E}$ has 4 elements: $\overline{0}$, $\overline{1}$, $\overline{x}$ and $\overline{x+1}$.

(b) Write out the 4×4 addition table for $\overline{E}$ and deduce that the additive group $\overline{E}$ is isomorphic to the Klein 4-group.

(c) Write out the 4×4 multiplication table for $\overline{E}$ and prove that $\overline{E}^\times$ is isomorphic to the cyclic group of order 3. Deduce that $\overline{E}$ is a field.

16. Let $x^4 - 16$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^4 - 16)$.

(a) Find a polynomial of degree ≤ 3 that is congruent to $7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3$ modulo $(x^4 - 16)$.

(b) Prove that $\overline{x-2}$ and $\overline{x+2}$ are zero divisors in $\overline{E}$.

17. Let $x^3 - 2x + 1$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^3 - 2x + 1)$. Let $p(x) = 2x^7 - 7x^5 + 4x^3 - 9x + 1$ and let $q(x) = (x-1)^4$.

(a) Express each of the following elements of $\overline{E}$ in the form $\overline{f(x)}$ for some polynomial $f(x)$ of degree ≤ 2: $\overline{p(x)}$, $\overline{q(x)}$, $\overline{p(x)+q(x)}$ and $\overline{p(x)q(x)}$.
(b) Prove that $\overline{E}$ is not an integral domain.
(c) Prove that $\bar{x}$ is a unit in $\overline{E}$.

18. Prove that if R is an integral domain and $R[[x]]$ is the ring of formal power series in the indeterminate x then the principal ideal generated by x is a prime ideal (cf. Exercise 3, Section 2). Prove that the principal ideal generated by x is a maximal ideal if and only if R is a field.

19. Let R be a finite commutative ring with identity. Prove that every prime ideal of R is a maximal ideal.

20. Prove that a nonzero finite commutative ring that has no zero divisors is a field (if the ring has an identity, this is Corollary 3, so do not assume the ring has a 1).

21. Prove that a finite ring with identity $1 \neq 0$ that has no zero divisors is a field (you may quote Wedderburn's Theorem).

22. Let $p \in \mathbb{Z}^+$ be a prime and let the $\mathbb{F}_p$ Quaternions be defined by

$$a + bi + cj + dk \qquad a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$$

where addition is componentwise and multiplication is defined using the same relations on i, j, k as for the real Quaternions.
(a) Prove that the $\mathbb{F}_p$ Quaternions are a homomorphic image of the integral Quaternions (cf. Section 1).
(b) Prove that the $\mathbb{F}_p$ Quaternions contain zero divisors (and so they cannot be a division ring). [Use the preceding exercise.]

23. Prove that in a Boolean ring (cf. Exercise 15, Section 1) every prime ideal is a maximal ideal.

24. Prove that in a Boolean ring every finitely generated ideal is principal.

25. Assume R is commutative and for each $a \in R$ there is an integer $n > 1$ (depending on a) such that $a^n = a$. Prove that every prime ideal of R is a maximal ideal.

26. Prove that a prime ideal in a commutative ring R contains every nilpotent element (cf. Exercise 13, Section 1). Deduce that the nilradical of R (cf. Exercise 29, Section 3) is contained in the intersection of all the prime ideals of R. (It is shown in Section 15.2 that the nilradical of R is equal to the intersection of all prime ideals of R.)

27. Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R then $1 - ab$ is a unit for all $b \in R$.

28. Prove that if R is a commutative ring and $N = (a_1, a_2, \ldots, a_m)$ where each a_i is a nilpotent element, then N is a nilpotent ideal (cf. Exercise 37, Section 3). Deduce that if the nilradical of R is finitely generated then it is a nilpotent ideal.

29. Let p be a prime and let G be a finite group of order a power of p (i.e., a p-group). Prove that the augmentation ideal in the group ring $\mathbb{Z}/p\mathbb{Z}G$ is a nilpotent ideal. (Note that this ring may be noncommutative.) [Use Exercise 2.]

30. Let I be an ideal of the commutative ring R and define

$$\text{rad } I = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\}$$

called the *radical* of I. Prove that rad I is an ideal containing I and that $(\text{rad } I)/I$ is the nilradical of the quotient ring R/I, i.e., $(\text{rad } I)/I = \mathfrak{N}(R/I)$ (cf. Exercise 29, Section 3).

31. An ideal I of the commutative ring R is called a *radical ideal* if rad $I = I$.

(a) Prove that every prime ideal of R is a radical ideal.

(b) Let $n > 1$ be an integer. Prove that 0 is a radical ideal in $\mathbb{Z}/n\mathbb{Z}$ if and only if n is a product of distinct primes to the first power (i.e., n is square free). Deduce that (n) is a radical ideal of $\mathbb{Z}$ if and only if n is a product of distinct primes in $\mathbb{Z}$.

32. Let I be an ideal of the commutative ring R and define

$$\text{Jac } I \text{ to be the intersection of all maximal ideals of } R \text{ that contain } I$$

where the convention is that Jac $R = R$. (If I is the zero ideal, Jac 0 is called the *Jacobson radical* of the ring R, so Jac I is the preimage in R of the Jacobson radical of R/I.)

(a) Prove that Jac I is an ideal of R containing I.

(b) Prove that rad $I \subseteq$ Jac I, where rad I is the radical of I defined in Exercise 30.

(c) Let $n > 1$ be an integer. Describe Jac $n\mathbb{Z}$ in terms of the prime factorization of n.

33. Let R be the ring of all continuous functions from the closed interval [0,1] to $\mathbb{R}$ and for each $c \in [0, 1]$ let $M_c = \{f \in R \mid f(c) = 0\}$ (recall that M_c was shown to be a maximal ideal of R).

(a) Prove that if M is *any* maximal ideal of R then there is a real number $c \in [0, 1]$ such that $M = M_c$.

(b) Prove that if b and c are distinct points in [0,1] then $M_b \neq M_c$.

(c) Prove that M_c is not equal to the principal ideal generated by $x - c$.

(d) Prove that M_c is not a finitely generated ideal.

The preceding exercise shows that there is a bijection between the *points* of the closed interval [0,1] and the set of *maximal ideals* in the ring R of all of continuous functions on [0,1] given by $c \leftrightarrow M_c$. For any subset X of $\mathbb{R}$ or, more generally, for any completely regular topological space X, the map $c \mapsto M_c$ is an *injection* from X to the set of maximal ideals of R, where R is the ring of all bounded continuous real valued functions on X and M_c is the maximal ideal of functions that vanish at c. Let $\beta(X)$ be the set of maximal ideals of R. One can put a topology on $\beta(X)$ in such a way that if we identify X with its image in $\beta(X)$ then X (in its given topology) becomes a subspace of $\beta(X)$. Moreover, $\beta(X)$ is a compact space under this topology and is called the *Stone-Čech compactification* of X.

34. Let R be the ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ and for each $c \in \mathbb{R}$ let M_c be the maximal ideal $\{f \in R \mid f(c) = 0\}$.

(a) Let I be the collection of functions $f(x)$ in R with *compact support* (i.e., $f(x) = 0$ for $|x|$ sufficiently large). Prove that I is an ideal of R that is not a prime ideal.

(b) Let M be a maximal ideal of R containing I (properly, by (a)). Prove that $M \neq M_c$ for any $c \in \mathbb{R}$ (cf. the preceding exercise).

35. Let $A = (a_1, a_2, \ldots, a_n)$ be a nonzero finitely generated ideal of R. Prove that there is an ideal B which is maximal with respect to the property that it does not contain A. [Use Zorn's Lemma.]

36. Assume R is commutative. Prove that the set of prime ideals in R has a minimal element with respect to inclusion (possibly the zero ideal). [Use Zorn's Lemma.]

37. A commutative ring R is called a *local ring* if it has a unique maximal ideal. Prove that if R is a local ring with maximal ideal M then every element of $R - M$ is a unit. Prove conversely that if R is a commutative ring with 1 in which the set of nonunits forms an ideal M, then R is a local ring with unique maximal ideal M.

38. Prove that the ring of all rational numbers whose denominators is odd is a local ring whose unique maximal ideal is the principal ideal generated by 2.

39. Following the notation of Exercise 26 in Section 1, let K be a field, let v be a discrete

valuation on K and let R be the valuation ring of v. For each integer $k \geq 0$ define $A_k = \{r \in R \mid v(r) \geq k\} \cup \{0\}$.

(a) Prove that A_k is a principal ideal and that $A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots$.

(b) Prove that if I is any nonzero ideal of R, then $I = A_k$ for some $k \geq 0$. Deduce that R is a local ring with unique maximal ideal A_1.

40. Assume R is commutative. Prove that the following are equivalent: (see also Exercises 13 and 14 in Section 1)

(i) R has exactly one prime ideal

(ii) every element of R is either nilpotent or a unit

(iii) $R/\eta(R)$ is a field (cf. Exercise 29, Section 3).

41. A proper ideal Q of the commutative ring R is called *primary* if whenever $ab \in Q$ and $a \notin Q$ then $b^n \in Q$ for some positive integer n. (Note that the symmetry between a and b in this definition implies that if Q is a primary ideal and $ab \in Q$ with *neither* a nor b in Q, then a positive power of a and a positive power of b both lie in Q.) Establish the following facts about primary ideals.

(a) The primary ideals of $\mathbb{Z}$ are 0 and (p^n), where p is a prime and n is a positive integer.

(b) Every prime ideal of R is a primary ideal.

(c) An ideal Q of R is primary if and only if every zero divisor in R/Q is a nilpotent element of R/Q.

(d) If Q is a primary ideal then $\text{rad}(Q)$ is a prime ideal (cf. Exercise 30).

7.5 RINGS OF FRACTIONS

Throughout this section R is a commutative ring. Proposition 2 shows that if a is not zero nor a zero divisor and $ab = ac$ in R then $b = c$. Thus a nonzero element that is not a zero divisor enjoys some of the properties of a unit without necessarily possessing a multiplicative inverse in R. On the other hand, we saw in Section 1 that a zero divisor a cannot be a unit in R and, by definition, if a is a zero divisor we cannot always cancel the a's in the equation $ab = ac$ to obtain $b = c$ (take $c = 0$ for example). The aim of this section is to prove that a commutative ring R is always a subring of a larger ring Q in which every nonzero element of R that is not a zero divisor is a unit in Q. The principal application of this will be to integral domains, in which case this ring Q will be a field — called its *field of fractions* or *quotient field*. Indeed, the paradigm for the construction of Q from R is the one offered by the construction of the field of rational numbers from the integral domain $\mathbb{Z}$.

In order to see the essential features of the construction of the field $\mathbb{Q}$ from the integral domain $\mathbb{Z}$ we review the basic properties of fractions. Each rational number may be represented in many different ways as the quotient of two integers (for example, $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \ldots$, etc.). These representations are related by

$$\frac{a}{b} = \frac{c}{d} \qquad \text{if and only if} \qquad ad = bc.$$

In more precise terms, the fraction $\frac{a}{b}$ is the equivalence class of ordered pairs (a, b) of integers with $b \neq 0$ under the equivalence relation: $(a, b) \sim (c, d)$ if and only if

$ad = bc$. The arithmetic operations on fractions are given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

These are well defined (independent of choice of representatives of the equivalence classes) and make the set of fractions into a commutative ring (in fact, a field), $\mathbb{Q}$. The integers $\mathbb{Z}$ are identified with the subring $\{\frac{a}{1} \mid a \in \mathbb{Z}\}$ of $\mathbb{Q}$ and every nonzero integer a has an inverse $\frac{1}{a}$ in $\mathbb{Q}$.

It seems reasonable to attempt to follow the same steps for any commutative ring R, allowing arbitrary denominators. If, however, b is zero or a zero divisor in R, say $bd = 0$, and if we allow b as a denominator, then we should expect to have

$$d = \frac{d}{1} = \frac{bd}{b} = \frac{0}{b} = 0$$

in the "ring of fractions" (where, for convenience, we have assumed R has a 1). Thus if we allow zero or zero divisors as denominators there must be some collapsing in the sense that we cannot expect R to appear naturally as a subring of this "ring of fractions." A second restriction is more obviously imposed by the laws of addition and multiplication: if ring elements b and d are allowed as denominators, then bd must also be a denominator, i.e., the set of denominators must be closed under multiplication in R. The main result of this section shows that these two restrictions are sufficient to construct a ring of fractions for R. Note that this theorem includes the construction of $\mathbb{Q}$ from $\mathbb{Z}$ as a special case.

Theorem 15. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors and is closed under multiplication (i.e., $ab \in D$ for all $a, b \in D$). Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties.

(1) every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$ then Q is a field.

(2) (uniqueness of Q) The ring Q is the *"smallest"* ring containing R in which all elements of D become units, in the following sense. Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Remark: In Section 15.4 a more general construction is given. The proof of the general result is more technical but relies on the same basic rationale and steps as the proof of Theorem 15. Readers wishing greater generality may read the proof below and the beginning of Section 15.4 in concert.

Proof: Let $\mathcal{F} = \{(r, d) \mid r \in R,\ d \in D\}$ and define the relation $\sim$ on $\mathcal{F}$ by

$$(r, d) \sim (s, e) \qquad \text{if and only if} \qquad re = sd.$$

It is immediate that this relation is reflexive and symmetric. Suppose $(r, d) \sim (s, e)$ and $(s, e) \sim (t, f)$. Then $re - sd = 0$ and $sf - te = 0$. Multiplying the first of these equations by f and the second by d and adding them gives $(rf - td)e = 0$. Since $e \in D$ is neither zero nor a zero divisor we must have $rf - td = 0$, i.e., $(r, d) \sim (t, f)$. This proves $\sim$ is transitive, hence an equivalence relation. Denote the equivalence class of (r, d) by $\frac{r}{d}$:

$$\frac{r}{d} = \{(a, b) \mid a \in R,\ b \in D \text{ and } rb = ad\}.$$

Let Q be the set of equivalence classes under $\sim$. Note that $\frac{r}{d} = \frac{re}{de}$ in Q for all $e \in D$, since D is closed under multiplication.

We now define an additive and multiplicative structure on Q:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

In order to prove that Q is a commutative ring with identity there are a number of things to check:

(1) these operations are well defined (i.e., do not depend on the choice of representatives for the equivalence classes),

(2) Q is an abelian group under addition, where the additive identity is $\frac{0}{d}$ for any $d \in D$ and the additive inverse of $\frac{a}{d}$ is $\frac{-a}{d}$,

(3) multiplication is associative, distributive and commutative, and

(4) Q has an identity ($= \frac{d}{d}$ for any $d \in D$).

These are all completely straightforward calculations involving only arithmetic in R and the definition of $\sim$. Again we need D to be closed under multiplication for addition and multiplication to be defined.

For example, to check that addition is well defined assume $\frac{a}{b} = \frac{a'}{b'}$ (i.e., $ab' = a'b$) and $\frac{c}{d} = \frac{c'}{d'}$ (i.e., $cd' = c'd$). We must show that $\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}$, i.e.,

$$(ad + bc)(b'd') = (a'd' + b'c')(bd).$$

The left hand side of this equation is $ab'dd' + cd'bb'$ substituting $a'b$ for ab' and $c'd$ for cd' gives $a'bdd' + c'dbb'$, which is the right hand side. Hence addition of fractions is well defined. Checking the details in the other parts of (1) to (4) involves even easier manipulations and so is left as an exercise.

Next we embed R into Q by defining

$$\iota : R \to Q \qquad \text{by} \qquad \iota : r \mapsto \frac{rd}{d} \quad \text{where } d \text{ is any element of } D.$$

Since $\frac{rd}{d} = \frac{re}{e}$ for all $d, e \in D$, $\iota(r)$ does not depend on the choice of $d \in D$. Since D is closed under multiplication, one checks directly that ι is a ring homomorphism.

Furthermore, ι is injective because

$$\iota(r) = 0 \Leftrightarrow \frac{rd}{d} = \frac{0}{d} \Leftrightarrow rd^2 = 0 \Leftrightarrow r = 0$$

because d (hence also d^2) is neither zero nor a zero divisor. The subring $\iota(R)$ of Q is therefore isomorphic to R. We henceforth identify each $r \in R$ with $\iota(r)$ and so consider R as a subring of Q.

Next note that each $d \in D$ has a multiplicative inverse in Q: namely, if d is represented by the fraction $\frac{de}{e}$ then its multiplicative inverse is $\frac{e}{de}$. One then sees that every element of Q may be written as $r \cdot d^{-1}$ for some $r \in R$ and some $d \in D$. In particular, if $D = R - \{0\}$, every nonzero element of Q has a multiplicative inverse and Q is a field.

It remains to establish the uniqueness property of Q. Assume $\varphi : R \to S$ is an injective ring homomorphism such that $\varphi(d)$ is a unit in S for all $d \in D$. Extend φ to a map $\Phi : Q \to S$ by defining $\Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1}$ for all $r \in R$, $d \in D$. This map is well defined, since $rd^{-1} = se^{-1}$ implies $re = sd$, so $\varphi(r)\varphi(e) = \varphi(s)\varphi(d)$, and then

$$\Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1} = \varphi(s)\varphi(e)^{-1} = \Phi(se^{-1}).$$

It is straightforward to check that Φ is a ring homomorphism — the details are left as an exercise. Finally, Φ is injective because $rd^{-1} \in \ker \Phi$ implies $r \in \ker \Phi \cap R = \ker \varphi$; since φ is injective this forces r and hence also rd^{-1} to be zero. This completes the proof.

Definition. Let R, D and Q be as in Theorem 15.

(1) The ring Q is called the *ring of fractions* of D with respect to R and is denoted $D^{-1}R$.

(2) If R is an integral domain and $D = R - \{0\}$, Q is called the *field of fractions* or *quotient field* of R.

If A is a subset of a field F (for example, if A is a subring of F), then the intersection of all the subfields of F containing A is a subfield of F and is called the subfield *generated* by A. This subfield is the smallest subfield of F containing A (namely, any subfield of F containing A contains the subfield generated by A).

The next corollary shows that the smallest field containing an integral domain R is its field of fractions.

Corollary 16. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R then the subfield of F generated by R' is isomorphic to Q.

Proof: Let $\varphi : R \cong R' \subseteq F$ be a (ring) isomorphism of R to R'. In particular, $\varphi : R \to F$ is an injective homomorphism from R into the field F. Let $\Phi : Q \to F$ be the extension of φ to Q as in the theorem. By Theorem 15, Φ is injective, so $\Phi(Q)$ is an isomorphic copy of Q in F containing $\varphi(R) = R'$. Now, any subfield of F containing $R' = \varphi(R)$ contains the elements $\varphi(r_1)\varphi(r_2)^{-1} = \varphi(r_1 r_2^{-1})$ for all $r_1, r_2 \in R$. Since

every element of Q is of the form $r_1 r_2^{-1}$ for some $r_1, r_2 \in R$, it follows that any subfield of F containing R' contains the field $\Phi(Q)$, so that $\Phi(Q)$ is the subfield of F generated by R', proving the corollary.

Examples

(1) If R is a field then its field of fractions is just R itself.

(2) The integers $\mathbb{Z}$ are an integral domain whose field of fractions is the field $\mathbb{Q}$ of rational numbers. The quadratic integer ring $\mathcal{O}$ of Section 1 is an integral domain whose field of fractions is the quadratic field $\mathbb{Q}(\sqrt{D})$.

(3) The subring $2\mathbb{Z}$ of $\mathbb{Z}$ also has no zero divisors (but has no identity). Its field of fractions is also $\mathbb{Q}$. Note how an identity "appears" in the field of fractions.

(4) If R is any integral domain, then the polynomial ring $R[x]$ is also an integral domain. The associated field of fractions is the field of *rational functions* in the variable x over R. The elements of this field are of the form $\dfrac{p(x)}{q(x)}$, where $p(x)$ and $q(x)$ are polynomials with coefficients in R with $q(x)$ not the zero polynomial. In particular, $p(x)$ and $q(x)$ may both be constant polynomials, so the field of rational functions contains the field of fractions of R: elements of the form $\dfrac{a}{b}$ such that $a, b \in R$ and $b \neq 0$. If F is a field, we shall denote the field of rational functions by $F(x)$. Thus if F is the field of fractions of the integral domain R then the field of rational functions over R is the same as the field of rational functions over F, namely $F(x)$.

For example, suppose $R = \mathbb{Z}$, so $F = \mathbb{Q}$. If $p(x), q(x)$ are polynomials in $\mathbb{Q}[x]$ then for some integer N, $Np(x), Nq(x)$ have integer coefficients (let N be a common denominator for all the coefficients in $p(x)$ and $q(x)$, for example). Then $\dfrac{p(x)}{q(x)} = \dfrac{Np(x)}{Nq(x)}$ can be written as the quotient of two polynomials with integer coefficients, so the field of fractions of $\mathbb{Q}[x]$ is the same as the field of fractions of $\mathbb{Z}[x]$.

(5) If R is any commutative ring with identity and d is neither zero nor a zero divisor in R we may form the ring $R[1/d]$ by setting $D = \{1, d, d^2, d^3, \dots\}$ and defining $R[1/d]$ to be the ring of fractions $D^{-1}R$. Note that R is the subring of elements of the form $\dfrac{r}{1}$. In this way any nonzero element of R that is not a zero divisor can be inverted in a larger ring containing R. Note that the elements of $R[1/d]$ look like polynomials in $1/d$ with coefficients in R, which explains the notation.

EXERCISES

Let R be a commutative ring with identity $1 \neq 0$.

1. Fill in all the details in the proof of Theorem 15.

2. Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R (hence is also an integral domain).

3. Let F be a field. Prove that F contains a unique smallest subfield F_0 and that F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p (F_0 is called the *prime subfield* of F). [See Exercise 26, Section 3.]

4. Prove that any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

5. If F is a field, prove that the field of fractions of $F[[x]]$ (the ring of formal power series in the indeterminate x with coefficients in F) is the ring $F((x))$ of formal Laurent series (cf. Exercises 3 and 5 of Section 2). Show the field of fractions of the power series ring $\mathbb{Z}[[x]]$ is *properly* contained in the field of Laurent series $\mathbb{Q}((x))$. [Consider the series for e^x.]
6. Prove that the real numbers, $\mathbb{R}$, contain a subring A with $1 \in A$ and A maximal (under inclusion) with respect to the property that $\frac{1}{2} \notin A$. [Use Zorn's Lemma.] (Exercise 13 in Section 15.3 shows $\mathbb{R}$ is the quotient field of A, so $\mathbb{R}$ is the quotient field of a proper subring.)

7.6 THE CHINESE REMAINDER THEOREM

Throughout this section we shall assume unless otherwise stated that all rings are commutative with an identity $1 \neq 0$.

Given an arbitrary collection of rings (not necessarily satisfying the conventions above), their *(ring) direct product* is defined to be their direct product as (abelian) groups made into a ring by defining multiplication componentwise. In particular, if R_1 and R_2 are two rings, we shall denote by $R_1 \times R_2$ their direct product (as rings), that is, the set of ordered pairs (r_1, r_2) with $r_1 \in R_1$ and $r_2 \in R_2$ where addition and multiplication are performed componentwise:

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \qquad \text{and} \qquad (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2).$$

We note that a map φ from a ring R into a direct product ring is a homomorphism if and only if the induced maps into each of the components are homomorphisms.

There is a generalization to arbitrary rings of the notion in $\mathbb{Z}$ of two integers n and m being relatively prime (even to rings where the notion of greatest common divisor is not defined). In $\mathbb{Z}$ this is equivalent to being able to solve the equation $nx + my = 1$ in integers x and y (this fact was stated in Chapter 0 and will be proved in Chapter 8). This in turn is equivalent to $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ as ideals (in general, $n\mathbb{Z} + m\mathbb{Z} = (m, n)\mathbb{Z}$). This motivates the following definition:

Definition. The ideals A and B of the ring R are said to be *comaximal* if $A + B = R$.

Recall that the *product*, AB, of the ideals A and B of R is the ideal consisting of all finite sums of elements of the form xy, $x \in A$ and $y \in B$ (cf. Exercise 34, Section 3). If $A = (a)$ and $B = (b)$, then $AB = (ab)$. More generally, the product of the ideals $A_1, A_2, \ldots, A_k$ is the ideal of all finite sums of elements of the form $x_1 x_2 \cdots x_k$ such that $x_i \in A_i$ for all i. If $A_i = (a_i)$, then $A_1 \cdots A_k = (a_1 \cdots a_k)$.

Theorem 17. *(Chinese Remainder Theorem)* Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \qquad \text{defined by} \qquad r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Proof: We first prove this for $k = 2$; the general case will follow by induction. Let $A = A_1$ and $B = A_2$. Consider the map $\varphi : R \to R/A \times R/B$ defined by $\varphi(r) = (r \bmod A, r \bmod B)$, where mod A means the class in R/A containing r (that is, $r + A$). This map is a ring homomorphism because φ is just the natural projection of R into R/A and R/B for the two components. The kernel of φ consists of all the elements $r \in R$ that are in A and in B, i.e., $A \cap B$. To complete the proof in this case it remains to show that when A and B are comaximal, φ is surjective and $A \cap B = AB$. Since $A + B = R$, there are elements $x \in A$ and $y \in B$ such that $x + y = 1$. This equation shows that $\varphi(x) = (0, 1)$ and $\varphi(y) = (1, 0)$ since, for example, x is an element of A and $x = 1 - y \in 1 + B$. If now $(r_1 \bmod A, r_2 \bmod B)$ is an arbitrary element in $R/A \times R/B$, then the element $r_2x + r_1y$ maps to this element since

$$\begin{aligned}\varphi(r_2x + r_1y) &= \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y)\\ &= (r_2 \bmod A, r_2 \bmod B)(0, 1) + (r_1 \bmod A, r_1 \bmod B)(1, 0)\\ &= (0, r_2 \bmod B) + (r_1 \bmod A, 0)\\ &= (r_1 \bmod A, r_2 \bmod B).\end{aligned}$$

This shows that φ is indeed surjective. Finally, the ideal AB is always contained in $A \cap B$. If A and B are comaximal and x and y are as above, then for any $c \in A \cap B$, $c = c1 = cx + cy \in AB$. This establishes the reverse inclusion $A \cap B \subseteq AB$ and completes the proof when $k = 2$.

The general case follows easily by induction from the case of two ideals using $A = A_1$ and $B = A_2 \cdots A_k$ once we show that A_1 and $A_2 \cdots A_k$ are comaximal. By hypothesis, for each $i \in \{2, 3, \ldots, k\}$ there are elements $x_i \in A_1$ and $y_i \in A_i$ such that $x_i + y_i = 1$. Since $x_i + y_i \equiv y_i \bmod A_1$, it follows that $1 = (x_2 + y_2) \cdots (x_k + y_k)$ is an element in $A_1 + (A_2 \cdots A_k)$. This completes the proof.

This theorem obtained its name from the special case $\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ *as rings* when m and n are relatively prime integers. We proved this isomorphism just for the additive groups earlier. This isomorphism, phrased in number-theoretic terms, relates to simultaneously solving two congruences modulo relatively prime integers (and states that such congruences can always be solved, and uniquely). Such problems were considered by the ancient Chinese, hence the name. Some examples are provided in the exercises.

Since the isomorphism in the Chinese Remainder Theorem is an isomorphism of *rings*, in particular the groups of *units* on both sides must be isomorphic. It is easy to see that the units in any direct product of rings are the elements that have units in each of the coordinates. In the case of $\mathbb{Z}/mn\mathbb{Z}$ the Chinese Remainder Theorem gives the following isomorphism on the groups of units:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

More generally we have the following result.

Corollary 18. Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}),$$

as rings, so in particular we have the following isomorphism of multiplicative groups:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$

If we compare orders on the two sides of this last isomorphism, we obtain the formula

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k})$$

for the Euler φ-function. This in turn implies that φ is what in elementary number theory is termed a *multiplicative function*, namely that $\varphi(ab) = \varphi(a)\varphi(b)$ whenever a and b are relatively prime positive integers. The value of φ on prime powers p^α is easily seen to be $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ (cf. Chapter 0). From this and the multiplicativity of φ we obtain its value on all positive integers.

Corollary 18 is also a step toward a determination of the decomposition of the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$ into a direct product of cyclic groups. The complete structure is derived at the end of Section 9.5.

EXERCISES

Let R be a ring with identity $1 \neq 0$.

1. An element $e \in R$ is called an *idempotent* if $e^2 = e$. Assume e is an idempotent in R and $er = re$ for all $r \in R$. Prove that Re and $R(1-e)$ are two-sided ideals of R and that $R \cong Re \times R(1-e)$. Show that e and $1-e$ are identities for the subrings Re and $R(1-e)$ respectively.
2. Let R be a finite Boolean ring with identity $1 \neq 0$ (cf. Exercise 15 of Section 1). Prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$. [Use the preceding exercise.]
3. Let R and S be rings with identities. Prove that every ideal of $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S.
4. Prove that if R and S are nonzero rings then $R \times S$ is never a field.
5. Let $n_1, n_2, \dots, n_k$ be integers which are relatively prime in pairs: $(n_i, n_j) = 1$ for all $i \neq j$.
   (a) Show that the Chinese Remainder Theorem implies that for any $a_1, \dots, a_k \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the simultaneous congruences
   $$x \equiv a_1 \bmod n_1\,, \qquad x \equiv a_2 \bmod n_2\,, \quad \dots, \quad x \equiv a_k \bmod n_k$$
   and that the solution x is unique mod $n = n_1 n_2 \dots n_k$.
   (b) Let $n_i' = n/n_i$ be the quotient of n by n_i, which is relatively prime to n_i by assumption. Let t_i be the inverse of n_i' mod n_i. Prove that the solution x in (a) is given by
   $$x = a_1 t_1 n_1' + a_2 t_2 n_2' + \cdots + a_k t_k n_k' \bmod n.$$
   Note that the elements t_i can be quickly found by the Euclidean Algorithm as described in Section 2 of the Preliminaries chapter (writing $an_i + bn_i' = (n_i, n_i') = 1$ gives $t_i = b$) and that these then quickly give the solutions to the system of congruences above for any choice of $a_1, a_2, \dots, a_k$.

(c) Solve the simultaneous system of congruences

$$x \equiv 1 \bmod 8\,, \qquad x \equiv 2 \bmod 25\,, \quad \text{and} \quad x \equiv 3 \bmod 81$$

and the simultaneous system

$$y \equiv 5 \bmod 8\,, \qquad y \equiv 12 \bmod 25\,, \quad \text{and} \quad y \equiv 47 \bmod 81.$$

6. Let $f_1(x), f_2(x), \ldots, f_k(x)$ be polynomials with integer coefficients of the same degree d. Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs (i.e., $(n_i, n_j) = 1$ for all $i \neq j$). Use the Chinese Remainder Theorem to prove there exists a polynomial $f(x)$ with integer coefficients and of degree d with

$$f(x) \equiv f_1(x) \bmod n_1\,, \qquad f(x) \equiv f_2(x) \bmod n_2\,, \quad \ldots, \quad f(x) \equiv f_k(x) \bmod n_k$$

i.e., the coefficients of $f(x)$ agree with the coefficients of $f_i(x) \bmod n_i$. Show that if all the $f_i(x)$ are monic, then $f(x)$ may also be chosen monic. [Apply the Chinese Remainder Theorem in $\mathbb{Z}$ to each of the coefficients separately.]

7. Let m and n be positive integers with n dividing m. Prove that the natural surjective ring projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is also surjective on the units: $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$.

The next four exercises develop the concept of *direct limits* and the "dual" notion of *inverse limits*. In these exercises I is a nonempty index set with a partial order $\leq$ (cf. Appendix I). For each $i \in I$ let A_i be an additive abelian group. In Exercise 8 assume also that I is a *directed set*: for every $i, j \in I$ there is some $k \in I$ with $i \leq k$ and $j \leq k$.

8. Suppose for every pair of indices i, j with $i \leq j$ there is a map $\rho_{ij} : A_i \to A_j$ such that the following hold:

i. $\rho_{jk} \circ \rho_{ij} = \rho_{ik}$ whenever $i \leq j \leq k$, and
ii. $\rho_{ii} = 1$ for all $i \in I$.

Let B be the disjoint union of all the A_i. Define a relation $\sim$ on B by

$$a \sim b \text{ if and only if there exists } k \text{ with } i, j \leq k \text{ and } \rho_{ik}(a) = \rho_{jk}(b),$$

for $a \in A_i$ and $b \in A_j$.

(a) Show that $\sim$ is an equivalence relation on B. (The set of equivalence classes is called the *direct* or *inductive limit* of the directed system $\{A_i\}$, and is denoted $\varinjlim A_i$. In the remaining parts of this exercise let $A = \varinjlim A_i$.)

(b) Let $\overline{x}$ denote the class of x in A and define $\rho_i : A_i \to A$ by $\rho_i(a) = \overline{a}$. Show that if each ρ_{ij} is injective, then so is ρ_i for all i (so we may then identify each A_i as a subset of A).

(c) Assume all ρ_{ij} are group homomorphisms. For $a \in A_i, b \in A_j$ show that the operation

$$\overline{a} + \overline{b} = \overline{\rho_{ik}(a) + \rho_{jk}(b)}$$

where k is any index with $i, j \leq k$, is well defined and makes A into an abelian group. Deduce that the maps ρ_i in (b) are group homomorphisms from A_i to A.

(d) Show that if all A_i are commutative rings with 1 and all ρ_{ij} are ring homomorphisms that send 1 to 1, then A may likewise be given the structure of a commutative ring with 1 such that all ρ_i are ring homomorphisms.

(e) Under the hypotheses in (c) prove that the direct limit has the following *universal property*: if C is any abelian group such that for each $i \in I$ there is a homomorphism $\varphi_i : A_i \to C$ with $\varphi_i = \varphi_j \circ \rho_{ij}$ whenever $i \leq j$, then there is a unique homomorphism $\varphi : A \to C$ such that $\varphi \circ \rho_i = \varphi_i$ for all i.

9. Let I be the collection of open intervals $U = (a, b)$ on the real line containing a fixed real number p. Order these by reverse inclusion: $U \leq V$ if $V \subseteq U$ (note that I is a directed set). For each U let A_U be the ring of continuous real valued functions on U. For $V \subseteq U$ define the *restriction maps* $\rho_{UV} : A_U \to A_V$ by $f \mapsto f|_V$, the usual restriction of a function on U to a function on the subset V (which is easily seen to be a ring homomorphism). Let $A = \varinjlim A_U$ be the direct limit. In the notation of the preceding exercise, show that the maps $\rho_U : A_U \to A$ are *not* injective but are all surjective (A is called the ring of *germs of continuous functions* at p).

We now develop the notion of *inverse limits*. Continue to assume I is a partially ordered set (but not necessarily directed), and A_i is a group for all $i \in I$.

10. Suppose for every pair of indices i, j with $i \leq j$ there is a map $\mu_{ji} : A_j \to A_i$ such that the following hold:

i. $\mu_{ji} \circ \mu_{kj} = \mu_{ki}$ whenever $i \leq j \leq k$, and
ii. $\mu_{ii} = 1$ for all $i \in I$.

Let P be the subset of elements $(a_i)_{i \in I}$ in the direct product $\prod_{i \in I} A_i$ such that $\mu_{ji}(a_j) = a_i$ whenever $i \leq j$ (here a_i and a_j are the i^{th} and j^{th} components respectively of the element in the direct product). The set P is called the *inverse* or *projective limit* of the system $\{A_i\}$, and is denoted $\varprojlim A_i$.)

(a) Assume all μ_{ji} are group homomorphisms. Show that P is a subgroup of the direct product group (cf. Exercise 15, Section 5.1).
(b) Assume the hypotheses in (a), and let $I = \mathbb{Z}^+$ (usual ordering). For each $i \in I$ let $\mu_i : P \to A_i$ be the projection of P onto its i^{th} component. Show that if each μ_{ji} is surjective, then so is μ_i for all i (so each A_i is a quotient group of P).
(c) Show that if all A_i are commutative rings with 1 and all μ_{ji} are ring homomorphisms that send 1 to 1, then A may likewise be given the structure of a commutative ring with 1 such that all μ_i are ring homomorphisms.
(d) Under the hypotheses in (a) prove that the inverse limit has the following *universal property*: if D is any group such that for each $i \in I$ there is a homomorphism $\pi_i : D \to A_i$ with $\pi_i = \mu_{ji} \circ \pi_j$ whenever $i \leq j$, then there is a unique homomorphism $\pi : D \to P$ such that $\mu_i \circ \pi = \pi_i$ for all i.

11. Let p be a prime let $I = \mathbb{Z}^+$, let $A_i = \mathbb{Z}/p^i\mathbb{Z}$ and let μ_{ji} be the natural projection maps

$$\mu_{ji} : a \pmod{p^j} \longmapsto a \pmod{p^i}.$$

The inverse limit $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ is called the ring of *p-adic integers*, and is denoted by $\mathbb{Z}_p$.

(a) Show that every element of $\mathbb{Z}_p$ may be written uniquely as an infinite formal sum $b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$ with each $b_i \in \{0, 1, \ldots, p-1\}$. Describe the rules for adding and multiplying such formal sums corresponding to addition and multiplication in the ring $\mathbb{Z}_p$. [Write a least residue in each $\mathbb{Z}/p^i\mathbb{Z}$ in its base p expansion and then describe the maps μ_{ji}.] (Note in particular that $\mathbb{Z}_p$ is uncountable.)
(b) Prove that $\mathbb{Z}_p$ is an integral domain that contains a copy of the integers.
(c) Prove that $b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$ as in (a) is a unit in $\mathbb{Z}_p$ if and only if $b_0 \neq 0$.
(d) Prove that $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$ and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ (where $p = 0 + 1p + 0p^2 + 0p^3 + \cdots$). Prove that every ideal of $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$ for some integer $n \geq 0$.
(e) Show that if $a_1 \not\equiv 0 \pmod{p}$ then there is an element $a = (a_i)$ in the direct limit $\mathbb{Z}_p$ satisfying $a_j^p \equiv 1 \pmod{p^j}$ and $\mu_{j1}(a_j) = a_1$ for all j. Deduce that $\mathbb{Z}_p$ contains $p - 1$ distinct $(p-1)^{\text{st}}$ roots of 1.

CHAPTER 8

Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

There are a number of classes of rings with more algebraic structure than generic rings. Those considered in this chapter are rings with a division algorithm (Euclidean Domains), rings in which every ideal is principal (Principal Ideal Domains) and rings in which elements have factorizations into primes (Unique Factorization Domains). The principal examples of such rings are the ring $\mathbb{Z}$ of integers and polynomial rings $F[x]$ with coefficients in some field F. We prove here all the theorems on the integers $\mathbb{Z}$ stated in the Preliminaries chapter as special cases of results valid for more general rings. These results will be applied to the special case of the ring $F[x]$ in the next chapter.

All rings in this chapter are commutative.

8.1 EUCLIDEAN DOMAINS

We first define the notion of a *norm* on an integral domain R. This is essentially no more than a measure of "size" in R.

Definition. Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a *norm* on the integral domain R. If $N(a) > 0$ for $a \neq 0$ define N to be a *positive norm.*

We observe that this notion of a norm is fairly weak and that it is possible for the same integral domain R to possess several different norms.

Definition. The integral domain R is said to be a *Euclidean Domain* (or possess a *Division Algorithm*) if there is a norm N on R such that for any two elements a and b of R with $b \neq 0$ there exist elements q and r in R with

$$a = qb + r \qquad \text{with } r = 0 \text{ or } N(r) < N(b).$$

The element q is called the *quotient* and the element r the *remainder* of the division.

The importance of the existence of a Division Algorithm on an integral domain R is that it allows a *Euclidean Algorithm* for two elements a and b of R: by successive "divisions" (these actually *are* divisions in the field of fractions of R) we can write

$$a = q_0 b + r_0 \tag{0}$$

$$b = q_1 r_0 + r_1 \tag{1}$$

$$r_0 = q_2 r_1 + r_2 \tag{2}$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \tag{n}$$

$$r_{n-1} = q_{n+1} r_n \tag{n+1}$$

where r_n is the last nonzero remainder. Such an r_n exists since $N(b) > N(r_0) > N(r_1) > \cdots > N(r_n)$ is a decreasing sequence of nonnegative integers if the remainders are nonzero, and such a sequence cannot continue indefinitely. Note also that there is no guarantee that these elements are *unique*.

Examples

(0) Fields are trivial examples of Euclidean Domains where any norm will satisfy the defining condition (e.g., $N(a) = 0$ for all a). This is because for every a, b with $b \neq 0$ we have $a = qb + 0$, where $q = ab^{-1}$.

(1) The integers $\mathbb{Z}$ are a Euclidean Domain with norm given by $N(a) = |a|$, the usual absolute value. The existence of a Division Algorithm in $\mathbb{Z}$ (the familiar "long division" of elementary arithmetic) is verified as follows. Let a and b be two nonzero integers and suppose first that $b > 0$. The half open intervals $[nb, (n+1)b)$, $n \in \mathbb{Z}$ partition the real line and so a is in one of them, say $a \in [kb, (k+1)b)$. For $q = k$ we have $a - qb = r \in [0, |b|)$ as needed. If $b < 0$ (so $-b > 0$), by what we have just seen there is an integer q such that $a = q(-b) + r$ with either $r = 0$ or $|r| < |-b|$; then $a = (-q)b + r$ satisfies the requirements of the Division Algorithm for a and b. This argument can be made more formal by using induction on $|a|$.

Note that if a is not a multiple of b there are always two possibilities for the pair q, r: the proof above always produced a positive remainder r. If for example $b > 0$ and q, r are as above with $r > 0$, then $a = q'b + r'$ with $q' = q + 1$ and $r' = r - b$ also satisfy the conditions of the Division Algorithm applied to a, b. Thus $5 = 2 \cdot 2 + 1 = 3 \cdot 2 - 1$ are the two ways of applying the Division Algorithm in $\mathbb{Z}$ to $a = 5$ and $b = 2$. The quotient and remainder are unique if we require the remainder to be nonnegative.

(2) If F is a field, then the polynomial ring $F[x]$ is a Euclidean Domain with norm given by $N(p(x)) =$ the degree of $p(x)$. The Division Algorithm for polynomials is simply "long division" of polynomials which may be familiar for polynomials with real coefficients. The proof is very similar to that for $\mathbb{Z}$ and is given in the next chapter (although for polynomials the quotient and remainder are shown to be unique). In order for a polynomial ring to be a Euclidean Domain the coefficients must come from a field since the division algorithm ultimately rests on being able to divide arbitrary nonzero coefficients. We shall prove in Section 2 that $R[x]$ is not a Euclidean Domain if R is not a field.

(3) The quadratic integer rings $\mathcal{O}$ in Section 7.1 are integral domains with a norm defined by the absolute value of the field norm (to ensure the values taken are nonnegative;

when $D < 0$ the field norm is itself a norm), but in general $\mathcal{O}$ is not Euclidean with respect to this norm (or any other norm). The Gaussian integers $\mathbb{Z}[i]$ (where $D = -1$), however, are a Euclidean Domain with respect to the norm $N(a + bi) = a^2 + b^2$, as we now show (cf. also the end of Section 3).

Let $\alpha = a + bi$, $\beta = c + di$ be two elements of $\mathbb{Z}[i]$ with $\beta \neq 0$. Then in the field $\mathbb{Q}(i)$ we have $\dfrac{\alpha}{\beta} = r + si$ where $r = (ac + bd)/(c^2 + d^2)$ and $s = (bc - ad)/(c^2 + d^2)$ are rational numbers. Let p be an integer closest to the rational number r and let q be an integer closest to the rational number s, so that both $|r - p|$ and $|s - q|$ are at most $1/2$. The Division Algorithm follows immediately once we show

$$\alpha = (p + qi)\beta + \gamma \qquad \text{for some } \gamma \in \mathbb{Z}[i] \text{ with } \quad N(\gamma) \leq \frac{1}{2}N(\beta)$$

which is even stronger than necessary. Let $\theta = (r - p) + (s - q)i$ and set $\gamma = \beta\theta$. Then $\gamma = \alpha - (p + qi)\beta$, so that $\gamma \in \mathbb{Z}[i]$ is a Gaussian integer and $\alpha = (p + qi)\beta + \gamma$. Since $N(\theta) = (r - p)^2 + (s - q)^2$ is at most $1/4 + 1/4 = 1/2$, the multiplicativity of the norm N implies that $N(\gamma) = N(\theta)N(\beta) \leq \dfrac{1}{2}N(\beta)$ as claimed.

Note that the algorithm is quite explicit since a quotient $p + qi$ is quickly determined from the rational numbers r and s, and then the remainder $\gamma = \alpha - (p + qi)\beta$ is easily computed. Note also that the quotient need not be unique: if r (or s) is half of an odd integer then there are two choices for p (or for q, respectively).

This proof that $\mathbb{Z}[i]$ is a Euclidean Domain can also be used to show that $\mathcal{O}$ is a Euclidean Domain (with respect to the field norm defined in Section 7.1) for $D = -2, -3, -7, -11$ (cf. the exercises). We shall see shortly that $\mathbb{Z}[\sqrt{-5}]$ is not Euclidean with respect to any norm, and a proof that $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is not a Euclidean Domain with respect to any norm appears at the end of this section.

(4) Recall (cf. Exercise 26 in Section 7.1) that a *discrete valuation ring* is obtained as follows. Let K be a field. A *discrete valuation* on K is a function $v : K^\times \to \mathbb{Z}$ satisfying

(i) $v(ab) = v(a) + v(b)$ (i.e., v is a homomorphism from the multiplicative group of nonzero elements of K to $\mathbb{Z}$),

(ii) v is surjective, and

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

The set $\{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$ is a subring of K called the valuation ring of v. An integral domain R is called a discrete valuation ring if there is a valuation v on its field of fractions such that R is the valuation ring of v.

For example the ring R of all rational numbers whose denominators are relatively prime to the fixed prime $p \in \mathbb{Z}$ is a discrete valuation ring contained in $\mathbb{Q}$.

A discrete valuation ring is easily seen to be a Euclidean Domain with respect to the norm defined by $N(0) = 0$ and $N = v$ on the nonzero elements of R. This is because for $a, b \in R$ with $b \neq 0$

(a) if $N(a) < N(b)$ then $a = 0 \cdot b + a$, and

(b) if $N(a) \geq N(b)$ then it follows from property (i) of a discrete valuation that $q = ab^{-1} \in R$, so $a = qb + 0$.

The first implication of a Division Algorithm for the integral domain R is that it forces every ideal of R to be *principal.*

Proposition 1. Every ideal in a Euclidean Domain is principal. More precisely, if I is any nonzero ideal in the Euclidean Domain R then $I = (d)$, where d is any nonzero element of I of minimum norm.

Proof: If I is the zero ideal, there is nothing to prove. Otherwise let d be any nonzero element of I of minimum norm (such a d exists since the set $\{N(a) \mid a \in I\}$ has a minimum element by the Well Ordering of $\mathbb{Z}$). Clearly $(d) \subseteq I$ since d is an element of I. To show the reverse inclusion let a be any element of I and use the Division Algorithm to write $a = qd + r$ with $r = 0$ or $N(r) < N(d)$. Then $r = a - qd$ and both a and qd are in I, so r is also an element of I. By the minimality of the norm of d, we see that r must be 0. Thus $a = qd \in (d)$ showing $I = (d)$.

Proposition 1 shows that every ideal of $\mathbb{Z}$ is principal. This fundamental property of $\mathbb{Z}$ was previously determined (in Section 7.3) from the (additive) group structure of $\mathbb{Z}$, using the classification of the subgroups of cyclic groups in Section 2.3. Note that these are really the same proof, since the results in Section 2.3 ultimately relied on the Euclidean Algorithm in $\mathbb{Z}$.

Proposition 1 can also be used to prove that some integral domains R are *not* Euclidean Domains (with respect to *any* norm) by proving the existence of ideals of R that are not principal.

Examples

(1) Let $R = \mathbb{Z}[x]$. Since the ideal $(2, x)$ is not principal (cf. Example 3 at the beginning of Section 7.4), it follows that the ring $\mathbb{Z}[x]$ of polynomials with *integer* coefficients is *not* a Euclidean Domain (for any choice of norm), even though the ring $\mathbb{Q}[x]$ of polynomials with *rational* coefficients is a Euclidean Domain.

(2) Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$, let N be the associated field norm $N(a+b\sqrt{-5}) = a^2+5b^2$ and consider the ideal $I = (3, 2+\sqrt{-5})$ generated by 3 and $2+\sqrt{-5}$. Suppose $I = (a+b\sqrt{-5})$, $a, b \in \mathbb{Z}$, were principal, i.e., $3 = \alpha(a+b\sqrt{-5})$ and $2+\sqrt{-5} = \beta(a+b\sqrt{-5})$ for some $\alpha, \beta \in R$. Taking norms in the first equation gives $9 = N(\alpha)(a^2+5b^2)$ and since a^2+5b^2 is a positive integer it must be 1,3 or 9. If the value is 9 then $N(\alpha) = 1$ and $\alpha = \pm 1$, so $a+b\sqrt{-5} = \pm 3$, which is impossible by the second equation since the coefficients of $2+\sqrt{-5}$ are not divisible by 3. The value cannot be 3 since there are no integer solutions to $a^2+5b^2 = 3$. If the value is 1, then $a+b\sqrt{-5} = \pm 1$ and the ideal I would be the entire ring R. But then 1 would be an element of I, so $3\gamma + (2+\sqrt{-5})\delta = 1$ for some $\gamma, \delta \in R$. Multiplying both sides by $2-\sqrt{-5}$ would then imply that $2-\sqrt{-5}$ is a multiple of 3 in R, a contradiction. It follows that I is not a principal ideal and so R is not a Euclidean Domain (with respect to any norm).

One of the fundamental consequences of the Euclidean Algorithm in $\mathbb{Z}$ is that it produces a greatest common divisor of two nonzero elements. This is true in any Euclidean Domain. The notion of a greatest common divisor of two elements (if it exists) can be made precise in general rings.

Definition. Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

(1) a is said to be a *multiple* of b if there exists an element $x \in R$ with $a = bx$. In this case b is said to *divide* a or be a *divisor* of a, written $b \mid a$.

(2) A *greatest common divisor* of a and b is a nonzero element d such that

(i) $d \mid a$ and $d \mid b$, and

(ii) if $d' \mid a$ and $d' \mid b$ then $d' \mid d$.

A greatest common divisor of a and b will be denoted by g.c.d.(a, b), or (abusing the notation) simply (a, b).

Note that $b \mid a$ in a ring R if and only if $a \in (b)$ if and only if $(a) \subseteq (b)$. In particular, if d is any divisor of both a and b then (d) must contain both a and b and hence must contain the ideal generated by a and b. The defining properties (i) and (ii) of a greatest common divisor of a and b translated into the language of ideals therefore become (respectively):

if I is the ideal of R generated by a and b, then d is a greatest common divisor of a and b if

(i) I is contained in the principal ideal (d), and

(ii) if (d') is any principal ideal containing I then $(d) \subseteq (d')$.

Thus a greatest common divisor of a and b (if such exists) is a generator for the unique smallest principal ideal containing a and b. There are rings in which greatest common divisors do not exist.

This discussion immediately gives the following *sufficient* condition for the existence of a greatest common divisor.

Proposition 2. If a and b are nonzero elements in the commutative ring R such that the ideal generated by a and b is a principal ideal (d), then d is a greatest common divisor of a and b.

This explains why the symbol (a, b) is often used to denote both the ideal generated by a and b and a greatest common divisor of a and b. An integral domain in which every ideal (a, b) generated by two elements is principal is called a *Bezout Domain*. The exercises in this and subsequent sections explore these rings and show that there are Bezout Domains containing nonprincipal (necessarily infinitely generated) ideals.

Note that the condition in Proposition 2 is *not* a *necessary* condition. For example, in the ring $R = \mathbb{Z}[x]$ the elements 2 and x generate a maximal, nonprincipal ideal (cf. the examples in Section 7.4). Thus $R = (1)$ is the unique principal ideal containing both 2 and x, so 1 is a greatest common divisor of 2 and x. We shall see other examples along these lines in Section 3.

Before returning to Euclidean Domains we examine the uniqueness of greatest common divisors.

Proposition 3. Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, i.e., $(d) = (d')$, then $d' = ud$ for some unit u in R. In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some unit u.

Proof: This is clear if either d or d' is zero so we may assume d and d' are nonzero. Since $d \in (d')$ there is some $x \in R$ such that $d = xd'$. Since $d' \in (d)$ there is some $y \in R$ such that $d' = yd$. Thus $d = xyd$ and so $d(1 - xy) = 0$. Since $d \neq 0$, $xy = 1$, that is, both x and y are units. This proves the first assertion. The second assertion follows from the first since any two greatest common divisors of a and b generate the same principal ideal (they divide each other).

One of the most important properties of Euclidean Domains is that greatest common divisors always exist and *can be computed algorithmically*.

Theorem 4. Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b described at the beginning of this chapter. Then

(1) d is a greatest common divisor of a and b, and

(2) the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an *R-linear combination* of a and b, i.e., there are elements x and y in R such that

$$d = ax + by.$$

Proof: By Proposition 1, the ideal generated by a and b is principal so a, b do have a greatest common divisor, namely any element which generates the (principal) ideal (a, b). Both parts of the theorem will follow therefore once we show $d = r_n$ generates this ideal, i.e., once we show that

(i) $d \mid a$ and $d \mid b$ (so $(a, b) \subseteq (d)$)

(ii) d is an R-linear combination of a and b (so $(d) \subseteq (a, b)$).

To prove that d divides both a and b simply keep track of the divisibilities in the Euclidean Algorithm. Starting from the $(n+1)^{\text{st}}$ equation, $r_{n-1} = q_{n+1}r_n$, we see that $r_n \mid r_{n-1}$. Clearly $r_n \mid r_n$. By induction (proceeding from index n downwards to index 0) assume r_n divides r_{k+1} and r_k. By the $(k+1)^{\text{st}}$ equation, $r_{k-1} = q_{k+1}r_k + r_{k+1}$, and since r_n divides both terms on the right hand side we see that r_n also divides r_{k-1}. From the 1^{st} equation in the Euclidean Algorithm we obtain that r_n divides b and then from the 0^{th} equation we get that r_n divides a. Thus (i) holds.

To prove that r_n is in the ideal (a, b) generated by a and b proceed similarly by induction proceeding from equation (0) to equation (n). It follows from equation (0) that $r_0 \in (a, b)$ and by equation (1) that $r_1 = b - q_1r_0 \in (b, r_0) \subseteq (a, b)$. By induction assume $r_{k-1}, r_k \in (a, b)$. Then by the $(k+1)^{\text{st}}$ equation

$$r_{k+1} = r_{k-1} - q_{k+1}r_k \in (r_{k-1}, r_k) \subseteq (a, b).$$

This induction shows $r_n \in (a, b)$, which completes the proof.

Much of the material above may be familiar from elementary arithmetic in the case of the integers $\mathbb{Z}$, except possibly for the translation into the language of ideals. For example, if $a = 2210$ and $b = 1131$ then the smallest ideal of $\mathbb{Z}$ that contains both a and b (the ideal generated by a and b) is $13\mathbb{Z}$, since 13 is the greatest common divisor of 2210 and 1131. This fact follows quickly from the Euclidean Algorithm:

$$2210 = 1 \cdot 1131 + 1079$$

$$1131 = 1 \cdot 1079 + 52$$
$$1079 = 20 \cdot 52 + 39$$
$$52 = 1 \cdot 39 + 13$$
$$39 = 3 \cdot 13$$

so that $13 = (2210, 1131)$ is the last nonzero remainder. Using the procedure of Theorem 4 we can also write 13 as a linear combination of 2210 and 1131 by first solving the next to last equation above for $13 = 52 - 1 \cdot 39$, then using previous equations to solve for 39 and 52, etc., finally writing 13 entirely in terms of 2210 and 1131. The answer in this case is

$$13 = (-22) \cdot 2210 + 43 \cdot 1131.$$

The Euclidean Algorithm in the integers $\mathbb{Z}$ is extremely fast. It is a theorem that the number of steps required to determine the greatest common divisor of two integers a and b is at worst 5 times the number of digits of the smaller of the two numbers. Put another way, this algorithm is *logarithmic* in the size of the integers. To obtain an appreciation of the speed implied here, notice that for the example above we would have expected at worst $5 \cdot 4 = 20$ divisions (the example required far fewer). If we had started with integers on the order of 10^{100} (large numbers by physical standards), we would have expected at worst only 500 divisions.

There is no uniqueness statement for the integers x and y in $(a, b) = ax + by$. Indeed, $x' = x + b$ and $y' = y - a$ satisfy $(a, b) = ax' + by'$. This is essentially the only possibility — one can prove that if x_0 and y_0 are solutions to the equation $ax + by = N$, then any other solutions x and y to this equation are of the form

$$x = x_0 + m\frac{b}{(a, b)}$$
$$y = y_0 - m\frac{a}{(a, b)}$$

for some integer m (positive or negative).

This latter theorem (a proof of which is outlined in the exercises) provides a complete solution of the *First Order Diophantine Equation* $ax + by = N$ provided we know there is *at least one* solution to this equation. But the equation $ax + by = N$ is simply another way of stating that N is an element of the ideal generated by a and b. Since we know this ideal is just (d), the principal ideal generated by the greatest common divisor d of a and b, this is the same as saying $N \in (d)$, i.e., N is divisible by d. Hence, *the equation* $ax + by = N$ *is solvable in integers* x *and* y *if and only if* N *is divisible by the g.c.d. of* a *and* b (and then the result quoted above gives a full set of solutions of this equation).

We end this section with another criterion that can sometimes be used to prove that a given integral domain is not a Euclidean Domain.[1] For any integral domain let

[1]The material here and in some of the following section follows the exposition by J.C. Wilson in *A principal ideal ring that is not a Euclidean ring*, Math. Mag., 46(1973), pp. 34–38, of ideas of Th. Motzkin, and use a simplification by Kenneth S. Williams in *Note on non-Euclidean Principal Ideal Domains*, Math. Mag., 48(1975), pp. 176–177.

$\widetilde{R} = R^\times \cup \{0\}$ denote the collection of units of R together with 0. An element $u \in R - \widetilde{R}$ is called a *universal side divisor* if for every $x \in R$ there is some $z \in \widetilde{R}$ such that u divides $x - z$ in R, i.e., there is a type of "division algorithm" for u: every x may be written $x = qu + z$ where z is either zero or a unit. The existence of universal side divisors is a weakening of the Euclidean condition:

Proposition 5. Let R be an integral domain that is not a field. If R is a Euclidean Domain then there are universal side divisors in R.

Proof: Suppose R is Euclidean with respect to some norm N and let u be an element of $R - \widetilde{R}$ (which is nonempty since R is not a field) of minimal norm. For any $x \in R$, write $x = qu + r$ where r is either 0 or $N(r) < N(u)$. In either case the minimality of u implies $r \in \widetilde{R}$. Hence u is a universal side divisor in R.

Example

We can use Proposition 5 to prove that the quadratic integer ring $R = \mathbb{Z}[(1 + \sqrt{-19})/2]$ is not a Euclidean Domain with respect to any norm by showing that R contains no universal side divisors (we shall see in the next section that all of the ideals in R are principal, so the technique in the examples following Proposition 1 do not apply to this ring). We have already determined that ± 1 are the only units in R and so $\widetilde{R} = \{0, \pm 1\}$. Suppose $u \in R$ is a universal side divisor and let $N(a + b(1 + \sqrt{-19})/2) = a^2 + ab + 5b^2$ denote the field norm on R as in Section 7.1. Note that if $a, b \in \mathbb{Z}$ and $b \neq 0$ then $a^2 + ab + 5b^2 = (a + b/2)^2 + 19/4b^2 \geq 5$ and so the smallest nonzero values of N on R are 1 (for the units ± 1) and 4 (for ± 2). Taking $x = 2$ in the definition of a universal side divisor it follows that u must divide one of $2 - 0$ or 2 ± 1 in R, i.e., u is a nonunit divisor of 2 or 3 in R. If $2 = \alpha\beta$ then $4 = N(\alpha)N(\beta)$ and by the remark above it follows that one of α or β has norm 1, i.e., equals ± 1. Hence the only divisors of 2 in R are $\{\pm 1, \pm 2\}$. Similarly, the only divisors of 3 in R are $\{\pm 1, \pm 3\}$, so the only possible values for u are ± 2 or ± 3. Taking $x = (1 + \sqrt{-19})/2$ it is easy to check that none of x, $x \pm 1$ are divisible by ± 2 or ± 3 in R, so none of these is a universal side divisor.

EXERCISES

1. For each of the following five pairs of integers a and b, determine their greatest common divisor d and write d as a linear combination $ax + by$ of a and b.
   - **(a)** $a = 20, b = 13$.
   - **(b)** $a = 69, b = 372$.
   - **(c)** $a = 11391, b = 5673$.
   - **(d)** $a = 507885, b = 60808$.
   - **(e)** $a = 91442056588823$, $b = 779086434385541$ (the Euclidean Algorithm requires only 7 steps for these integers).
2. For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the inverse of a mod n (cf. Section 3 of the Preliminaries chapter).
   - **(a)** $a = 13, n = 20$.
   - **(b)** $a = 69, n = 89$.
   - **(c)** $a = 1891, n = 3797$.

(d) $a = 6003722857$, $n = 77695236973$ (the Euclidean Algorithm requires only 3 steps for these integers).

3. Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.

4. Let R be a Euclidean Domain.

(a) Prove that if $(a, b) = 1$ and a divides bc, then a divides c. More generally, show that if a divides bc with nonzero a, b then $\frac{a}{(a, b)}$ divides c.

(b) Consider the Diophantine Equation $ax + by = N$ where a, b and N are integers and a, b are nonzero. Suppose x_0, y_0 is a solution: $ax_0 + by_0 = N$. Prove that the full set of solutions to this equation is given by

$$x = x_0 + m\frac{b}{(a, b)}, \qquad y = y_0 - m\frac{a}{(a, b)}$$

as m ranges over the integers. [If x, y is a solution to $ax + by = N$, show that $a(x - x_0) = b(y_0 - y)$ and use (a).]

5. Determine all integer solutions of the following equations:

(a) $2x + 4y = 5$

(b) $17x + 29y = 31$

(c) $85x + 145y = 505$.

6. (*The Postage Stamp Problem*) Let a and b be two relatively prime positive integers. Prove that every sufficiently large positive integer N can be written as a linear combination $ax + by$ of a and b where x and y are both *nonnegative*, i.e., there is an integer N_0 such that for all $N \geq N_0$ the equation $ax + by = N$ can be solved with both x and y nonnegative integers. Prove in fact that the integer $ab - a - b$ cannot be written as a positive linear combination of a and b but that every integer greater than $ab - a - b$ is a positive linear combination of a and b (so every "postage" greater than $ab - a - b$ can be obtained using only stamps in denominations a and b).

7. Find a generator for the ideal $(85, 1+13i)$ in $\mathbb{Z}[i]$, i.e., a greatest common divisor for 85 and $1+13i$, by the Euclidean Algorithm. Do the same for the ideal $(47 - 13i, 53 + 56i)$.

It is known (but not so easy to prove) that $D = -1, -2, -3, -7, -11, -19, -43, -67$, and -163 are the only negative values of D for which every ideal in $\mathcal{O}$ is principal (i.e., $\mathcal{O}$ is a P.I.D. in the terminology of the next section). The results of the next exercise determine precisely which quadratic integer rings with $D < 0$ are Euclidean.

8. Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field with associated quadratic integer ring $\mathcal{O}$ and field norm N as in Section 7.1.

(a) Suppose D is $-1, -2, -3, -7$ or -11. Prove that $\mathcal{O}$ is a Euclidean Domain with respect to N. [Modify the proof for $\mathbb{Z}[i]$ ($D = -1$) in the text. For $D = -3, -7, -11$ prove that every element of F differs from an element in $\mathcal{O}$ by an element whose norm is at most $(1 + |D|)^2/(16|D|)$, which is less than 1 for these values of D. Plotting the points of $\mathcal{O}$ in $\mathbb{C}$ may be helpful.]

(b) Suppose that $D = -43, -67$, or -163. Prove that $\mathcal{O}$ is not a Euclidean Domain with respect to any norm. [Apply the same proof as for $D = -19$ in the text.]

9. Prove that the ring of integers $\mathcal{O}$ in the quadratic integer ring $\mathbb{Q}(\sqrt{2})$ is a Euclidean Domain with respect to the norm given by the absolute value of the field norm N in Section 7.1.

10. Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$. [Use the fact

that $I = (\alpha)$ for some nonzero α and then use the Division Algorithm in this Euclidean Domain to see that every coset of I is represented by an element of norm less than $N(\alpha)$.]

11. Let R be a commutative ring with 1 and let a and b be nonzero elements of R. A *least common multiple* of a and b is an element e of R such that
(i) $a \mid e$ and $b \mid e$, and
(ii) if $a \mid e'$ and $b \mid e'$ then $e \mid e'$.

(a) Prove that a least common multiple of a and b (if such exists) is a generator for the unique largest principal ideal contained in $(a) \cap (b)$.

(b) Deduce that any two nonzero elements in a Euclidean Domain have a least common multiple which is unique up to multiplication by a unit.

(c) Prove that in a Euclidean Domain the least common multiple of a and b is $\dfrac{ab}{(a, b)}$, where (a, b) is the greatest common divisor of a and b.

12. (*A Public Key Code*) Let N be a positive integer. Let M be an integer relatively prime to N and let d be an integer relatively prime to $\varphi(N)$, where φ denotes Euler's φ-function. Prove that if $M_1 \equiv M^d \pmod{N}$ then $M \equiv M_1^{d'} \pmod{N}$ where d' is the inverse of d mod $\varphi(N)$: $dd' \equiv 1 \pmod{\varphi(N)}$.

Remark: This result is the basis for a standard *Public Key Code*. Suppose $N = pq$ is the product of two distinct large primes (each on the order of 100 digits, for example). If M is a message, then $M_1 \equiv M^d \pmod{N}$ is a scrambled (*encoded*) version of M, which can be unscrambled (*decoded*) by computing $M_1^{d'} \pmod{N}$ (these powers can be computed quite easily even for large values of M and N by successive squarings). The values of N and d (but not p and q) are made publicly known (hence the name) and then anyone with a message M can send their encoded message $M^d \pmod{N}$. To decode the message it seems necessary to determine d', which requires the determination of the value $\varphi(N) = \varphi(pq) = (p-1)(q-1)$ (no one has as yet *proved* that there is no other decoding scheme, however). The success of this method as a code rests on the necessity of determining the *factorization* of N into primes, for which no sufficiently efficient algorithm exists (for example, the most naive method of checking all factors up to $\sqrt{N}$ would here require on the order of 10^{100} computations, or approximately 300 years even at 10 billion computations per second, and of course one can always increase the size of p and q).

8.2 PRINCIPAL IDEAL DOMAINS (P.I.D.s)

Definition. A *Principal Ideal Domain* (P.I.D.) is an integral domain in which every ideal is principal.

Proposition 1 proved that *every Euclidean Domain is a Principal Ideal Domain* so that every result about Principal Ideal Domains automatically holds for Euclidean Domains.

Examples

(1) As mentioned after Proposition 1, the integers $\mathbb{Z}$ are a P.I.D. We saw in Section 7.4 that the polynomial ring $\mathbb{Z}[x]$ contains nonprincipal ideals, hence is not a P.I.D.

(2) Example 2 following Proposition 1 showed that the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is not a P.I.D., in fact the ideal $(3, 1+\sqrt{-5})$ is a nonprincipal ideal. It is possible

for the product IJ of two nonprincipal ideals I and J to be principal, for example the ideals $(3, 1+\sqrt{-5})$ and $(3, 1-\sqrt{-5})$ are both nonprincipal and their product is the principal ideal generated by 3, i.e., $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (3)$ (cf. Exercise 5 and the example preceding Proposition 12 below).

It is not true that every Principal Ideal Domain is a Euclidean Domain. We shall prove below that the quadratic integer ring $\mathbb{Z}[(1+\sqrt{-19})/2]$, which was shown not to be a Euclidean Domain in the previous section, nevertheless is a P.I.D.

From an ideal-theoretic point of view Principal Ideal Domains are a natural class of rings to study beyond rings which are fields (where the ideals are just the trivial ones: (0) and (1)). Many of the properties enjoyed by Euclidean Domains are also satisfied by Principal Ideal Domains. A significant advantage of Euclidean Domains over Principal Ideal Domains, however, is that although greatest common divisors exist in both settings, in Euclidean Domains one has an *algorithm* for computing them. Thus (as we shall see in Chapter 12 in particular) results which depend on the existence of greatest common divisors may often be proved in the larger class of Principal Ideal Domains although computation of examples (i.e., concrete applications of these results) are more effectively carried out using a Euclidean Algorithm (if one is available).

We collect some facts about greatest common divisors proved in the preceding section.

Proposition 6. Let R be a Principal Ideal Domain and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then

(1) d is a greatest common divisor of a and b

(2) d can be written as an *R-linear combination* of a and b, i.e., there are elements x and y in R with

$$d = ax + by$$

(3) d is unique up to multiplication by a unit of R.

Proof: This is just Propositions 2 and 3.

Recall that maximal ideals are always prime ideals but the converse is not true in general. We observed in Section 7.4, however, that every nonzero prime ideal of $\mathbb{Z}$ is a maximal ideal. This useful fact is true in an arbitrary Principal Ideal Domain, as the following proposition shows.

Proposition 7. Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Proof: Let (p) be a nonzero prime ideal in the Principal Ideal Domain R and let $I = (m)$ be any ideal containing (p). We must show that $I = (p)$ or $I = R$. Now $p \in (m)$ so $p = rm$ for some $r \in R$. Since (p) is a prime ideal and $rm \in (p)$, either r or m must lie in (p). If $m \in (p)$ then $(p) = (m) = I$. If, on the other hand, $r \in (p)$ write $r = ps$. In this case $p = rm = psm$, so $sm = 1$ (recall that R is an integral domain) and m is a unit so $I = R$.

As we have already mentioned, if F is a field, then the polynomial ring $F[x]$ is a Euclidean Domain, hence also a Principal Ideal Domain (this will be proved in the next chapter). The converse to this is also true. Intuitively, if I is an ideal in R (such as the ideal (2) in $\mathbb{Z}$) then the ideal (I, x) in $R[x]$ (such as the ideal $(2, x)$ in $\mathbb{Z}[x]$) requires one more generator than does I, hence in general is not principal.

Corollary 8. If R is any commutative ring such that the polynomial ring $R[x]$ is a Principal Ideal Domain (or a Euclidean Domain), then R is necessarily a field.

Proof: Assume $R[x]$ is a Principal Ideal Domain. Since R is a subring of $R[x]$ then R must be an integral domain (recall that $R[x]$ has an identity if and only if R does). The ideal (x) is a nonzero prime ideal in $R[x]$ because $R[x]/(x)$ is isomorphic to the integral domain R. By Proposition 7, (x) is a maximal ideal, hence the quotient R is a field by Proposition 12 in Section 7.4.

The last result in this section will be used to prove that not every P.I.D. is a Euclidean Domain and relates the principal ideal property with another weakening of the Euclidean condition.

Definition. Define N to be a *Dedekind–Hasse norm* if N is a positive norm and for every nonzero $a, b \in R$ either a is an element of the ideal (b) or there is a nonzero element in the ideal (a, b) of norm strictly smaller than the norm of b (i.e., either b divides a in R or there exist $s, t \in R$ with $0 < N(sa - tb) < N(b)$).

Note that R is Euclidean with respect to a positive norm N if it is always possible to satisfy the Dedekind–Hasse condition with $s = 1$, so this is indeed a weakening of the Euclidean condition.

Proposition 9. The integral domain R is a P.I.D. if and only if R has a Dedekind–Hasse norm.[2]

Proof: Let I be any nonzero ideal in R and let b be a nonzero element of I with $N(b)$ minimal. Suppose a is any nonzero element in I, so that the ideal (a, b) is contained in I. Then the Dedekind–Hasse condition on N and the minimality of b implies that $a \in (b)$, so $I = (b)$ is principal. The converse will be proved in the next section (Corollary 16).

---

[2]That a Dedekind–Hasse norm on R implies that R is a P.I.D. (and is equivalent when R is a ring of algebraic integers) is the classical *Criterion of Dedekind and Hasse*, cf. *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen*, Jour. für die Reine und Angew. Math., 159(1928), pp. 3–12. The observation that the converse holds generally is more recent and due to John Greene, *Principal Ideal Domains are almost Euclidean*, Amer. Math. Monthly, 104(1997), pp. 154–156.

Example

Let $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ be the quadratic integer ring considered at the end of the previous section. We show that the positive field norm $N(a + b(1 + \sqrt{-19})/2) = a^2 + ab + 5b^2$ defined on R is a Dedekind–Hasse norm, which by Proposition 9 and the results of the previous section will prove that R is a P.I.D. but not a Euclidean Domain.

Suppose α, β are nonzero elements of R and $\alpha/\beta \notin R$. We must show that there are elements $s, t \in R$ with $0 < N(s\alpha - t\beta) < N(\beta)$, which by the multiplicativity of the field norm is equivalent to

$$0 < N(\frac{\alpha}{\beta}s - t) < 1. \qquad (*)$$

Write $\frac{\alpha}{\beta} = \frac{a + b\sqrt{-19}}{c} \in \mathbb{Q}[\sqrt{-19}]$ with integers a, b, c having no common divisor and with $c > 1$ (since β is assumed not to divide α). Since a, b, c have no common divisor there are integers x, y, z with $ax + by + cz = 1$. Write $ay - 19bx = cq + r$ for some quotient q and remainder r with $|r| \leq c/2$ and let $s = y + x\sqrt{-19}$ and $t = q - z\sqrt{-19}$. Then a quick computation shows that

$$0 < N(\frac{\alpha}{\beta}s - t) = \frac{(ay - 19bx - cq)^2 + 19(ax + by + cz)^2}{c^2} \leq \frac{1}{4} + \frac{19}{c^2}$$

and so $(*)$ is satisfied with this s and t provided $c \geq 5$.

Suppose that $c = 2$. Then one of a, b is even and the other is odd (otherwise $\alpha/\beta \in R$), and then a quick check shows that $s = 1$ and $t = \frac{(a-1) + b\sqrt{-19}}{2}$ are elements of R satisfying $(*)$.

Suppose that $c = 3$. The integer $a^2 + 19b^2$ is not divisible by 3 (modulo 3 this is $a^2 + b^2$ which is easily seen to be 0 modulo 3 if and only if a and b are both 0 modulo 3; but then a, b, c have a common factor). Write $a^2 + 19b^2 = 3q + r$ with $r = 1$ or 2. Then again a quick check shows that $s = a - b\sqrt{-19}$, $t = q$ are elements of R satisfying $(*)$.

Finally, suppose that $c = 4$, so a and b are not both even. If one of a, b is even and the other odd, then $a^2 + 19b^2$ is odd, so we can write $a^2 + 19b^2 = 4q + r$ for some $q, r \in \mathbb{Z}$ and $0 < r < 4$. Then $s = a - b\sqrt{-19}$ and $t = q$ satisfy $(*)$. If a and b are both odd, then $a^2 + 19b^2 \equiv 1 + 3 \bmod 8$, so we can write $a^2 + 19b^2 = 8q + 4$ for some $q \in \mathbb{Z}$. Then $s = \frac{a - b\sqrt{-19}}{2}$ and $t = q$ are elements of R that satisfy $(*)$.

EXERCISES

1. Prove that in a Principal Ideal Domain two ideals (a) and (b) are comaximal (cf. Section 7.6) if and only if a greatest common divisor of a and b is 1 (in which case a and b are said to be *coprime* or *relatively prime*).
2. Prove that any two nonzero elements of a P.I.D. have a least common multiple (cf. Exercise 11, Section 1).
3. Prove that a quotient of a P.I.D. by a prime ideal is again a P.I.D.
4. Let R be an integral domain. Prove that if the following two conditions hold then R is a Principal Ideal Domain:
   (i) any two nonzero elements a and b in R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and

(ii) if $a_1, a_2, a_3, \ldots$ are nonzero elements of R such that $a_{i+1} \mid a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n \geq N$.

5. Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. Define the ideals $I_2 = (2, 1+\sqrt{-5})$, $I_3 = (3, 2+\sqrt{-5})$, and $I_3' = (3, 2-\sqrt{-5})$.
   (a) Prove that I_2, I_3, and I_3' are nonprincipal ideals in R. [Note that Example 2 following Proposition 1 proves this for I_3.]
   (b) Prove that the product of two nonprincipal ideals can be principal by showing that I_2^2 is the principal ideal generated by 2, i.e., $I_2^2 = (2)$.
   (c) Prove similarly that $I_2 I_3 = (1-\sqrt{-5})$ and $I_2 I_3' = (1+\sqrt{-5})$ areprincipal. Conclude that the principal ideal (6) is the product of 4 ideals: $(6) = I_2^2 I_3 I_3'$.

6. Let R be an integral domain and suppose that every *prime* ideal in R is principal. This exercise proves that every ideal of R is principal, i.e., R is a P.I.D.
   (a) Assume that the set of ideals of R that are not principal is nonempty and prove that this set has a maximal element under inclusion (which, by hypothesis, is not prime). [Use Zorn's Lemma.]
   (b) Let I be an ideal which is maximal with respect to being nonprincipal, and let $a, b \in R$ with $ab \in I$ but $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$ be the ideal generated by I and a, let $I_b = (I, b)$ be the ideal generated by I and b, and define $J = \{r \in R \mid rI_a \subseteq I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in R with $I \subsetneq I_b \subseteq J$ and $I_a J = (\alpha\beta) \subseteq I$.
   (c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_a J$ is principal, a contradiction, and conclude that R is a P.I.D.

7. An integral domain R in which every ideal generated by two elements is principal (i.e., for every $a, b \in R$, $(a, b) = (d)$ for some $d \in R$) is called a *Bezout Domain.* [cf. also Exercise 11 in Section 3.]
   (a) Prove that the integral domain R is a Bezout Domain if and only if every pair of elements a, b of R has a g.c.d. d in R that can be written as an R-linear combination of a and b, i.e., $d = ax + by$ for some $x, y \in R$.
   (b) Prove that every finitely generated ideal of a Bezout Domain is principal. [cf. the exercises in Sections 9.2 and 9.3 for Bezout Domains in which not every ideal is principal.]
   (c) Let F be the fraction field of the Bezout Domain R. Prove that every element of F can be written in the form a/b with $a, b \in R$ and a and b relatively prime (cf. Exercise 1).

8. Prove that if R is a Principal Ideal Domain and D is a multiplicatively closed subset of R, then $D^{-1}R$ is also a P.I.D. (cf. Section 7.5).

8.3 UNIQUE FACTORIZATION DOMAINS (U.F.D.s)

In the case of the integers $\mathbb{Z}$, there is another method for determining the greatest common divisor of two elements a and b familiar from elementary arithmetic, namely the notion of "factorization into primes" for a and b, from which the greatest common divisor can easily be determined. This can also be extended to a larger class of rings called Unique Factorization Domains (U.F.D.s) — these will be defined shortly. We shall then prove that

every Principal Ideal Domain is a Unique Factorization Domain

so that every result about Unique Factorization Domains will automatically hold for both Euclidean Domains and Principal Ideal Domains.

We first introduce some terminology.

Definition. Let R be an integral domain.

(1) Suppose $r \in R$ is nonzero and is not a unit. Then r is called *irreducible* in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise r is said to be *reducible*.

(2) The nonzero element $p \in R$ is called *prime* in R if the ideal (p) generated by p is a prime ideal. In other words, a nonzero element p is a prime if it is not a unit and whenever $p \mid ab$ for any $a, b \in R$, then either $p \mid a$ or $p \mid b$.

(3) Two elements a and b of R differing by a unit are said to be *associate* in R (i.e., $a = ub$ for some unit u in R).

Proposition 10. In an integral domain a prime element is always irreducible.

Proof: Suppose (p) is a nonzero prime ideal and $p = ab$. Then $ab = p \in (p)$, so by definition of prime ideal one of a or b, say a, is in (p). Thus $a = pr$ for some r. This implies $p = ab = prb$ so $rb = 1$ and b is a unit. This shows that p is irreducible.

It is not true in general that an irreducible element is necessarily prime. For example, consider the element 3 in the quadratic integer ring $R = \mathbb{Z}[\sqrt{-5}]$. The computations in Section 1 show that 3 is irreducible in R, but 3 is not a prime since $(2+\sqrt{-5})(2-\sqrt{-5}) = 3^2$ is divisible by 3, but neither $2+\sqrt{-5}$ nor $2-\sqrt{-5}$ is divisible by 3 in R.

If R is a Principal Ideal Domain however, the notions of prime and irreducible elements are the same. In particular these notions coincide in $\mathbb{Z}$ and in $F[x]$ (where F is a field).

Proposition 11. In a Principal Ideal Domain a nonzero element is a prime if and only if it is irreducible.

Proof: We have shown above that prime implies irreducible. We must show conversely that if p is irreducible, then p is a prime, i.e., the ideal (p) is a prime ideal. If M is any ideal containing (p) then by hypothesis $M = (m)$ is a principal ideal. Since $p \in (m)$, $p = rm$ for some r. But p is irreducible so by definition either r or m is a unit. This means either $(p) = (m)$ or $(m) = (1)$, respectively. Thus the only ideals containing (p) are (p) or (1), i.e., (p) is a maximal ideal. Since maximal ideals are prime ideals, the proof is complete.

Example

Proposition 11 gives another proof that the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is not a P.I.D. since 3 is irreducible but not prime in this ring.

The irreducible elements in the integers $\mathbb{Z}$ are the prime numbers (and their negatives) familiar from elementary arithmetic, and two integers a and b are associates of one another if and only if $a = \pm b$.

In the integers $\mathbb{Z}$ any integer n can be written as a product of primes (not necessarily distinct), as follows. If n is not itself a prime then by definition it is possible to write $n = n_1 n_2$ for two other integers n_1 and n_2 neither of which is a unit, i.e., neither of which is ± 1. Both n_1 and n_2 must be smaller in absolute value than n itself. If they are both primes, we have already written n as a product of primes. If one of n_1 or n_2 is not prime, then it in turn can be factored into two (smaller) integers. Since integers cannot decrease in absolute value indefinitely, we must at some point be left only with prime integer factors, and so we have written n as a product of primes.

For example, if $n = 2210$, the algorithm above proceeds as follows: n is not itself prime, since we can write $n = 2 \cdot 1105$. The integer 2 is a prime, but 1105 is not: $1105 = 5 \cdot 221$. The integer 5 is prime, but 221 is not: $221 = 13 \cdot 17$. Here the algorithm terminates, since both 13 and 17 are primes. This gives the *prime factorization* of 2210 : $2210 = 2 \cdot 5 \cdot 13 \cdot 17$. Similarly, we find $1131 = 3 \cdot 13 \cdot 29$. In these examples each prime occurs only to the first power, but of course this need not be the case generally.

In the ring $\mathbb{Z}$ not only is it true that every integer n can be written as a product of primes, but in fact this decomposition is *unique* in the sense that any two prime factorizations of the same positive integer n differ only in the order in which the positive prime factors are written. The restriction to positive integers is to avoid considering the factorizations (3)(5) and $(-3)(-5)$ of 15 as essentially distinct. This *unique factorization* property of $\mathbb{Z}$ (which we shall prove very shortly) is extremely useful for the arithmetic of the integers. General rings with the analogous property are given a name.

Definition. A *Unique Factorization Domain* (U.F.D.) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

- **(i)** r can be written as a finite product of irreducibles p_i of R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$ and
- **(ii)** the decomposition in (i) is *unique up to associates*: namely, if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i for $i = 1, 2, \ldots, n$.

Examples

- **(1)** A field F is trivially a Unique Factorization Domain since every nonzero element is a unit, so there are no elements for which properties (i) and (ii) must be verified.
- **(2)** As indicated above, we shall prove shortly that every Principal Ideal Domain is a Unique Factorization Domain (so, in particular, $\mathbb{Z}$ and $F[x]$ where F is a field are both Unique Factorization Domains).
- **(3)** We shall also prove in the next chapter that the ring $R[x]$ of polynomials is a Unique Factorization Domain whenever R itself is a Unique Factorization Domain (in contrast to the properties of being a Principal Ideal Domain or being a Euclidean Domain, which do not carry over from a ring R to the polynomial ring $R[x]$). This result together with the preceding example will show that $\mathbb{Z}[x]$ is a Unique Factorization Domain.
- **(4)** The subring of the Gaussian integers $R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$, where $i^2 = -1$, is an integral domain but not a Unique Factorization Domain (rings of this nature were introduced in Exercise 23 of Section 7.1). The elements 2 and $2i$ are

irreducibles which are not associates in R since $i \notin R$, and $4 = 2 \cdot 2 = (-2i) \cdot (2i)$ has two distinct factorizations in R. One may also check directly that $2i$ is irreducible but not prime in R (since $R/(2i) \cong \mathbb{Z}/4\mathbb{Z}$). In the larger ring of Gaussian integers, $\mathbb{Z}[i]$, (which is a Unique Factorization Domain) 2 and $2i$ *are* associates since i is a unit in this larger ring. We shall give a slightly different proof that $\mathbb{Z}[2i]$ is not a Unique Factorization Domain at the end of Section 9.3 (one in which we do not have to check that 2 and $2i$ are irreducibles).

(5) The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is another example of an integral domain that is not a Unique Factorization Domain, since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ gives two distinct factorizations of 6 into irreducibles. The principal ideal (6) in $\mathbb{Z}[\sqrt{-5}]$ can be written as a product of 4 nonprincipal prime ideals: $(6) = P_2^2 P_3 P_3'$ and the two distinct factorizations of the element 6 in $\mathbb{Z}[\sqrt{-5}]$ can be interpreted as arising from two rearrangements of this product of ideals into products of principal ideals: the product of $P_2^2 = (2)$ with $P_3 P_3' = (3)$, and the product of $P_2 P_3 = (1 + \sqrt{-5})$ with $P_2 P_3' = (1 - \sqrt{-5})$ (cf. Exercise 8).

While the *elements* of the quadratic integer ring $\mathcal{O}$ need not have unique factorization, it is a theorem (Corollary 16.16) that every *ideal* in $\mathcal{O}$ can be written uniquely as a product of prime *ideals*. The unique factorization of ideals into the product of prime ideals holds in general for rings of integers of algebraic number fields (examples of which are the quadratic integer rings) and leads to the notion of a Dedekind Domain considered in Chapter 16. It was the failure to have unique factorization into irreducibles for elements in algebraic integer rings in number theory that originally led to the definition of an ideal. The resulting uniqueness of the decomposition into prime ideals in these rings gave the elements of the ideals an "ideal" (in the sense of "perfect" or "desirable") behavior that is the basis for the choice of terminology for these (now fundamental) algebraic objects.

The first property of irreducible elements in a Unique Factorization Domain is that they are also primes. One might think that we could deduce Proposition 11 from this proposition together with the previously mentioned theorem (that we shall prove shortly) that every Principal Ideal Domain is a Unique Factorization Domain, however Proposition 11 will be used in the proof of the latter theorem.

Proposition 12. In a Unique Factorization Domain a nonzero element is a prime if and only if it is irreducible.

Proof: Let R be a Unique Factorization Domain. Since by Proposition 10, primes of R are irreducible it remains to prove that each irreducible element is a prime. Let p be an irreducible in R and assume $p \mid ab$ for some $a, b \in R$; we must show that p divides either a or b. To say that p divides ab is to say $ab = pc$ for some c in R. Writing a and b as a product of irreducibles, we see from this last equation and from the *uniqueness* of the decomposition into irreducibles of ab that the irreducible element p must be *associate* to one of the irreducibles occurring either in the factorization of a or in the factorization of b. We may assume that p is associate to one of the irreducibles in the factorization of a, i.e., that a can be written as a product $a = (up)p_2 \cdots p_n$ for u a unit and some (possibly empty set of) irreducibles $p_2, \ldots, p_n$. But then p divides a, since $a = pd$ with $d = up_2 \cdots p_n$, completing the proof.

In a Unique Factorization Domain we shall now use the terms "prime" and "irreducible" interchangeably although we shall usually refer to the "primes" in $\mathbb{Z}$ and the "irreducibles" in $F[x]$.

We shall use the preceding proposition to show that in a Unique Factorization Domain any two nonzero elements a and b have a greatest common divisor:

Proposition 13. Let a and b be two nonzero elements of the Unique Factorization Domain R and suppose

$$a = up_1^{e_1}p_2^{e_2}\cdots p_n^{e_n} \qquad \text{and} \qquad b = vp_1^{f_1}p_2^{f_2}\cdots p_n^{f_n}$$

are prime factorizations for a and b, where u and v are units, the primes $p_1, p_2, \ldots, p_n$ are *distinct* and the exponents e_i and f_i are ≥ 0. Then the element

$$d = p_1^{\min(e_1, f_1)}p_2^{\min(e_2, f_2)}\cdots p_n^{\min(e_n, f_n)}$$

(where $d = 1$ if all the exponents are 0) is a greatest common divisor of a and b.

Proof: Since the exponents of each of the primes occurring in d are no larger than the exponents occurring in the factorizations of both a and b, d divides both a and b. To show that d is a greatest common divisor, let c be any common divisor of a and b and let $c = q_1^{g_1}q_2^{g_2}\cdots q_m^{g_m}$ be the prime factorization of c. Since each q_i divides c, hence divides a and b, we see from the preceding proposition that q_i must divide one of the primes p_j. In particular, up to associates (so up to multiplication by a unit) the primes occurring in c must be a subset of the primes occurring in a and b : $\{q_1, q_2, \ldots, q_m\} \subseteq \{p_1, p_2, \ldots, p_n\}$. Similarly, the exponents for the primes occurring in c must be no larger than those occurring in d. This implies that c divides d, completing the proof.

Example

In the example above, where $a = 2210$ and $b = 1131$, we find immediately from their prime factorizations that $(a, b) = 13$. Note that if the prime factorizations for a and b are known, the proposition above gives their greatest common divisor instantly, but that finding these prime factorizations is extremely time-consuming computationally. The Euclidean Algorithm is the fastest method for determining the g.c.d. of two integers but unfortunately it gives almost no information on the prime factorizations of the integers.

We now come to one of the principal results relating some of the rings introduced in this chapter.

Theorem 14. Every Principal Ideal Domain is a Unique Factorization Domain. In particular, every Euclidean Domain is a Unique Factorization Domain.

Proof: Note that the second assertion follows from the first since Euclidean Domains are Principal Ideal Domains. To prove the first assertion let R be a Principal Ideal Domain and let r be a nonzero element of R which is not a unit. We must show first that r can be written as a finite product of irreducible elements of R and then we must verify that this decomposition is unique up to units.

The method of proof of the first part is precisely analogous to the determination of the prime factor decomposition of an integer. Assume r is nonzero and is not a unit. If r is itself irreducible, then we are done. If not, then by definition r can be written as a product $r = r_1 r_2$ where neither r_1 nor r_2 is a unit. If both these elements are irreducibles, then again we are done, having written r as a product of irreducible elements. Otherwise, at least one of the two elements, say r_1 is reducible, hence can be written as a product of two nonunit elements $r_1 = r_{11} r_{12}$, and so forth. What we must verify is that this process *terminates*, i.e., that we must necessarily reach a point where all of the elements obtained as factors of r are irreducible. Suppose this is not the case. From the factorization $r = r_1 r_2$ we obtain a *proper* inclusion of ideals: $(r) \subset (r_1) \subset R$. The first inclusion is proper since r_2 is not a unit, and the last inclusion is proper since r_1 is not a unit. From the factorization of r_1 we similarly obtain $(r) \subset (r_1) \subset (r_{11}) \subset R$. If this process of factorization did not terminate after a finite number of steps, then we would obtain an *infinite ascending chain* of ideals:

$$(r) \subset (r_1) \subset (r_{11}) \subset \cdots \subset R$$

where all containments are proper, and the Axiom of Choice ensures that an infinite chain exists (cf. Appendix I).

We now show that any ascending chain $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ of ideals in a Principal Ideal Domain eventually becomes stationary, i.e., there is some positive integer n such that $I_k = I_n$ for all $k \geq n$.[3] In particular, it is not possible to have an infinite ascending chain of ideals where all containments are proper. Let $I = \cup_{i=1}^{\infty} I_i$. It follows easily (as in the proof of Proposition 11 in Section 7.4) that I is an ideal. Since R is a Principal Ideal Domain it is principally generated, say $I = (a)$. Since I is the union of the ideals above, a must be an element of one of the ideals in the chain, say $a \in I_n$. But then we have $I_n \subseteq I = (a) \subseteq I_n$ and so $I = I_n$ and the chain becomes stationary at I_n. This proves that every nonzero element of R which is not a unit has some factorization into irreducibles in R.

It remains to prove that the above decomposition is essentially unique. We proceed by induction on the number, n, of irreducible factors in some factorization of the element r. If $n = 0$, then r is a unit. If we had $r = qc$ (some other factorization) for some irreducible q, then q would divide a unit, hence would itself be a unit, a contradiction. Suppose now that n is at least 1 and that we have two products

$$r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \qquad m \geq n$$

for r where the p_i and q_j are (not necessarily distinct) irreducibles. Since then p_1 divides the product on the right, we see by Proposition 11 that p_1 must divide one of the factors. Renumbering if necessary, we may assume p_1 divides q_1. But then $q_1 = p_1 u$ for some element u of R which must in fact be a unit since q_1 is irreducible. Thus p_1 and q_1 are associates. Cancelling p_1 (recall we are in an integral domain, so this is legitimate), we obtain the equation

$$p_2 \cdots p_n = u q_2 q_3 \cdots q_m = q_2' q_3 \cdots q_m \qquad m \geq n.$$

[3]This same argument can be used to prove the more general statement: an ascending chain of ideals becomes stationary in any commutative ring where all the ideals are *finitely generated*. This result will be needed in Chapter 12 where the details will be repeated.

where $q_2' = uq_2$ is again an irreducible (associate to q_2). By induction on n, we conclude that each of the factors on the left matches bijectively (up to associates) with the factors on the far right, hence with the factors in the middle (which are the same, up to associates). Since p_1 and q_1 (after the initial renumbering) have already been shown to be associate, this completes the induction step and the proof of the theorem.

Corollary 15. *(Fundamental Theorem of Arithmetic)* The integers $\mathbb{Z}$ are a Unique Factorization Domain.

Proof: The integers $\mathbb{Z}$ are a Euclidean Domain, hence are a Unique Factorization Domain by the theorem.

We can now complete the equivalence (Proposition 9) between the existence of a Dedekind–Hasse norm on the integral domain R and whether R is a P.I.D.

Corollary 16. Let R be a P.I.D. Then there exists a multiplicative Dedekind–Hasse norm on R.

Proof: If R is a P.I.D. then R is a U.F.D. Define the norm N by setting $N(0) = 0$, $N(u) = 1$ if u is a unit, and $N(a) = 2^n$ if $a = p_1 p_2 \cdots p_n$ where the p_i are irreducibles in R (well defined since the number of irreducible factors of a is unique). Clearly $N(ab) = N(a)N(b)$ so N is positive and multiplicative. To show that N is a Dedekind–Hasse norm, suppose that a, b are nonzero elements of R. Then the ideal generated by a and b is principal by assumption, say $(a, b) = (r)$. If a is not contained in the ideal (b) then also r is not contained in (b), i.e., r is not divisible by b. Since $b = xr$ for some $x \in R$, it follows that x is not a unit in R and so $N(b) = N(x)N(r) > N(r)$. Hence (a, b) contains a nonzero element with norm strictly smaller than the norm of b, completing the proof.

Factorization in the Gaussian Integers

We end our discussion of Unique Factorization Domains by describing the irreducible elements in the Gaussian integers $\mathbb{Z}[i]$ and the corresponding application to a famous theorem of Fermat in elementary number theory. This is particularly appropriate since the classical study of $\mathbb{Z}[i]$ initiated the algebraic study of rings.

In general, let $\mathcal{O}$ be a quadratic integer ring and let N be the associated field norm introduced in Section 7.1. Suppose $\alpha \in \mathcal{O}$ is an element whose norm is a prime p in $\mathbb{Z}$. If $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathcal{O}$ then $p = N(\alpha) = N(\beta)N(\gamma)$ so that one of $N(\beta)$ or $N(\gamma)$ is ± 1 and the other is $\pm p$. Since we have seen that an element of $\mathcal{O}$ has norm ± 1 if and only if it is a unit in $\mathcal{O}$, one of the factors of α is a unit. It follows that

if $N(\alpha)$ is $\pm$ a prime (in $\mathbb{Z}$), then α is irreducible in $\mathcal{O}$.

Suppose that π is a prime element in $\mathcal{O}$ and let (π) be the ideal generated by π in $\mathcal{O}$. Since (π) is a prime ideal in $\mathcal{O}$ it is easy to check that $(\pi) \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ (if a and b are integers with $ab \in (\pi)$ then either a or b is an element of (π), so a or b is in $(\pi) \cap \mathbb{Z}$). Since $N(\pi)$ is a nonzero integer in (π) we have $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$ for some integer prime p. It follows from $p \in (\pi)$ that π is a divisor in $\mathcal{O}$ of the

integer prime p, and so the prime elements in $\mathcal{O}$ can be found by determining how the primes in $\mathbb{Z}$ factor in the larger ring $\mathcal{O}$. Suppose π divides the prime p in $\mathcal{O}$, say $p = \pi\pi'$. Then $N(\pi)N(\pi') = N(p) = p^2$, so since π is not a unit there are only two possibilities: either $N(\pi) = \pm p^2$ or $N(\pi) = \pm p$. In the former case $N(\pi') = \pm 1$, hence π' is a unit and $p = \pi$ (up to associates) is irreducible in $\mathbb{Z}[i]$. In the latter case $N(\pi) = N(\pi') = \pm p$, hence π' is also irreducible and $p = \pi\pi'$ is the product of precisely two irreducibles.

Consider now the special case $D = -1$ of the Gaussian integers $\mathbb{Z}[i]$. We have seen that the units in $\mathbb{Z}[i]$ are the elements ± 1 and $\pm i$. We proved in Section 1 that $\mathbb{Z}[i]$ is a Euclidean Domain, hence is also a Principal Ideal Domain and a Unique Factorization Domain, so the irreducible elements are the same as the prime elements, and can be determined by seeing how the primes in $\mathbb{Z}$ factor in the larger ring $\mathbb{Z}[i]$.

In this case $\alpha = a + bi$ has $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$, where $\overline{\alpha} = a - bi$ is the complex conjugate of α. It follows by what we just saw that *p factors in $\mathbb{Z}[i]$ into precisely two irreducibles if and only if $p = a^2 + b^2$ is the sum of two integer squares (otherwise p remains irreducible in $\mathbb{Z}[i]$).* If $p = a^2 + b^2$ then the corresponding irreducible elements in $\mathbb{Z}[i]$ are $a \pm bi$.

Clearly $2 = 1^2 + 1^2$ is the sum of two squares, giving the factorization $2 = (1+i)(1-i) = -i(1+i)^2$. The irreducibles $1+i$ and $1-i = -i(1+i)$ are associates and it is easy to check that this is the only situation in which conjugate irreducibles $a + bi$ and $a - bi$ can be associates.

Since the square of any integer is congruent to either 0 or 1 modulo 4, an odd prime in $\mathbb{Z}$ that is the sum of two squares must be congruent to 1 modulo 4. Thus if p is a prime of $\mathbb{Z}$ with $p \equiv 3 \bmod 4$ then p is not the sum of two squares and p remains irreducible in $\mathbb{Z}[i]$.

Suppose now that p is a prime of $\mathbb{Z}$ with $p \equiv 1 \bmod 4$. We shall prove that p cannot be irreducible in $\mathbb{Z}[i]$ which will show that $p = (a + bi)(a - bi)$ factors as the product of two distinct irreducibles in $\mathbb{Z}[i]$ or, equivalently, that $p = a^2 + b^2$ is the sum of two squares. We first prove the following result from elementary number theory:

Lemma 17. The prime number $p \in \mathbb{Z}$ divides an integer of the form $n^2 + 1$ if and only if p is either 2 or is an odd prime congruent to 1 modulo 4.

Proof: The statement for $p = 2$ is trivial since $2 \mid 1^2 + 1$. If p is an odd prime, note that $p \mid n^2 + 1$ is equivalent to $n^2 = -1$ in $\mathbb{Z}/p\mathbb{Z}$. This in turn is equivalent to saying the residue class of n is of order 4 in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus p divides an integer of the form $n^2 + 1$ if and only if $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4. By Lagrange's Theorem, if $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4 then $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ is divisible by 4, i.e., p is congruent to 1 modulo 4.

Conversely, suppose $p - 1$ is divisible by 4. We first argue that $(\mathbb{Z}/p\mathbb{Z})^\times$ contains a unique element of order 2. If $m^2 \equiv 1 \bmod p$ then p divides $m^2 - 1 = (m-1)(m+1)$. Thus p divides either $m - 1$ (i.e., $m \equiv 1 \bmod p$) or $m + 1$ (i.e., $m \equiv -1 \bmod p$), so -1 is the unique residue class of order 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$. Now the abelian group $(\mathbb{Z}/p\mathbb{Z})^\times$ contains a subgroup H of order 4 (for example, the quotient by the subgroup $\{\pm 1\}$ contains a subgroup of order 2 whose preimage is a subgroup of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$).

Since the Klein 4-group has three elements of order 2 whereas $(\mathbb{Z}/p\mathbb{Z})^\times$ — hence also H — has a unique element of order 2, H must be the cyclic group of order 4. Thus $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4, namely a generator for H.

Remark: We shall prove later (Corollary 19 in Section 9.5) that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group, from which it is immediate that there is an element of order 4 if and only if $p-1$ is divisible by 4.

By Lemma 17, if $p \equiv 1 \bmod 4$ is a prime then p divides n^2+1 in $\mathbb{Z}$ for some $n \in \mathbb{Z}$, so certainly p divides $n^2+1 = (n+i)(n-i)$ in $\mathbb{Z}[i]$. If p were irreducible in $\mathbb{Z}[i]$ then p would divide either $n+i$ or $n-i$ in $\mathbb{Z}[i]$. In this situation, since p is a real number, it would follow that p divides both $n+i$ and its complex conjugate $n-i$; hence p would divide their difference, $2i$. This is clearly not the case. We have proved the following result:

Proposition 18.

(1) *(Fermat's Theorem on sums of squares)* The prime p is the sum of two integer squares, $p = a^2+b^2$, $a, b \in \mathbb{Z}$, if and only if $p = 2$ or $p \equiv 1 \bmod 4$. Except for interchanging a and b or changing the signs of a and b, the representation of p as a sum of two squares is unique.

(2) The irreducible elements in the Gaussian integers $\mathbb{Z}[i]$ are as follows:

- **(a)** $1+i$ (which has norm 2),
- **(b)** the primes $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$ (which have norm p^2), and
- **(c)** $a+bi$, $a-bi$, the distinct irreducible factors of $p = a^2+b^2 = (a+bi)(a-bi)$ for the primes $p \in \mathbb{Z}$ with $p \equiv 1 \bmod 4$ (both of which have norm p).

The first part of Proposition 18 is a famous theorem of Fermat in elementary number theory, for which a number of alternate proofs can be given.

More generally, the question of whether the integer $n \in \mathbb{Z}$ can be written as a sum of two integer squares, $n = A^2+B^2$, is equivalent to the question of whether n is the norm of an element $A+Bi$ in the Gaussian integers, i.e., $n = A^2+B^2 = N(A+Bi)$. Writing $A+Bi = \pi_1\pi_2\cdots\pi_k$ as a product of irreducibles (uniquely up to units) it follows from the explicit description of the irreducibles in $\mathbb{Z}[i]$ in Proposition 18 that n is a norm if and only if the prime divisors of n that are congruent to 3 mod 4 occur to even exponents. Further, if this condition on n is satisfied, then the uniqueness of the factorization of $A+Bi$ in $\mathbb{Z}[i]$ allows us to count the number of representations of n as a sum of two squares, as in the following corollary.

Corollary 19. Let n be a positive integer and write

$$n = 2^k p_1^{a_1}\cdots p_r^{a_r} q_1^{b_1}\cdots q_s^{b_s}$$

where $p_1, \ldots, p_r$ are distinct primes congruent to 1 modulo 4 and $q_1, \ldots, q_s$ are distinct primes congruent to 3 modulo 4. Then n can be written as a sum of two squares in $\mathbb{Z}$, i.e., $n = A^2+B^2$ with $A, B \in \mathbb{Z}$, if and only if each b_i is even. Further, if this condition on n is satisfied, then the number of representations of n as a sum of two squares is $4(a_1+1)(a_2+1)\cdots(a_r+1)$.

Proof: The first statement in the corollary was proved above. Assume now that $b_1, \ldots, b_s$ are all even. For each prime p_i congruent to 1 modulo 4 write $p_i = \pi_i \overline{\pi_i}$ for $i = 1, 2, \ldots, r$, where π_i and $\overline{\pi_i}$ are irreducibles as in (2)(c) of Proposition 18. If $N(A + Bi) = n$ then examining norms we see that, up to units, the factorization of $A + Bi$ into irreducibles in $\mathbb{Z}[i]$ is given by

$$A + Bi = (1 + i)^k (\pi_1^{a_{1,1}} \overline{\pi_1}^{a_{1,2}}) \ldots (\pi_r^{a_{r,1}} \overline{\pi_r}^{a_{r,2}}) q_1^{b_1/2} \ldots q_s^{b_s/2}$$

with nonnegative integers $a_{i,1}, a_{i,2}$ satisfying $a_{i,1} + a_{i,2} = a_i$ for $i = 1, 2, \ldots, r$. Since $a_{i,1}$ can have the values $0, 1, \ldots, a_i$ (and then $a_{i,2}$ is determined), there are a total of $(a_1 + 1)(a_2 + 1) \cdots (a_r + 1)$ distinct elements $A + Bi$ in $\mathbb{Z}[i]$ of norm n, up to units. Finally, since there are four units in $\mathbb{Z}[i]$, the second statement in the corollary follows.

Example

Since $493 = 17 \cdot 29$ and both primes are congruent to 1 modulo 4, $493 = A^2 + B^2$ is the sum of two integer squares. Since $17 = (4 + i)(4 - i)$ and $29 = (5 + 2i)(5 - 2i)$ the possible factorizations of $A + Bi$ in $\mathbb{Z}[i]$ up to units are $(4 + i)(5 + 2i) = 18 + 13i$, $(4 + i)(5 - 2i) = 22 - 3i$, $(4 - i)(5 - 2i) = 22 + 3i$, and $(4 - i)(5 - 2i) = 18 - 13i$. Multiplying by -1 reverses both signs and multiplication by i interchanges the A and B and introduces one sign change. Then $493 = (\pm 18)^2 + (\pm 13)^2 = (\pm 22)^2 + (\pm 3)^2$ with all possible choices of signs give 8 of the 16 possible representations of 493 as the sum of two squares; the remaining 8 are obtained by interchanging the two summands.

Similarly, the integer $58000957 = 7^6 \cdot 17 \cdot 29$ can be written as a sum of two squares in precisely 16 ways, obtained by multiplying each of the integers A, B in $493 = A^2 + B^2$ above by 7^3.

Summary

In summary, we have the following inclusions among classes of commutative rings with identity:

$$\textit{fields} \subset \textit{Euclidean Domains} \subset \textit{P.I.D.s} \subset \textit{U.F.D.s} \subset \textit{integral domains}$$

with all containments being proper. Recall that $\mathbb{Z}$ is a Euclidean Domain that is not a field, the quadratic integer ring $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a Principal Ideal Domain that is not a Euclidean Domain, $\mathbb{Z}[x]$ is a Unique Factorization Domain (Theorem 7 in Chapter 9) that is not a Principal Ideal Domain and $\mathbb{Z}[\sqrt{-5}]$ is an integral domain that is not a Unique Factorization Domain.

EXERCISES

1. Let $G = \mathbb{Q}^\times$ be the multiplicative group of nonzero rational numbers. If $\alpha = p/q \in G$, where p and q are relatively prime integers, let $\varphi : G \to G$ be the map which interchanges the primes 2 and 3 in the prime power factorizations of p and q (so, for example, $\varphi(2^4 3^{11} 5^1 13^2) = 3^4 2^{11} 5^1 13^2$, $\varphi(3/16) = \varphi(3/2^4) = 2/3^4 = 2/81$, and φ is the identity on all rational numbers with numerators and denominators relatively prime to 2 and to 3).
(a) Prove that φ is a group isomorphism.
(b) Prove that there are infinitely many isomorphisms of the group G to itself.

(c) Prove that none of the isomorphisms above can be extended to an isomorphism of the *ring* $\mathbb{Q}$ to itself. In fact prove that the identity map is the only ring isomorphism of $\mathbb{Q}$.

2. Let a and b be nonzero elements of the Unique Factorization Domain R. Prove that a and b have a least common multiple (cf. Exercise 11 of Section 1) and describe it in terms of the prime factorizations of a and b in the same fashion that Proposition 13 describes their greatest common divisor.

3. Determine all the representations of the integer $2130797 = 17^2 \cdot 73 \cdot 101$ as a sum of two squares.

4. Prove that if an integer is the sum of two rational squares, then it is the sum of two integer squares (for example, $13 = (1/5)^2 + (18/5)^2 = 2^2 + 3^2$).

5. Let $R = \mathbb{Z}[\sqrt{-n}]$ where n is a squarefree integer greater than 3.

(a) Prove that 2, $\sqrt{-n}$ and $1 + \sqrt{-n}$ are irreducibles in R.

(b) Prove that R is not a U.F.D. Conclude that the quadratic integer ring $\mathcal{O}$ is not a U.F.D. for $D \equiv 2, 3 \bmod 4$, $D < -3$ (so also not Euclidean and not a P.I.D.). [Show that either $\sqrt{-n}$ or $1 + \sqrt{-n}$ is not prime.]

(c) Give an explicit ideal in R that is not principal. [Using (b) consider a maximal ideal containing the nonprime ideal $(\sqrt{-n})$ or $(1 + \sqrt{-n})$.]

6. (a) Prove that the quotient ring $\mathbb{Z}[i]/(1 + i)$ is a field of order 2.

(b) Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \bmod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

(c) Let $p \in \mathbb{Z}$ be a prime with $p \equiv 1 \bmod 4$ and write $p = \pi\bar{\pi}$ as in Proposition 18. Show that the hypotheses for the Chinese Remainder Theorem (Theorem 17 in Section 7.6) are satisfied and that $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi})$ as rings. Show that the quotient ring $\mathbb{Z}[i]/(p)$ has order p^2 and conclude that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\bar{\pi})$ are both fields of order p.

7. Let π be an irreducible element in $\mathbb{Z}[i]$.

(a) For any integer $n \geq 0$, prove that $(\pi^{n+1}) = \pi^{n+1}\mathbb{Z}[i]$ is an ideal in $(\pi^n) = \pi^n\mathbb{Z}[i]$ and that multiplication by π^n induces an isomorphism $\mathbb{Z}[i]/(\pi) \cong (\pi^n)/(\pi^{n+1})$ as additive abelian groups.

(b) Prove that $|\mathbb{Z}[i]/(\pi^n)| = |\mathbb{Z}[i]/(\pi)|^n$.

(c) Prove for any nonzero α in $\mathbb{Z}[i]$ that the quotient ring $\mathbb{Z}[i]/(\alpha)$ has order equal to $N(\alpha)$. [Use (b) together with the Chinese Remainder Theorem and the results of the previous exercise.]

8. Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ and define the ideals $I_2 = (2, 1 + \sqrt{-5})$, $I_3 = (3, 2 + \sqrt{-5})$, and $I_3' = (3, 2 - \sqrt{-5})$.

(a) Prove that 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducibles in R, no two of which are associate in R, and that $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ are two distinct factorizations of 6 into irreducibles in R.

(b) Prove that I_2, I_3, and I_3' are prime ideals in R. [One approach: for I_3, observe that $R/I_3 \cong (R/(3))/(I_3/(3))$ by the Third Isomorphism Theorem for Rings. Show that $R/(3)$ has 9 elements, $(I_3/(3))$ has 3 elements, and that $R/I_3 \cong \mathbb{Z}/3\mathbb{Z}$ as an additive abelian group. Conclude that I_3 is a maximal (hence prime) ideal and that $R/I_3 \cong \mathbb{Z}/3\mathbb{Z}$ as rings.]

(c) Show that the factorizations in (a) imply the equality of ideals $(6) = (2)(3)$ and $(6) = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Show that these two ideal factorizations give the same factorization of the ideal (6) as the product of prime ideals (cf. Exercise 5 in Section 2).

9. Suppose that the quadratic integer ring $\mathcal{O}$ is a P.I.D. Prove that the absolute value of the field norm N on $\mathcal{O}$ (cf. Section 7.1) is a Dedekind–Hasse norm on $\mathcal{O}$. Conclude that if the quadratic integer ring $\mathcal{O}$ possesses *any* Dedekind–Hasse norm, then in fact the absolute value of the field norm on $\mathcal{O}$ already provides a Dedekind–Hasse norm on $\mathcal{O}$. [If $\alpha, \beta \in \mathcal{O}$ then $(\alpha, \beta) = (\gamma)$ for some $\gamma \in \mathcal{O}$. Show that if β does not divide α then $0 < |N(\gamma)| < |N(\beta)|$ — use the fact that the units in $\mathcal{O}$ are precisely the elements whose norm is ± 1.]

Remark: If $\mathcal{O}$ is a Euclidean Domain with respect to some norm it is not necessarily true that it is a Euclidean Domain with respect to the absolute value of the field norm (although this is true for $D < 0$, cf. Exercise 8 in Section 1). An example is $D = 69$ (cf. D. Clark, *A quadratic field which is Euclidean but not norm-Euclidean*, Manuscripta Math., 83(1994), pp. 327–330).

10. (*k-stage Euclidean Domains*) Let R be an integral domain and let $N : R \to \mathbb{Z}^+ \cup \{0\}$ be a norm on R. The ring R is Euclidean with respect to N if for any $a, b \in R$ with $b \neq 0$, there exist elements q and r in R with

$$a = qb + r \qquad \text{with } r = 0 \text{ or } N(r) < N(b).$$

Suppose now that this condition is weakened, namely that for any $a, b \in R$ with $b \neq 0$, there exist elements q, q' and r, r' in R with

$$a = qb + r, \quad b = q'r + r' \qquad \text{with } r' = 0 \text{ or } N(r') < N(b),$$

i.e., the remainder after two divisions is smaller. Call such a domain a *2-stage Euclidean Domain.*

(a) Prove that iterating the divisions in a 2-stage Euclidean Domain produces a greatest common divisor of a and b which is a linear combination of a and b. Conclude that every *finitely generated* ideal of a 2-stage Euclidean Domain is principal. (There are 2-stage Euclidean Domains that are *not* P.I.D.s, however.) [Imitate the proof of Theorem 4.]

(b) Prove that a 2-stage Euclidean Domain in which every nonzero nonunit can be factored into a finite number of irreducibles is a Unique Factorization Domain. [Prove first that irreducible elements are prime, as follows. If p is irreducible and $p \mid ab$ with p not dividing a, use part (a) to write $px + ay = 1$ for some x, y. Multiply through by b to conclude that $p \mid b$, so p is prime. Now follow the proof of uniqueness in Theorem 14.]

(c) Make the obvious generalization to define the notion of a k-stage Euclidean Domain for any integer $k \geq 1$. Prove that statements (a) and (b) remain valid if "2-stage Euclidean" is replaced by "k-stage Euclidean."

Remarks: There are examples of rings which are 2-stage Euclidean but are not Euclidean. There are also examples of rings which are not Euclidean with respect to a given norm but which are k-stage Euclidean with respect to the norm (for example, the ring $\mathbb{Z}[\sqrt{14}]$ is not Euclidean with respect to the usual norm $N(a+b\sqrt{14}) = |a^2 - 14b^2|$, but is 2-stage Euclidean with respect to this norm). The k-stage Euclidean condition is also related to the question of whether the group $GL_n(R)$ of invertible $n \times n$ matrices with entries from R is generated by elementary matrices (matrices with 1's along the main diagonal, a single 1 somewhere off the main diagonal, and 0's elsewhere).

11. (*Characterization of P.I.D.s*) Prove that R is a P.I.D. if and only if R is a U.F.D. that is also a Bezout Domain (cf. Exercise 7 in Section 2). [One direction is given by Theorem 14. For the converse, let a be a nonzero element of the ideal I with a minimal number of irreducible factors. Prove that $I = (a)$ by showing that if there is an element $b \in I$ that is not in (a) then $(a, b) = (d)$ leads to a contradiction.]

CHAPTER 9

Polynomial Rings

We begin this chapter on polynomial rings with a summary of facts from the preceding two chapters (with references where needed). The basic definitions were given in slightly greater detail in Section 7.2. For convenience, the ring R will always be a commutative ring with identity $1 \neq 0$.

9.1 DEFINITIONS AND BASIC PROPERTIES

The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ and each $a_i \in R$. If $a_n \neq 0$ then the polynomial is of degree n, $a_n x^n$ is the leading term, and a_n is the leading coefficient (where the leading coefficient of the zero polynomial is defined to be 0). The polynomial is monic if $a_n = 1$. Addition of polynomials is "componentwise":

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

(here a_n or b_n may be zero in order for addition of polynomials of different degrees to be defined). Multiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ and then extending to all polynomials by the distributive laws so that in general

$$\left(\sum_{i=0}^{n} a_i x^i\right) \times \left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

In this way $R[x]$ is a commutative ring with identity (the identity 1 from R) in which we identify R with the subring of constant polynomials.

We have already noted that if R is an integral domain then the leading term of a product of polynomials is the product of the leading terms of the factors. The following is Proposition 4 of Section 7.2 which we record here for completeness.

Proposition 1. Let R be an integral domain. Then

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$ if $p(x), q(x)$ are nonzero

(2) the units of $R[x]$ are just the units of R

(3) $R[x]$ is an integral domain.

Recall also that if R is an integral domain, the quotient field of $R[x]$ consists of all

quotients $\frac{p(x)}{q(x)}$ where $q(x)$ is not the zero polynomial (and is called the field of rational functions in x with coefficients in R).

The next result describes a relation between the ideals of R and those of $R[x]$.

Proposition 2. Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polynomials with coefficients in I). Then

$$R[x]/(I) \cong (R/I)[x].$$

In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$.

Proof: There is a natural map $\varphi : R[x] \to (R/I)[x]$ given by reducing each of the coefficients of a polynomial modulo I. The definition of addition and multiplication in these two rings shows that φ is a ring homomorphism. The kernel is precisely the set of polynomials each of whose coefficients is an element of I, which is to say that $\ker \varphi = I[x] = (I)$, proving the first part of the proposition. The last statement follows from Proposition 1, since if I is a prime ideal in R, then R/I is an integral domain, hence also $(R/I)[x]$ is an integral domain. This shows if I is a prime ideal of R, then (I) is a prime ideal of $R[x]$.

Note that it is not true that if I is a maximal ideal of R then (I) is a maximal ideal of $R[x]$. However, if I is maximal in R then the ideal of $R[x]$ generated by I and x is maximal in $R[x]$.

We now give an example of the "reduction homomorphism" of Proposition 2 which will be useful on a number of occasions later ("reduction homomorphisms" were also discussed at the end of Section 7.3 with reference to reducing the integers mod n) .

Example

Let $R = \mathbb{Z}$ and consider the ideal $n\mathbb{Z}$ of $\mathbb{Z}$. Then the isomorphism above can be written

$$\mathbb{Z}[x]/n\mathbb{Z}[x] \cong \mathbb{Z}/n\mathbb{Z}[x]$$

and the natural projection map of $\mathbb{Z}[x]$ to $\mathbb{Z}/n\mathbb{Z}[x]$ by reducing the coefficients modulo n is a ring homomorphism. If n is composite, then the quotient ring is not an integral domain. If, however, n is a prime p, then $\mathbb{Z}/p\mathbb{Z}$ is a field and so $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain (in fact, a Euclidean Domain, as we shall see shortly). We also see that the set of polynomials whose coefficients are divisible by p is a prime ideal in $\mathbb{Z}[x]$.

We close this section with a description of the natural extension to polynomial rings in *several* variables.

Definition. The *polynomial ring in the variables* $x_1, x_2, \ldots, x_n$ *with coefficients in* R, denoted $R[x_1, x_2, \ldots, x_n]$, is defined inductively by

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$$

This definition means that we can consider polynomials in n variables with coefficients in R simply as polynomials in *one* variable (say x_n) but now with coefficients that

are themselves *polynomials in $n-1$ variables*. In a slightly more concrete formulation, a nonzero polynomial in $x_1, x_2, \ldots, x_n$ with coefficients in R is a finite sum of nonzero *monomial terms*, i.e., a finite sum of elements of the form

$$ax_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$$

where $a \in R$ (the *coefficient* of the term) and the d_i are nonnegative integers. A monic term $x_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$ is called simply a *monomial* and is the *monomial part* of the term $ax_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$. The exponent d_i is called the *degree in* x_i of the term and the sum

$$d = d_1 + d_2 + \cdots + d_n$$

is called the *degree* of the term. The ordered n-tuple $(d_1, d_2, \ldots, d_n)$ is the *multidegree* of the term. The *degree* of a nonzero polynomial is the largest degree of any of its monomial terms. A polynomial is called *homogeneous* or a *form* if all its terms have the same degree. If f is a nonzero polynomial in n variables, the sum of all the monomial terms in f of degree k is called the *homogeneous component of f of degree k*. If f has degree d then f may be written uniquely as the sum $f_0 + f_1 + \cdots + f_d$ where f_k is the homogeneous component of f of degree k, for $0 \leq k \leq d$ (where some f_k may be zero).

Finally, to define a polynomial ring in an *arbitrary* number of variables with coefficients in R we take finite sums of monomial terms of the type above (but where the variables are not restricted to just $x_1, \ldots, x_n$), with the natural addition and multiplication. Alternatively, we could define this ring as the *union* of *all* the polynomial rings in a *finite* number of the variables being considered.

Example

The polynomial ring $\mathbb{Z}[x, y]$ in two variables x and y with integer coefficients consists of all finite sums of monomial terms of the form ax^iy^j (of degree $i + j$). For example,

$$p(x, y) = 2x^3 + xy - y^2$$

and

$$q(x, y) = -3xy + 2y^2 + x^2y^3$$

are both elements of $\mathbb{Z}[x, y]$, of degrees 3 and 5, respectively. We have

$$p(x, y) + q(x, y) = 2x^3 - 2xy + y^2 + x^2y^3$$

and

$$p(x, y)q(x, y) = -6x^4y + 4x^3y^2 + 2x^5y^3 - 3x^2y^2 + 5xy^3 + x^3y^4 - 2y^4 - x^2y^5,$$

a polynomial of degree 8. To view this last polynomial, say, as a polynomial in y with coefficients in $\mathbb{Z}[x]$ as in the definition of several variable polynomial rings above, we would write the polynomial in the form

$$(-6x^4)y + (4x^3 - 3x^2)y^2 + (2x^5 + 5x)y^3 + (x^3 - 2)y^4 - (x^2)y^5.$$

The nonzero homogeneous components of $f = f(x, y) = p(x, y)q(x, y)$ are the polynomials $f_4 = -3x^2y^2 + 5xy^3 - 2y^4$ (degree 4), $f_5 = -6x^4y + 4x^3y^2$ (degree 5), $f_7 = x^3y^4 - x^2y^5$ (degree 7), and $f_8 = 2x^5y^3$ (degree 8).

Each of the statements in Proposition 1 is true for polynomial rings with an arbitrary number of variables. This follows by induction for finitely many variables and from the definition in terms of unions in the case of polynomial rings in arbitrarily many variables.

EXERCISES

1. Let $p(x, y, z) = 2x^2y - 3xy^3z + 4y^2z^5$ and $q(x, y, z) = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$ be polynomials in $\mathbb{Z}[x, y, z]$.
   (a) Write each of p and q as a polynomial in x with coefficients in $\mathbb{Z}[y, z]$.
   (b) Find the degree of each of p and q.
   (c) Find the degree of p and q in each of the three variables x, y and z.
   (d) Compute pq and find the degree of pq in each of the three variables x, y and z.
   (e) Write pq as a polynomial in the variable z with coefficients in $\mathbb{Z}[x, y]$.
2. Repeat the preceding exercise under the assumption that the coefficients of p and q are in $\mathbb{Z}/3\mathbb{Z}$.
3. If R is a commutative ring and $x_1, x_2, \ldots, x_n$ are independent variables over R, prove that $R[x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}]$ is isomorphic to $R[x_1, x_2, \ldots, x_n]$ for any permutation π of $\{1, 2, \ldots, n\}$.
4. Prove that the ideals (x) and (x, y) are prime ideals in $\mathbb{Q}[x, y]$ but only the latter ideal is a maximal ideal.
5. Prove that (x, y) and $(2, x, y)$ are prime ideals in $\mathbb{Z}[x, y]$ but only the latter ideal is a maximal ideal.
6. Prove that (x, y) is not a principal ideal in $\mathbb{Q}[x, y]$.
7. Let R be a commutative ring with 1. Prove that a polynomial ring in more than one variable over R is not a Principal Ideal Domain.
8. Let F be a field and let $R = F[x, x^2y, x^3y^2, \ldots, x^ny^{n-1}, \ldots]$ be a subring of the polynomial ring $F[x, y]$.
   (a) Prove that the fields of fractions of R and $F[x, y]$ are the same.
   (b) Prove that R contains an ideal that is not finitely generated.
9. Prove that a polynomial ring in infinitely many variables with coefficients in any commutative ring contains ideals that are not finitely generated.
10. Prove that the ring $\mathbb{Z}[x_1, x_2, x_3, \ldots]/(x_1x_2, x_3x_4, x_5x_6, \ldots)$ contains infinitely many minimal prime ideals (cf. Exercise 36 of Section 7.4).
11. Show that the radical of the ideal $I = (x, y^2)$ in $\mathbb{Q}[x, y]$ is (x, y) (cf. Exercise 30, Section 7.4). Deduce that I is a primary ideal that is not a power of a prime ideal (cf. Exercise 41, Section 7.4).
12. Let $R = \mathbb{Q}[x, y, z]$ and let bars denote passage to $\mathbb{Q}[x, y, z]/(xy - z^2)$. Prove that $\overline{P} = (\overline{x}, \overline{z})$ is a prime ideal. Show that $\overline{xy} \in \overline{P}^2$ but that no power of $\overline{y}$ lies in $\overline{P}^2$. (This shows $\overline{P}$ is a prime ideal whose square is *not* a primary ideal — cf. Exercise 41, Section 7.4).
13. Prove that the rings $F[x, y]/(y^2 - x)$ and $F[x, y]/(y^2 - x^2)$ are not isomorphic for any field F.
14. Let R be an integral domain and let i, j be relatively prime integers. Prove that the ideal $(x^i - y^j)$ is a prime ideal in $R[x, y]$. [Consider the ring homomorphism φ from $R[x, y]$ to $R[t]$ defined by mapping x to t^j and mapping y to t^i. Show that an element of $R[x, y]$

differs from an element in $(x^i - y^j)$ by a polynomial $f(x)$ of degree at most $j-1$ in y and observe that the exponents of $\varphi(x^r y^s)$ are distinct for $0 \leq s < j$.]

15. Let $p(x_1, x_2, \ldots, x_n)$ be a homogeneous polynomial of degree k in $R[x_1, \ldots, x_n]$. Prove that for all $\lambda \in R$ we have $p(\lambda x_1, \lambda x_2, \ldots, \lambda x_n) = \lambda^k p(x_1, x_2, \ldots, x_n)$.

16. Prove that the product of two homogeneous polynomials is again homogeneous.

17. An ideal I in $R[x_1, \ldots, x_n]$ is called a *homogeneous ideal* if whenever $p \in I$ then each homogeneous component of p is also in I. Prove that an ideal is a homogeneous ideal if and only if it may be generated by homogeneous polynomials. [Use induction on degrees to show the "if" implication.]

The following exercise shows that some care must be taken when working with polynomials over noncommutative rings R (the ring operations in $R[x]$ are defined in the same way as for commutative rings R), in particular when considering polynomials as functions.

18. Let R be an arbitrary ring and let Func(R) be the ring of all functions from R to itself. If $p(x) \in R[x]$ is a polynomial, let $f_p \in$ Func(R) be the function on R defined by $f_p(r) = p(r)$ (the usual way of viewing a polynomial in $R[x]$ as defining a function on R by "evaluating at r").

(a) For fixed $a \in R$, prove that "evaluation at a" is a ring homomorphism from Func(R) to R (cf. Example 4 following Theorem 7 in Section 7.3).

(b) Prove that the map $\varphi : R[x] \to$ Func(R) defined by $\varphi(p(x)) = f_p$ is not a ring homomorphism in general. Deduce that polynomial identities need not give corresponding identities when the polynomials are viewed as functions. [If $R = \mathbb{H}$ is the ring of real Hamilton Quaternions show that $p(x) = x^2 + 1$ factors as $(x+i)(x-i)$, but that $p(j) = 0$ while $(j+i)(j-i) \neq 0$.]

(c) For fixed $a \in R$, prove that the composite "evaluation at a" of the maps in (a) and (b) mapping $R[x]$ to R is a ring homomorphism if and only if a is in the center of R.

9.2 POLYNOMIAL RINGS OVER FIELDS I

We now consider more carefully the situation where the coefficient ring is a *field* F. We can define a *norm* on $F[x]$ by defining $N(p(x)) =$ degree of $p(x)$ (where we set $N(0) = 0$). From elementary algebra we know that we can divide one polynomial with, say, rational coefficients by another (nonzero) polynomial with rational coefficients to obtain a quotient and remainder. The same is true over any field.

Theorem 3. Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or degree } r(x) < \text{degree } b(x) .$$

Proof: If $a(x)$ is the zero polynomial then take $q(x) = r(x) = 0$. We may therefore assume $a(x) \neq 0$ and prove the existence of $q(x)$ and $r(x)$ by induction on $n =$ degree $a(x)$. Let $b(x)$ have degree m. If $n < m$ take $q(x) = 0$ and $r(x) = a(x)$. Otherwise $n \geq m$. Write

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

and

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

Then the polynomial $a'(x) = a(x) - \dfrac{a_n}{b_m}x^{n-m}b(x)$ is of degree less than n (we have arranged to subtract the leading term from $a(x)$). Note that this polynomial is well defined because the coefficients are taken from a *field* and $b_m \neq 0$. By induction then, there exist polynomials $q'(x)$ and $r(x)$ with

$$a'(x) = q'(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or degree } r(x) < \text{degree } b(x).$$

Then, letting $q(x) = q'(x) + \dfrac{a_n}{b_m}x^{n-m}$ we have

$$a(x) = q(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or degree } r(x) < \text{degree } b(x)$$

completing the induction step.

As for the uniqueness, suppose $q_1(x)$ and $r_1(x)$ also satisfied the conditions of the theorem. Then both $a(x) - q(x)b(x)$ and $a(x) - q_1(x)b(x)$ are of degree less than m = degree $b(x)$. The difference of these two polynomials, i.e., $b(x)(q(x) - q_1(x))$ is also of degree less than m. But the degree of the product of two nonzero polynomials is the sum of their degrees (since F is an integral domain), hence $q(x) - q_1(x)$ must be 0, that is, $q(x) = q_1(x)$. This implies $r(x) = r_1(x)$, completing the proof.

Corollary 4. If F is a field, then $F[x]$ is a Principal Ideal Domain and a Unique Factorization Domain.

Proof: This is immediate from the results of the last chapter.

Recall also from Corollary 8 in Section 8.2 that if R is any commutative ring such that $R[x]$ is a Principal Ideal Domain (or Euclidean Domain) then R must be a field. We shall see in the next section, however, that $R[x]$ is a Unique Factorization Domain whenever R itself is a Unique Factorization Domain.

Examples

(1) By the above remarks the ring $\mathbb{Z}[x]$ is not a Principal Ideal Domain. As we have already seen (Example 3 beginning of Section 7.4) the ideal $(2, x)$ is not principal in this ring.

(2) $\mathbb{Q}[x]$ is a Principal Ideal Domain since the coefficients lie in the field $\mathbb{Q}$. The ideal generated in $\mathbb{Z}[x]$ by 2 and x is not principal in the subring $\mathbb{Z}[x]$ of $\mathbb{Q}[x]$. However, the ideal generated in $\mathbb{Q}[x]$ is principal; in fact it is the entire ring (so has 1 as a generator) since 2 is a unit in $\mathbb{Q}[x]$.

(3) If p is a prime, the ring $\mathbb{Z}/p\mathbb{Z}[x]$ obtained by reducing $\mathbb{Z}[x]$ modulo the prime ideal (p) is a Principal Ideal Domain, since the coefficients lie in the field $\mathbb{Z}/p\mathbb{Z}$. This example shows that the quotient of a ring which is not a Principal Ideal Domain *may* be a Principal Ideal Domain. To follow the ideal $(2, x)$ above in this example, note that if $p = 2$, then the ideal $(2, x)$ reduces to the ideal (x) in the quotient $\mathbb{Z}/2\mathbb{Z}[x]$, which is a proper (maximal) ideal. If $p \neq 2$, then 2 is a unit in the quotient, so the ideal $(2, x)$ reduces to the entire ring $\mathbb{Z}/p\mathbb{Z}[x]$.

(4) $\mathbb{Q}[x, y]$, the ring of polynomials in two variables with rational coefficients, is *not* a Principal Ideal Domain since this ring is $\mathbb{Q}[x][y]$ and $\mathbb{Q}[x]$ is not a field (any element

of positive degree is not invertible). It is an exercise to see that the ideal (x, y) is not a principal ideal in this ring. We shall see shortly that $\mathbb{Q}[x, y]$ *is* a Unique Factorization Domain.

We note that the quotient and remainder in the Division Algorithm applied to $a(x), b(x) \in F[x]$ are *independent of field extensions* in the following sense. Suppose the field F is contained in the field E and $a(x) = Q(x)b(x) + R(x)$ for some $Q(x)$, $R(x)$ satisfying the conditions of Theorem 3 in $E[x]$. Write $a(x) = q(x)b(x)+r(x)$ for some $q(x), r(x) \in F[x]$ and apply the uniqueness condition of Theorem 3 in the ring $E[x]$ to deduce that $Q(x) = q(x)$ and $R(x) = r(x)$. In particular, $b(x)$ divides $a(x)$ in the ring $E[x]$ if and only if $b(x)$ divides $a(x)$ in $F[x]$. Also, the greatest common divisor of $a(x)$ and $b(x)$ (which can be obtained from the Euclidean Algorithm) is the same, once we make it unique by specifying it to be monic, whether these elements are viewed in $F[x]$ or in $E[x]$.

EXERCISES

Let F be a field and let x be an indeterminate over F.

1. Let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$ and let bars denote passage to the quotient $F[x]/(f(x))$. Prove that for each $\overline{g(x)}$ there is a unique polynomial $g_0(x)$ of degree $\leq n - 1$ such that $\overline{g(x)} = \overline{g_0(x)}$ (equivalently, the elements $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ are a *basis* of the vector space $F[x]/(f(x))$ over F — in particular, the dimension of this space is n). [Use the Division Algorithm.]
2. Let F be a finite field of order q and let $f(x)$ be a polynomial in $F[x]$ of degree $n \geq 1$. Prove that $F[x]/(f(x))$ has q^n elements. [Use the preceding exercise.]
3. Let $f(x)$ be a polynomial in $F[x]$. Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible. [Use Proposition 7, Section 8.2.]
4. Let F be a finite field. Prove that $F[x]$ contains infinitely many primes. (Note that over an infinite field the polynomials of degree 1 are an infinite set of primes in the ring of polynomials).
5. Exhibit *all* the ideals in the ring $F[x]/(p(x))$, where F is a field and $p(x)$ is a polynomial in $F[x]$ (describe them in terms of the factorization of $p(x)$).
6. Describe (briefly) the ring structure of the following rings:
   (a) $\mathbb{Z}[x]/(2)$, **(b)** $\mathbb{Z}[x]/(x)$, **(c)** $\mathbb{Z}[x]/(x^2)$, **(d)** $\mathbb{Z}[x, y]/(x^2, y^2, 2)$.
   Show that $\alpha^2 = 0$ or 1 for every α in the last ring and determine those elements with $\alpha^2 = 0$. Determine the characteristics of each of these rings (cf. Exercise 26, Section 7.3).
7. Determine all the ideals of the ring $\mathbb{Z}[x]/(2, x^3 + 1)$.
8. Determine the greatest common divisor of $a(x) = x^3 - 2$ and $b(x) = x + 1$ in $\mathbb{Q}[x]$ and write it as a linear combination (in $\mathbb{Q}[x]$) of $a(x)$ and $b(x)$.
9. Determine the greatest common divisor of $a(x) = x^5+2x^3+x^2+x+1$ and the polynomial $b(x) = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1$ in $\mathbb{Q}[x]$ and write it as a linear combination (in $\mathbb{Q}[x]$) of $a(x)$ and $b(x)$.
10. Determine the greatest common divisor of $a(x) = x^3+4x^2+x-6$ and $b(x) = x^5-6x+5$ in $\mathbb{Q}[x]$ and write it as a linear combination (in $\mathbb{Q}[x]$) of $a(x)$ and $b(x)$.
11. Suppose $f(x)$ and $g(x)$ are two nonzero polynomials in $\mathbb{Q}[x]$ with greatest common divisor $d(x)$.

(a) Given $h(x) \in \mathbb{Q}[x]$, show that there are polynomials $a(x), b(x) \in \mathbb{Q}[x]$ satisfying the equation $a(x)f(x) + b(x)g(x) = h(x)$ if and only if $h(x)$ is divisible by $d(x)$.

(b) If $a_0(x), b_0(x) \in \mathbb{Q}[x]$ are particular solutions to the equation in (a), show that the full set of solutions to this equation is given by

$$a(x) = a_0(x) + m(x)\frac{g(x)}{(x)d}$$
$$b(x) = b_0(x) - m(x)\frac{f(x)}{d(x)}$$

as $m(x)$ ranges over the polynomials in $\mathbb{Q}[x]$. [cf. Exercise 4 in Section 8.1]

12. Let $F[x, y_1, y_2, \ldots]$ be the polynomial ring in the infinite set of variables $x, y_1, y_2, \ldots$ over the field F, and let I be the ideal $(x - y_1^2, y_1 - y_2^2, \ldots, y_i - y_{i+1}^2, \ldots)$ in this ring. Define R to be the ring $F[x, y_1, y_2, \ldots]/I$, so that in R the square of each y_{i+1} is y_i and $y_1^2 = x$ modulo I, i.e., x has a 2^ith root, for every i. Denote the image of y_i in R as $x^{1/2^i}$. Let R_n be the subring of R generated by F and $x^{1/2^n}$.

(a) Prove that $R_1 \subseteq R_2 \subseteq \cdots$ and that R is the union of all R_n, i.e., $R = \cup_{n=1}^{\infty} R_n$.

(b) Prove that R_n is isomorphic to a polynomial ring in one variable over F, so that R_n is a P.I.D. Deduce that R is a Bezout Domain (cf. Exercise 7 in Section 8.2). [First show that the ring $S_n = F[x, y_1, \ldots, y_n]/(x - y_1^2, y_1 - y_2^2, \ldots, y_{n-1} - y_n^2)$ is isomorphic to the polynomial ring $F[y_n]$. Then show any polynomial relation y_n satisfies in R_n gives a corresponding relation in S_N for some $N \geq n$.]

(c) Prove that the ideal generated by $x, x^{1/2}, x^{1/4}, \ldots$ in R is not finitely generated (so R is not a P.I.D.).

13. This exercise introduces a noncommutative ring which is a "right" Euclidean Domain (and a "left" Principal Ideal Domain) but is not a "left" Euclidean Domain (and not a "right" Principal Ideal Domain). Let F be a field of characteristic p in which not every element is a p^{th} power: $F \neq F^p$ (for example the field $F = \mathbb{F}_p(t)$ of rational functions in the variable t with coefficients in $\mathbb{F}_p$ is such a field). Let $R = F\{x\}$ be the "twisted" polynomial ring of polynomials $\sum_{i=0}^{n} a_i x^i$ in x with coefficients in F with the usual (termwise) addition

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

but with a noncommutative multiplication defined by

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i b_j^{p^i}\right) x^k .$$

This multiplication arises from defining $xa = a^p x$ for every $a \in F$ (so the powers of x do not commute with the coefficients) and extending in a natural way. Let N be the norm defined by taking the degree of a polynomial in R: $N(f) = \deg(f)$.

(a) Show that $x^k a = a^{p^k} x^k$ for every $a \in F$ and every integer $k \geq 0$ and that R is a ring with this definition of multiplication. [Use the fact that $(a + b)^p = a^p + b^p$ for every $a, b \in F$ since F has characteristic p, so also $(a + b)^{p^k} = a^{p^k} + b^{p^k}$ for every $a, b \in F$.]

(b) Prove that the degree of a product of two elements of R is the sum of the degrees of the elements. Prove that R has no zero divisors.

(c) Prove that R is "right Euclidean" with respect to N, i.e., for any polynomials $f, g \in R$ with $g \neq 0$, there exist polynomials q and r in R with

$$f = qg + r \qquad \text{with } r = 0 \text{ or } \deg(r) < \deg(g).$$

Use this to prove that every *left* ideal of R is principal.

(d) Let $f = \theta x$ for some $\theta \in F$, $\theta \notin F^p$ and let $g = x$. Prove that there are no polynomials q and r in R with

$$f = gq + r \qquad \text{with } r = 0 \text{ or } \deg(r) < \deg(g),$$

so in particular R is not "left Euclidean" with respect to N. Prove that the right ideal of R generated by x and θx is not principal. Conclude that R is not "left Euclidean" with respect to *any* norm.

9.3 POLYNOMIAL RINGS THAT ARE UNIQUE FACTORIZATION DOMAINS

We have seen in Proposition 1 that if R is an integral domain then $R[x]$ is also an integral domain. Also, such an R can be embedded in its field of fractions F (Theorem 15, Section 7.5), so that $R[x] \subseteq F[x]$ is a subring, and $F[x]$ is a Euclidean Domain (hence a Principal Ideal Domain and a Unique Factorization Domain). Many computations for $R[x]$ may be accomplished in $F[x]$ at the expense of allowing fractional coefficients. This raises the immediate question of how computations (such as factorizations of polynomials) in $F[x]$ can be used to give information in $R[x]$.

For instance, suppose $p(x)$ is a polynomial in $R[x]$. Since $F[x]$ is a Unique Factorization Domain we can factor $p(x)$ uniquely into a product of irreducibles in $F[x]$. It is natural to ask whether we can do the same in $R[x]$, i.e., is $R[x]$ a Unique Factorization Domain? In general the answer is no because if $R[x]$ were a Unique Factorization Domain, the constant polynomials would have to be uniquely factored into irreducible elements of $R[x]$, necessarily of degree 0 since the degrees of products add, that is, R would itself have to be a Unique Factorization Domain. Thus if R is an integral domain which is not a Unique Factorization Domain, $R[x]$ cannot be a Unique Factorization Domain. On the other hand, it turns out that if R is a Unique Factorization Domain, then $R[x]$ is also a Unique Factorization Domain. The method of proving this is to first factor uniquely in $F[x]$ and then "clear denominators" to obtain a unique factorization in $R[x]$. The first step in making this precise is to compare the factorization of a polynomial in $F[x]$ to a factorization in $R[x]$.

Proposition 5. *(Gauss' Lemma)* Let R be a Unique Factorization Domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Proof: The coefficients of the polynomials on the right hand side of the equation $p(x) = A(x)B(x)$ are elements in the field F, hence are quotients of elements from the Unique Factorization Domain R. Multiplying through by a common denominator

for all these coefficients, we obtain an equation $dp(x) = a'(x)b'(x)$ where now $a'(x)$ and $b'(x)$ are elements of $R[x]$ and d is a nonzero element of R. If d is a unit in R, the proposition is true with $a(x) = d^{-1}a'(x)$ and $b(x) = b'(x)$. Assume d is not a unit and write d as a product of irreducibles in R, say $d = p_1 \cdots p_n$. Since p_1 is irreducible in R, the ideal (p_1) is prime (cf. Proposition 12, Section 8.3), so by Proposition 2 above, the ideal $p_1R[x]$ is prime in $R[x]$ and $(R/p_1R)[x]$ is an integral domain. Reducing the equation $dp(x) = a'(x)b'(x)$ modulo p_1, we obtain the equation $0 = \overline{a'(x)}\,\overline{b'(x)}$ in this integral domain (the bars denote the images of these polynomials in the quotient ring), hence one of the two factors, say $\overline{a'(x)}$ must be 0. But this means all the coefficients of $a'(x)$ are divisible by p_1, so that $\frac{1}{p_1}a'(x)$ also has coefficients in R. In other words, in the equation $dp(x) = a'(x)b'(x)$ we can cancel a factor of p_1 from d (on the left) and from either $a'(x)$ or $b'(x)$ (on the right) and still have an equation in $R[x]$. But now the factor d on the left hand side has one fewer irreducible factors. Proceeding in the same fashion with each of the remaining factors of d, we can cancel all of the factors of d into the two polynomials on the right hand side, leaving an equation $p(x) = a(x)b(x)$ with $a(x), b(x) \in R[x]$ and with $a(x), b(x)$ being F-multiples of $A(x)$, $B(x)$, respectively. This completes the proof.

Note that we cannot prove that $a(x)$ and $b(x)$ are necessarily R-multiples of $A(x)$, $B(x)$, respectively, because, for example, we could factor x^2 in $\mathbb{Q}[x]$ with $A(x) = 2x$ and $B(x) = \frac{1}{2}x$ but no *integer* multiples of $A(x)$ and $B(x)$ give a factorization of x^2 in $\mathbb{Z}[x]$.

The elements of the ring R become *units* in the Unique Factorization Domain $F[x]$ (the units in $F[x]$ being the nonzero elements of F). For example, $7x$ factors in $\mathbb{Z}[x]$ into a product of two irreducibles: 7 and x (so $7x$ is not irreducible in $\mathbb{Z}[x]$), whereas $7x$ is the unit 7 times the irreducible x in $\mathbb{Q}[x]$ (so $7x$ is irreducible in $\mathbb{Q}[x]$). The following corollary shows that this is essentially the *only* difference between the irreducible elements in $R[x]$ and those in $F[x]$.

Corollary 6. Let R be a Unique Factorization Domain, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Proof: By Gauss' Lemma above, if $p(x)$ is reducible in $F[x]$, then it is reducible in $R[x]$. Conversely, the assumption on the greatest common divisor of the coefficients of $p(x)$ implies that if it is reducible in $R[x]$, then $p(x) = a(x)b(x)$ where neither $a(x)$ nor $b(x)$ are constant polynomials in $R[x]$. This same factorization shows that $p(x)$ is reducible in $F[x]$, completing the proof.

Theorem 7. R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.

Proof: We have indicated above that $R[x]$ a Unique Factorization Domain forces R to be a Unique Factorization Domain. Suppose conversely that R is a Unique Factorization Domain, F is its field of fractions and $p(x)$ is a nonzero element of $R[x]$. Let d be

the greatest common divisor of the coefficients of $p(x)$, so that $p(x) = dp'(x)$, where the g.c.d. of the coefficients of $p'(x)$ is 1. Such a factorization of $p(x)$ is unique up to a change in d (so up to a unit in R), and since d can be factored uniquely into irreducibles in R (and these are also irreducibles in the larger ring $R[x]$), it suffices to prove that $p'(x)$ can be factored uniquely into irreducibles in $R[x]$. Thus we may assume that the greatest common divisor of the coefficients of $p(x)$ is 1. We may further assume $p(x)$ is not a unit in $R[x]$, i.e., degree $p(x) > 0$.

Since $F[x]$ is a Unique Factorization Domain, $p(x)$ can be factored uniquely into irreducibles in $F[x]$. By Gauss' Lemma, such a factorization implies there is a factorization of $p(x)$ in $R[x]$ whose factors are F-multiples of the factors in $F[x]$. Since the greatest common divisor of the coefficients of $p(x)$ is 1, the g.c.d. of the coefficients in each of these factors in $R[x]$ must be 1. By Corollary 6, each of these factors is an irreducible in $R[x]$. This shows that $p(x)$ can be written as a finite product of irreducibles in $R[x]$.

The uniqueness of the factorization of $p(x)$ follows from the uniqueness in $F[x]$. Suppose

$$p(x) = q_1(x) \cdots q_r(x) = q_1'(x) \cdots q_s'(x)$$

are two factorizations of $p(x)$ into irreducibles in $R[x]$. Since the g.c.d. of the coefficients of $p(x)$ is 1, the same is true for each of the irreducible factors above — in particular, each has positive degree. By Corollary 6, each $q_i(x)$ and $q_j'(x)$ is an irreducible in $F[x]$. By unique factorization in $F[x]$, $r = s$ and, possibly after rearrangement, $q_i(x)$ and $q_i'(x)$ are associates in $F[x]$ for all $i \in \{1, \ldots, r\}$. It remains to show they are associates in $R[x]$. Since the units of $F[x]$ are precisely the elements of $F^\times$ we need to consider when $q(x) = \frac{a}{b}q'(x)$ for some $q(x), q'(x) \in R[x]$ and nonzero elements a, b of R, where the greatest common divisor of the coefficients of each of $q(x)$ and $q'(x)$ is 1. In this case $bq(x) = aq'(x)$; the g.c.d. of the coefficients on the left hand side is b and on the right hand side is a. Since in a Unique Factorization Domain the g.c.d. of the coefficients of a nonzero polynomial is unique up to units, $a = ub$ for some unit u in R. Thus $q(x) = uq'(x)$ and so $q(x)$ and $q'(x)$ are associates in R as well. This completes the proof.

Corollary 8. If R is a Unique Factorization Domain, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a Unique Factorization Domain.

Proof: For finitely many variables, this follows by induction from Theorem 7, since a polynomial ring in n variables can be considered as a polynomial ring in one variable with coefficients in a polynomial ring in $n-1$ variables. The general case follows from the definition of a polynomial ring in an arbitrary number of variables as the union of polynomial rings in finitely many variables.

Examples

(1) $\mathbb{Z}[x]$, $\mathbb{Z}[x, y]$, etc. are Unique Factorization Domains. The ring $\mathbb{Z}[x]$ gives an example of a Unique Factorization Domain that is not a Principal Ideal Domain.

(2) Similarly, $\mathbb{Q}[x]$, $\mathbb{Q}[x, y]$, etc. are Unique Factorization Domains.

We saw earlier that if R is a Unique Factorization Domain with field of fractions F and $p(x) \in R[x]$, then we can factor out the greatest common divisor d of the coefficients of $p(x)$ to obtain $p(x) = dp'(x)$, where $p'(x)$ is irreducible in both $R[x]$ and $F[x]$. Suppose now that R is an *arbitrary* integral domain with field of fractions F. In R the notion of greatest common divisor may not make sense, however one might still ask if, say, a *monic* polynomial which is irreducible in $R[x]$ is still irreducible in $F[x]$ (i.e., whether the last statement in Corollary 6 is true).

Note first that if a monic polynomial $p(x)$ is reducible, it must have a factorization $p(x) = a(x)b(x)$ in $R[x]$ with both $a(x)$ and $b(x)$ *monic, nonconstant* polynomials (recall that the leading term of $p(x)$ is the product of the leading terms of the factors, so the leading coefficients of both $a(x)$ and $b(x)$ are units — we can thus arrange these to be 1). In other words, a nonconstant *monic* polynomial $p(x)$ is irreducible if and only if it cannot be factored as a product of two *monic* polynomials of smaller degree.

We now see that it is not true that if R is an arbitrary integral domain and $p(x)$ is a monic irreducible polynomial in $R[x]$, then $p(x)$ is irreducible in $F[x]$. For example, let $R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$ (a subring of the complex numbers) and let $p(x) = x^2+1$. Then the fraction field of R is $F = \{a+bi \mid a, b \in \mathbb{Q}\}$. The polynomial $p(x)$ factors uniquely into a product of two linear factors in $F[x]$: $x^2+1 = (x-i)(x+i)$ so in particular, $p(x)$ *is reducible in* $F[x]$. Neither of these factors lies in $R[x]$ (because $i \notin R$) so $p(x)$ *is irreducible in* $R[x]$. In particular, by Corollary 6, $\mathbb{Z}[2i]$ *is not a Unique Factorization Domain.*

EXERCISES

1. Let R be an integral domain with quotient field F and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of smaller degree than $p(x)$. Prove that if $a(x) \notin R[x]$ then R is not a Unique Factorization Domain. Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a U.F.D.
2. Prove that if $f(x)$ and $g(x)$ are polynomials with rational coefficients whose product $f(x)g(x)$ has integer coefficients, then the product of any coefficient of $g(x)$ with any coefficient of $f(x)$ is an integer.
3. Let F be a field. Prove that the set R of polynomials in $F[x]$ whose coefficient of x is equal to 0 is a subring of $F[x]$ and that R is not a U.F.D. [Show that $x^6 = (x^2)^3 = (x^3)^2$ gives two distinct factorizations of x^6 into irreducibles.]
4. Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.
   (a) Prove that R is an integral domain and its units are ± 1.
   (b) Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1. Prove that these irreducibles are prime in R.
   (c) Show that x cannot be written as the product of irreducibles in R (in particular, x is not irreducible) and conclude that R is not a U.F.D.
   (d) Show that x is not a prime in R and describe the quotient ring $R/(x)$.
5. Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the ring considered in the previous exercise.
   (a) Suppose that $f(x), g(x) \in \mathbb{Q}[x]$ are two nonzero polynomials with rational coefficients and that x^r is the largest power of x dividing both $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$, (i.e., r is the degree of the lowest order term appearing in either $f(x)$ or $g(x)$). Let f_r and

g_r be the coefficients of x^r in $f(x)$ and $g(x)$, respectively (one of which is nonzero by definition of r). Then $\mathbb{Z}f_r + \mathbb{Z}g_r = \mathbb{Z}d_r$ for some nonzero $d_r \in \mathbb{Q}$ (cf. Exercise 14 in Section 2.4). Prove that there is a polynomial $d(x) \in \mathbb{Q}[x]$ that is a g.c.d. of $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$ and whose term of minimal degree is $d_r x^r$.

(b) Prove that $f(x) = d(x)q_1(x)$ and $g(x) = d(x)q_2(x)$ where $q_1(x)$ and $q_2(x)$ are elements of the subring R of $\mathbb{Q}[x]$.

(c) Prove that $d(x) = a(x)f(x) + b(x)g(x)$ for polynomials $a(x), b(x)$ in R. [The existence of $a(x), b(x)$ in the Euclidean Domain $\mathbb{Q}[x]$ is immediate. Use Exercise 11 in Section 2 to show that $a(x)$ and $b(x)$ can be chosen to lie in R.]

(d) Conclude from (a) and (b) that $Rf(x) + Rg(x) = Rd(x)$ in $\mathbb{Q}[x]$ and use this to prove that R is a Bezout Domain (cf. Exercise 7 in Section 8.2).

(e) Show that (d), the results of the previous exercise, and Exercise 11 of Section 8.3 imply that R must contain ideals that are not principal (hence not finitely generated). Prove that in fact $I = x\mathbb{Q}[x]$ is an ideal of R that is not finitely generated.

9.4 IRREDUCIBILITY CRITERIA

If R is a Unique Factorization Domain, then by Corollary 8 a polynomial ring in any number of variables with coefficients in R is also a Unique Factorization Domain. It is of interest then to determine the irreducible elements in such a polynomial ring, particularly in the ring $R[x]$. In the one-variable case, a nonconstant monic polynomial is irreducible in $R[x]$ if it cannot be factored as the product of two other polynomials of smaller degrees. Determining whether a polynomial has factors is frequently difficult to check, particularly for polynomials of large degree in several variables. The purpose of irreducibility criteria is to give an easier mechanism for determining when some types of polynomials are irreducible.

For the most part we restrict attention to polynomials in one variable where the coefficient ring is a Unique Factorization Domain. By Gauss' Lemma it suffices to consider factorizations in $F[x]$ where F is the field of fractions of R (although we shall occasionally consider questions of irreducibility when the coefficient ring is just an integral domain). The next proposition considers when there is a factor of degree one (a *linear* factor).

Proposition 9. Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, i.e., there is an $\alpha \in F$ with $p(\alpha) = 0$.

Proof: If $p(x)$ has a factor of degree one, then since F is a field, we may assume the factor is monic, i.e., is of the form $(x - \alpha)$ for some $\alpha \in F$. But then $p(\alpha) = 0$. Conversely, suppose $p(\alpha) = 0$. By the Division Algorithm in $F[x]$ we may write

$$p(x) = q(x)(x - \alpha) + r$$

where r is a constant. Since $p(\alpha) = 0$, r must be 0, hence $p(x)$ has $(x - \alpha)$ as a factor.

Proposition 9 gives a criterion for irreducibility for polynomials of small degree:

Proposition 10. A polynomial of degree two or three over a field F is reducible if and only if it has a root in F.

Proof: This follows immediately from the previous proposition, since a polynomial of degree two or three is reducible if and only if it has at least one linear factor.

The next result limits the possibilities for roots of polynomials with integer coefficients (it is stated for $\mathbb{Z}[x]$ for convenience although it clearly generalizes to $R[x]$, where R is any Unique Factorization Domain).

Proposition 11. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms (i.e., r and s are relatively prime integers) and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$: $r \mid a_0$ and $s \mid a_n$. In particular, if $p(x)$ is a *monic* polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

Proof: By hypothesis, $p(r/s) = 0 = a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_0$. Multiplying through by s^n gives

$$0 = a_n r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n.$$

Thus $a_n r^n = s(-a_{n-1}r^{n-1} - \cdots - a_0 s^{n-1})$, so s divides $a_n r^n$. By assumption, s is relatively prime to r and it follows that $s \mid a_n$. Similarly, solving the equation for $a_0 s^n$ shows that $r \mid a_0$. The last assertion of the proposition follows from the previous ones.

Examples

(1) The polynomial $x^3 - 3x - 1$ is irreducible in $\mathbb{Z}[x]$. To prove this, by Gauss' Lemma and Proposition 10 it suffices to show it has no rational roots. By Proposition 11 the only candidates for rational roots are integers which divide the constant term 1, namely ± 1. Substituting both 1 and -1 into the polynomial shows that these are not roots.

(2) For p any prime the polynomials $x^2 - p$ and $x^3 - p$ are irreducible in $\mathbb{Q}[x]$. This is because they have degrees ≤ 3 so it suffices to show they have no rational roots. By Proposition 11 the only candidates for roots are ± 1 and $\pm p$, but none of these give 0 when they are substituted into the polynomial.

(3) The polynomial $x^2 + 1$ is reducible in $\mathbb{Z}/2\mathbb{Z}[x]$ since it has 1 as a root, and it factors as $(x + 1)^2$.

(4) The polynomial $x^2 + x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$ since it does not have a root in $\mathbb{Z}/2\mathbb{Z}$: $0^2 + 0 + 1 = 1$ and $1^2 + 1 + 1 = 1$.

(5) Similarly, the polynomial $x^3 + x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$.

This technique is limited to polynomials of low degree because it relies on the presence of a factor of degree one. A polynomial of degree 4, for example, may be the product of two irreducible quadratics, hence be reducible but have no linear factor. One fairly general technique for checking irreducibility uses Proposition 2 above and consists of reducing the coefficients modulo some ideal.

Proposition 12. Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proof: Suppose $p(x)$ cannot be factored in $(R/I)[x]$ but that $p(x)$ is reducible in $R[x]$. As noted at the end of the preceding section this means there are monic, nonconstant polynomials $a(x)$ and $b(x)$ in $R[x]$ such that $p(x) = a(x)b(x)$. By Proposition 2, reducing the coefficients modulo I gives a factorization in $(R/I)[x]$ with nonconstant factors, a contradiction.

This proposition indicates that if it is possible to find a proper ideal I such that the *reduced* polynomial cannot be factored, then the polynomial is itself irreducible. Unfortunately, there are examples of polynomials even in $\mathbb{Z}[x]$ which are irreducible but whose reductions modulo every ideal are reducible (so their irreducibility is not detectable by this technique). For example, the polynomial $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every prime (we shall verify this in Chapter 14) and the polynomial $x^4 - 72x^2 + 4$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every integer.

Examples

(1) Consider the polynomial $p(x) = x^2 + x + 1$ in $\mathbb{Z}[x]$. Reducing modulo 2, we see from Example 4 above that $p(x)$ is irreducible in $\mathbb{Z}[x]$. Similarly, $x^3 + x + 1$ is irreducible in $\mathbb{Z}[x]$ because it is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$.

(2) The polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ since it is irreducible in $\mathbb{Z}/3\mathbb{Z}[x]$ (no root in $\mathbb{Z}/3\mathbb{Z}$), but is reducible mod 2. This shows that the converse to Proposition 12 does not hold.

(3) The idea of reducing modulo an ideal to determine irreducibility can be used also in several variables, but some care must be exercised. For example, the polynomial $x^2 + xy + 1$ in $\mathbb{Z}[x, y]$ is irreducible since modulo the ideal (y) it is $x^2 + 1$ in $\mathbb{Z}[x]$, which is irreducible and of the same degree. In this sort of argument it is necessary to be careful about "collapsing." For example, the polynomial $xy + x + y + 1$ (which is $(x + 1)(y + 1)$) is reducible, but appears irreducible modulo both (x) and (y). The reason for this is that nonunit polynomials in $\mathbb{Z}[x, y]$ can reduce to units in the quotient. To take account of this it is necessary to determine which elements in the original ring become units in the quotient. The elements in $\mathbb{Z}[x, y]$ which are units modulo (y), for example, are the polynomials in $\mathbb{Z}[x, y]$ with constant term ± 1 and all nonconstant terms divisible by y. The fact that $x^2 + xy + 1$ and its reduction mod (y) have the same degree therefore eliminates the possibility of a factor which is a unit modulo (y), but not a unit in $\mathbb{Z}[x, y]$ and gives the irreducibility of this polynomial.

A special case of reducing modulo an ideal to test for irreducibility which is frequently useful is known as *Eisenstein's Criterion* (although originally proved earlier by Schönemann, so more properly known as the *Eisenstein-Schönemann Criterion*):

Proposition 13. *(Eisenstein's Criterion)* Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial in $R[x]$ (here $n \geq 1$). Suppose $a_{n-1}, \ldots, a_1, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$.

Proof: Suppose $f(x)$ were reducible, say $f(x) = a(x)b(x)$ in $R[x]$, where $a(x)$ and $b(x)$ are nonconstant polynomials. Reducing this equation modulo P and using the assumptions on the coefficients of $f(x)$ we obtain the equation $x^n = \overline{a(x)}\overline{b(x)}$ in $(R/P)[x]$, where the bar denotes the polynomials with coefficients reduced mod P. Since P is a prime ideal, R/P is an integral domain, and it follows that both $\overline{a(x)}$ and $\overline{b(x)}$ have 0 constant term, i.e., the constant terms of both $a(x)$ and $b(x)$ are elements of P. But then the constant term a_0 of $f(x)$ as the product of these two would be an element of P^2, a contradiction.

Eisenstein's Criterion is most frequently applied to $\mathbb{Z}[x]$ so we state the result explicitly for this case:

Corollary 14. *(Eisenstein's Criterion for $\mathbb{Z}[x]$)* Let p be a prime in $\mathbb{Z}$ and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, $n \geq 1$. Suppose p divides a_i for all $i \in \{0, 1, \ldots, n-1\}$ but that p^2 does not divide a_0. Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Proof: This is simply a restatement of Proposition 13 in the case of the prime ideal (p) in $\mathbb{Z}$ together with Corollary 6.

Examples

(1) The polynomial $x^4 + 10x + 5$ in $\mathbb{Z}[x]$ is irreducible by Eisenstein's Criterion applied for the prime 5.

(2) If a is any integer which is divisible by some prime p but not divisible by p^2, then $x^n - a$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein's Criterion. In particular, $x^n - p$ is irreducible for all positive integers n and so for $n \geq 2$ the n^{th} roots of p are not rational numbers (i.e., this polynomial has no root in $\mathbb{Q}$).

(3) Consider the polynomial $f(x) = x^4 + 1$ mentioned previously. Eisenstein's Criterion does not apply directly to $f(x)$. The polynomial $g(x) = f(x+1)$ is $(x+1)^4 + 1$, i.e., $x^4 + 4x^3 + 6x^2 + 4x + 2$, and Eisenstein's Criterion for the prime 2 shows that this polynomial is irreducible. It follows then that $f(x)$ must also be irreducible, since any factorization for $f(x)$ would provide a factorization for $g(x)$ (just replace x by $x + 1$ in each of the factors). This example shows that Eisenstein's Criterion can sometimes be used to verify the irreducibility of a polynomial to which it does not immediately apply.

(4) As another example of this, let p be a prime and consider the polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

an example of a *cyclotomic polynomial* which we shall consider more thoroughly in Part IV. Again, Eisenstein's Criterion does not immediately apply, but it does apply for the prime p to the polynomial

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p \in \mathbb{Z}[x]$$

since all the coefficients except the first are divisible by p by the Binomial Theorem. As before, this shows $\Phi_p(x)$ is irreducible in $\mathbb{Z}[x]$.

(5) As an example of the use of the more general Eisenstein's Criterion in Proposition 13 we mimic Example 2 above. Let $R = \mathbb{Q}[x]$ and let n be any positive integer. Consider

the polynomial $X^n - x$ in the ring $R[X]$. The ideal (x) is prime in the coefficient ring R since $R/(x) = \mathbb{Q}[x]/(x)$ is the integral domain $\mathbb{Q}$. Eisenstein's Criterion for the ideal (x) of R applies directly to show that $X^n - x$ is irreducible in $R[X]$. Note that this construction works with $\mathbb{Q}$ replaced by any field or, indeed, by any integral domain.

There are now efficient algorithms for factoring polynomials over certain fields. For polynomials with integer coefficients these algorithms have been implemented in a number of computer packages. An efficient algorithm for factoring polynomials over $\mathbb{F}_p$, called the Berlekamp Algorithm, is described in detail in the exercises at the end of Section 14.3.

EXERCISES

1. Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$, p a prime.
   (a) $x^2 + x + 1$ in $\mathbb{F}_2[x]$.
   (b) $x^3 + x + 1$ in $\mathbb{F}_3[x]$.
   (c) $x^4 + 1$ in $\mathbb{F}_5[x]$.
   (d) $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$.
2. Prove that the following polynomials are irreducible in $\mathbb{Z}[x]$:
   (a) $x^4 - 4x^3 + 6$
   (b) $x^6 + 30x^5 - 15x^3 + 6x - 120$
   (c) $x^4 + 4x^3 + 6x^2 + 2x + 1$ [Substitute $x - 1$ for x.]
   (d) $\dfrac{(x+2)^p - 2^p}{x}$, where p is an odd prime.
3. Show that the polynomial $(x-1)(x-2)\cdots(x-n) - 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$. [If the polynomial factors consider the values of the factors at $x = 1, 2, \ldots, n$.]
4. Show that the polynomial $(x-1)(x-2)\cdots(x-n)+1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$, $n \neq 4$.
5. Find all the monic irreducible polynomials of degree ≤ 3 in $\mathbb{F}_2[x]$, and the same in $\mathbb{F}_3[x]$.
6. Construct fields of each of the following orders: **(a)** 9, **(b)** 49, **(c)** 8, **(d)** 81 (you may exhibit these as $F[x]/(f(x))$ for some F and f). [Use Exercises 2 and 3 in Section 2.]
7. Prove that $\mathbb{R}[x]/(x^2 + 1)$ is a field which is isomorphic to the complex numbers.
8. Prove that $K_1 = \mathbb{F}_{11}[x]/(x^2+1)$ and $K_2 = \mathbb{F}_{11}[y]/(y^2+2y+2)$ are both fields with 121 elements. Prove that the map which sends the element $p(\bar{x})$ of K_1 to the element $p(\bar{y}+1)$ of K_2 (where p is any polynomial with coefficients in $\mathbb{F}_{11}$) is well defined and gives a ring (hence field) isomorphism from K_1 to K_2.
9. Prove that the polynomial $x^2 - \sqrt{2}$ is irreducible over $\mathbb{Z}[\sqrt{2}]$ (you may use the fact that $\mathbb{Z}[\sqrt{2}]$ is a U.F.D. — cf. Exercise 9 of Section 8.1).
10. Prove that the polynomial $p(x) = x^4 - 4x^2 + 8x + 2$ is irreducible over the quadratic field $F = \mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Q}\}$. [First use the method of Proposition 11 for the Unique Factorization Domain $\mathbb{Z}[\sqrt{-2}]$ (cf. Exercise 8, Section 8.1) to show that if $\alpha \in \mathbb{Z}[\sqrt{-2}]$ is a root of $p(x)$ then α is a divisor of 2 in $\mathbb{Z}[\sqrt{-2}]$. Conclude that α must be ± 1, $\pm\sqrt{-2}$ or ± 2, and hence show $p(x)$ has no linear factor over F. Show similarly that $p(x)$ is not the product of two quadratics with coefficients in F.]

11. Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

12. Prove that $x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible over $\mathbb{Z}$ if and only if n is a prime.

13. Prove that $x^3 + nx + 2$ is irreducible over $\mathbb{Z}$ for all integers $n \neq 1, -3, -5$.

14. Factor each of the two polynomials: $x^8 - 1$ and $x^6 - 1$ into irreducibles over each of the following rings: **(a)** $\mathbb{Z}$, **(b)** $\mathbb{Z}/2\mathbb{Z}$, **(c)** $\mathbb{Z}/3\mathbb{Z}$.

15. Prove that if F is a field then the polynomial $X^n - x$ which has coefficients in the ring $F[[x]]$ of formal power series (cf. Exercise 3 of Section 7.2) is irreducible over $F[[x]]$. [Recall that $F[[x]]$ is a Euclidean Domain — cf. Exercise 5, Section 7.2 and Example 4, Section 8.1.]

16. Let F be a field and let $f(x)$ be a polynomial of degree n in $F[x]$. The polynomial $g(x) = x^n f(1/x)$ is called the *reverse* of $f(x)$.

(a) Describe the coefficients of g in terms of the coefficients of f.

(b) Prove that f is irreducible if and only if g is irreducible.

17. Prove the following variant of Eisenstein's Criterion: let P be a prime ideal in the Unique Factorization Domain R and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$, $n \geq 1$. Suppose $a_n \notin P$, $a_{n-1}, \ldots, a_0 \in P$ and $a_0 \notin P^2$. Prove that $f(x)$ is irreducible in $F[x]$, where F is the quotient field of R.

18. Show that $6x^5 + 14x^3 - 21x + 35$ and $18x^5 - 30x^2 + 120x + 360$ are irreducible in $\mathbb{Q}[x]$.

19. Let F be a field and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$. The *derivative*, $D_x(f(x))$, of $f(x)$ is defined by

$$D_x(f(x)) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

where, as usual, $na = a + a + \cdots + a$ (n times). Note that $D_x(f(x))$ is again a polynomial with coefficients in F.

The polynomial $f(x)$ is said to have a *multiple root* if there is some field E containing F and some $\alpha \in E$ such that $(x - \alpha)^2$ divides $f(x)$ in $E[x]$. For example, the polynomial $f(x) = (x - 1)^2(x - 2) \in \mathbb{Q}[x]$ has $\alpha = 1$ as a multiple root and the polynomial $f(x) = x^4 + 2x^2 + 1 = (x^2 + 1)^2 \in \mathbb{R}[x]$ has $\alpha = \pm i \in \mathbb{C}$ as multiple roots. We shall prove in Section 13.5 that a nonconstant polynomial $f(x)$ has a multiple root if and only if $f(x)$ is not relatively prime to its derivative (which can be detected by the Euclidean Algorithm in $F[x]$). Use this criterion to determine whether the following polynomials have multiple roots:

(a) $x^3 - 3x - 2 \in \mathbb{Q}[x]$

(b) $x^3 + 3x + 2 \in \mathbb{Q}[x]$

(c) $x^6 - 4x^4 + 6x^3 + 4x^2 - 12x + 9 \in \mathbb{Q}[x]$

(d) Show for any prime p and any $a \in \mathbb{F}_p$ that the polynomial $x^p - a$ has a multiple root.

20. Show that the polynomial $f(x) = x$ in $\mathbb{Z}/6\mathbb{Z}[x]$ factors as $(3x + 4)(4x + 3)$, hence is not an irreducible polynomial.

(a) Show that the reduction of $f(x)$ modulo both of the nontrivial ideals (2) and (3) of $\mathbb{Z}/6\mathbb{Z}$ is an irreducible polynomial, showing that the condition that R be an integral domain in Proposition 12 is necessary.

(b) Show that in any factorization $f(x) = g(x)h(x)$ in $\mathbb{Z}/6\mathbb{Z}[x]$ the reduction of $g(x)$ modulo (2) is either 1 or x and the reduction of $h(x)$ modulo (2) is then either x or 1, and similarly for the reductions modulo (3). Determine all the factorizations of $f(x)$ in $\mathbb{Z}/6\mathbb{Z}[x]$. [Use the Chinese Remainder Theorem.]

(c) Show that the ideal $(3, x)$ is a principal ideal in $\mathbb{Z}/6\mathbb{Z}[x]$.

(d) Show that over the ring $\mathbb{Z}/30\mathbb{Z}[x]$ the polynomial $f(x) = x$ has the factorization

$f(x) = (10x+21)(15x+16)(6x+25)$. Prove that the product of any of these factors is again of the same degree. Prove that the reduction of $f(x)$ modulo any prime in $\mathbb{Z}/30\mathbb{Z}$ is an irreducible polynomial. Determine all the factorizations of $f(x)$ in $\mathbb{Z}/30\mathbb{Z}[x]$. [Consider the reductions modulo (2), (3) and (5) and use the Chinese Remainder Theorem.]

(e) Generalize part (d) to $\mathbb{Z}/n\mathbb{Z}[x]$ where n is the product of k distinct primes.

9.5 POLYNOMIAL RINGS OVER FIELDS II

Let F be a field. We prove here some additional results for the one-variable polynomial ring $F[x]$. The first is a restatement of results obtained earlier.

Proposition 15. The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proof: This follows from Proposition 7 of Section 8.2 applied to the Principal Ideal Domain $F[x]$.

Proposition 16. Let $g(x)$ be a nonconstant element of $F[x]$ and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$$

be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then we have the following isomorphism of rings:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots \times F[x]/(f_k(x)^{n_k}).$$

Proof: This follows from the Chinese Remainder Theorem (Theorem 7.17), since the ideals $(f_i(x)^{n_i})$ and $(f_j(x)^{n_j})$ are comaximal if $f_i(x)$ and $f_j(x)$ are distinct (they are relatively prime in the Euclidean Domain $F[x]$, hence the ideal generated by them is $F[x]$).

The next result concerns the number of roots of a polynomial over a field F. By Proposition 9, a root α corresponds to a linear factor $(x-\alpha)$ of $f(x)$. If $f(x)$ is divisible by $(x-\alpha)^m$ but not by $(x-\alpha)^{m+1}$, then α is said to be a root of *multiplicity* m.

Proposition 17. If the polynomial $f(x)$ has roots $\alpha_1, \alpha_2, \ldots, \alpha_k$ in F (not necessarily distinct), then $f(x)$ has $(x-\alpha_1)\cdots(x-\alpha_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in F, even counted with multiplicity.

Proof: The first statement follows easily by induction from Proposition 9. Since linear factors are irreducible, the second statement follows since $F[x]$ is a Unique Factorization Domain.

This last result has the following interesting consequence.

Proposition 18. A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Proof: We give a proof of this result using the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 3 in Section 5.2). A more number-theoretic proof is outlined in the exercises, or Proposition 5 in Section 6.1 may be used in place of the Fundamental Theorem. By the Fundamental Theorem, the finite subgroup can be written as the direct product of cyclic groups

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

where $n_k \mid n_{k-1} \mid \cdots \mid n_2 \mid n_1$. In general, if G is a cyclic group and $d \mid |G|$ then G contains precisely d elements of order dividing d. Since n_k divides the order of each of the cyclic groups in the direct product, it follows that each direct factor contains n_k elements of order dividing n_k. If k were greater than 1, there would therefore be a total of more than n_k such elements. But then there would be more than n_k roots of the polynomial $x^{n_k} - 1$ in the field F, contradicting Proposition 17. Hence $k = 1$ and the group is cyclic.

Corollary 19. Let p be a prime. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes mod p is cyclic.

Proof: This is the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$.

Corollary 20. Let $n \geq 2$ be an integer with factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ in $\mathbb{Z}$, where $p_1, \ldots, p_r$ are distinct primes. We have the following isomorphisms of (multiplicative) groups:

(1) $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$

(2) $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$, for all $\alpha \geq 2$

(3) $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$, for all odd primes p.

Remark: These isomorphisms describe the group-theoretic structure of the automorphism group of the cyclic group, Z_n, of order n since $\mathrm{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ (cf. Proposition 16 in Section 4.4). In particular, for p a prime the automorphism group of the cyclic group of order p is cyclic of order $p-1$.

Proof: This is mainly a matter of collecting previous results. The isomorphism in (1) follows from the Chinese Remainder Theorem (see Corollary 18, Section 7.6). The isomorphism in (2) follows directly from Exercises 22 and 23 of Section 2.3.

For p an odd prime, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is an abelian group of order $p^{\alpha-1}(p-1)$. By Exercise 21 of Section 2.3 the Sylow p-subgroup of this group is cyclic. The map

$$\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \qquad \text{defined by} \qquad a + (p^\alpha) \mapsto a + (p)$$

is a ring homomorphism (reduction mod p) which gives a surjective group homomorphism from $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ onto $(\mathbb{Z}/p\mathbb{Z})^\times$. The latter group is cyclic of order $p-1$

(Corollary 19). The kernel of this map is of order $p^{\alpha-1}$, hence for all primes $q \neq p$, the Sylow q-subgroup of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ maps isomorphically into the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. All Sylow subgroups of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ are therefore cyclic, so (3) holds, completing the proof.

EXERCISES

1. Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Describe the nilradical of $F[x]/(f(x))$ in terms of the factorization of $f(x)$ (cf. Exercise 29, Section 7.3).
2. For each of the fields constructed in Exercise 6 of Section 4 exhibit a generator for the (cyclic) multiplicative group of nonzero elements.
3. Let p be an odd prime in $\mathbb{Z}$ and let n be a positive integer. Prove that $x^n - p$ is irreducible over $\mathbb{Z}[i]$. [Use Proposition 18 in Chapter 8 and Eisenstein's Criterion.]
4. Prove that $x^3 + 12x^2 + 18x + 6$ is irreducible over $\mathbb{Z}[i]$. [Use Proposition 8.18 and Eisenstein's Criterion.]
5. Let φ denote Euler's φ-function. Prove the identity $\sum_{d|n} \varphi(d) = n$, where the sum is extended over all the divisors d of n. [First observe that the identity is valid when $n = p^m$ is the power of a prime p since the sum telescopes. Write $n = p^m n'$ where p does not divide n'. Prove that $\sum_{d|n} \varphi(d) = \sum_{d''|p^m} \varphi(d'') \sum_{d'|n'} \varphi(d')$ by multiplying out the right hand side and using the multiplicativity $\varphi(ab) = \varphi(a)\varphi(b)$ when a and b are relatively prime. Use induction to complete the proof. This problem may be done alternatively by letting Z be the cyclic group of order n and showing that since Z contains a unique subgroup of order d for each d dividing n, the number of elements of Z of order d is $\varphi(d)$. Then $|Z|$ is the sum of $\varphi(d)$ as d runs over all divisors of n.]
6. Let G be a finite subgroup of order n of the multiplicative group $F^\times$ of nonzero elements of the field F. Let φ denote Euler's φ-function and let $\psi(d)$ denote the number of elements of G of order d. Prove that $\psi(d) = \varphi(d)$ for every divisor d of n. In particular conclude that $\psi(n) \geq 1$, so that G is a cyclic group. [Observe that for any integer $N \geq 1$ the polynomial $x^N - 1$ has at most N roots in F. Conclude that for any integer N we have $\sum_{d|N} \psi(d) \leq N$. Since $\sum_{d|N} \varphi(d) = N$ by the previous exercise, show by induction that $\psi(d) \leq \varphi(d)$ for every divisor d of n. Since $\sum_{d|n} \psi(d) = n = \sum_{d|n} \varphi(d)$ show that this implies $\psi(d) = \varphi(d)$ for every divisor d of n.]
7. Prove that the additive and multiplicative groups of a field are never isomorphic. [Consider three cases: when $|F|$ is finite, when $-1 \neq 1$ in F, and when $-1 = 1$ in F.]

9.6 POLYNOMIALS IN SEVERAL VARIABLES OVER A FIELD AND GRÖBNER BASES

In this section we consider polynomials in many variables, present some basic computational tools, and indicate some applications. The results of this section are not required in Chapters 10 through 14. Additional applications will be given in Chapter 15.

We proved in Section 2 that a polynomial ring $F[x]$ in a variable x over a field F is a Euclidean Domain, and Corollary 8 showed that the polynomial ring $F[x_1, \ldots, x_n]$ is a U.F.D. However it follows from Corollary 8 in Section 8.2 that the latter ring is not a P.I.D. unless $n = 1$. Our first result below shows that ideals in such polynomial rings, although not necessarily principal, are always finitely generated. General rings with this property are given a special name:

Definition. A commutative ring R with 1 is called *Noetherian* if every ideal of R is finitely generated.

Noetherian rings will be studied in greater detail in Chapters 15 and 16. In this section we develop some of the basic theory and resulting algorithms for working with (finitely generated) ideals in $F[x_1, \ldots, x_n]$.

As we saw in Section 1, a polynomial ring in n variables can be considered as a polynomial ring in one variable with coefficients in a polynomial ring in $n-1$ variables. By following this inductive approach—as we did in Theorem 7 and Corollary 8—we can deduce that $F[x_1, x_2, \ldots, x_n]$ is Noetherian from the following more general result.

Theorem 21. *(Hilbert's Basis Theorem)* If R is a Noetherian ring then so is the polynomial ring $R[x]$.

Proof: Let I be an ideal in $R[x]$ and let L be the set of all leading coefficients of the elements in I. We first show that L is an ideal of R, as follows. Since I contains the zero polynomial, $0 \in L$. Let $f = ax^d + \cdots$ and $g = bx^e + \cdots$ be polynomials in I of degrees d, e and leading coefficients $a, b \in R$. Then for any $r \in R$ either $ra - b$ is zero or it is the leading coefficient of the polynomial $rx^e f - x^d g$. Since the latter polynomial is in I we have $ra - b \in L$, which shows L is an ideal of R. Since R is assumed Noetherian, the ideal L in R is finitely generated, say by $a_1, a_2, \ldots, a_n \in R$. For each $i = 1, \ldots, n$ let f_i be an element of I whose leading coefficient is a_i. Let e_i denote the degree of f_i, and let N be the maximum of $e_1, e_2, \ldots, e_n$.

For each $d \in \{0, 1, \ldots, N-1\}$, let L_d be the set of all leading coefficients of polynomials in I of degree d together with 0. A similar argument as that for L shows each L_d is also an ideal of R, again finitely generated since R is Noetherian. For each nonzero ideal L_d let $b_{d,1}, b_{d,2}, \ldots, b_{d,n_d} \in R$ be a set of generators for L_d, and let $f_{d,i}$ be a polynomial in I of degree d with leading coefficient $b_{d,i}$.

We show that the polynomials $f_1, \ldots, f_n$ together with all the polynomials $f_{d,i}$ for all the nonzero ideals L_d are a set of generators for I, i.e., that

$$I = (\{f_1, \ldots, f_n\} \cup \{f_{d,i} \mid 0 \le d < N,\ 1 \le i \le n_d\}).$$

By construction, the ideal I' on the right above is contained in I since all the generators were chosen in I. If $I' \neq I$, there exists a nonzero polynomial $f \in I$ of minimum degree with $f \notin I'$. Let $d = \deg f$ and let a be the leading coefficient of f.

Suppose first that $d \ge N$. Since $a \in L$ we may write a as an R-linear combination of the generators of L: $a = r_1 a_1 + \cdots + r_n a_n$. Then $g = r_1 x^{d-e_1} f_1 + \cdots + r_n x^{d-e_n} f_n$ is an element of I' with the same degree d and the same leading coefficient a as f. Then $f - g \in I$ is a polynomial in I of smaller degree than f. By the minimality of f, we must have $f - g = 0$, so $f = g \in I'$, a contradiction.

Suppose next that $d < N$. In this case $a \in L_d$ for some $d < N$, and so we may write $a = r_1 b_{d,1} + \cdots + r_{n_d} b_{n_d}$ for some $r_i \in R$. Then $g = r_1 f_{d,1} + \cdots + r_{n_d} f_{n_d}$ is a polynomial in I' with the same degree d and the same leading coefficient a as f, and we have a contradiction as before.

It follows that $I = I'$ is finitely generated, and since I was arbitrary, this completes the proof that $R[x]$ is Noetherian.

Since a field is clearly Noetherian, Hilbert's Basis Theorem and induction immediately give:

Corollary 22. Every ideal in the polynomial ring $F[x_1, x_2, \ldots, x_n]$ with coefficients from a field F is finitely generated.

If I is an ideal in $F[x_1, \ldots, x_n]$ generated by a (possibly infinite) set $\mathcal{S}$ of polynomials, Corollary 22 shows that I is finitely generated, and in fact I is generated by a finite number of the polynomials from the set $\mathcal{S}$ (cf. Exercise 1).

As the proof of Hilbert's Basis Theorem shows, the collection of leading coefficients of the polynomials in an ideal I in $R[x]$ forms an extremely useful ideal in R that can be used to understand I. This suggests studying "leading terms" in $F[x_1, x_2, \ldots, x_n]$ more generally (and somewhat more intrinsically). To do this we need to specify a total ordering on the monomials, since without some sort of ordering we cannot in general tell which is the "leading" term of a polynomial. We implicitly chose such an ordering in the inductive proof of Corollary 22—we first viewed a polynomial f as a polynomial in x_1 with coefficients in $R = F[x_2, \ldots, x_n]$, say, then viewed its "leading coefficient" in $F[x_2, \ldots, x_n]$ as a polynomial in x_2 with coefficients in $F[x_3, \ldots, x_n]$, etc. This is an example of a *lexicographic* monomial ordering on the polynomial ring $F[x_1, \ldots, x_n]$ which is defined by first declaring an ordering of the variables, for example $x_1 > x_2 > \cdots > x_n$ and then declaring that the monomial term $Ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ with exponents $(a_1, a_2, \ldots, a_n)$ has higher order than the monomial term $Bx_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ with exponents $(b_1, b_2, \ldots, b_n)$ if the first component where the n-tuples differ has $a_i > b_i$. This is analogous to the ordering used in a dictionary (hence the name), where the letter "a" comes before "b" which in turn comes before "c", etc., and then "aardvark" comes before "abacus" (although the 'word' $a^2 = aa$ comes before a in the lexicographical order). Note that the ordering is only defined up to multiplication by units (elements of $F^\times$) and that multiplying two monomials by the same nonzero monomial does not change their ordering. This can be formalized in general.

Definition. A *monomial ordering* is a well ordering "$\geq$" on the set of monomials that satisfies $mm_1 \geq mm_2$ whenever $m_1 \geq m_2$ for monomials m, m_1, m_2. Equivalently, a monomial ordering may be specified by defining a well ordering on the n-tuples $\alpha = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ of multidegrees of monomials $Ax_1^{a_1} \cdots x_n^{a_n}$ that satisfies $\alpha + \gamma \geq \beta + \gamma$ if $\alpha \geq \beta$.

It is easy to show for any monomial ordering that $m \geq 1$ for every monomial m (cf. Exercise 2). It is not difficult to show, using Hilbert's Basis Theorem, that any total ordering on monomials which for every monomial m satisfies $m \geq 1$ and $mm_1 \geq mm_2$ whenever $m_1 \geq m_2$, is necessarily a well ordering (hence a monomial ordering)—this equivalent set of axioms for a monomial ordering may be easier to verify. For simplicity we shall limit the examples to the particularly easy and intuitive lexicographic ordering, but it is important to note that there are useful computational advantages to using other monomial orderings in practice. Some additional commonly used monomial orderings are introduced in the exercises.

As mentioned, once we have a monomial ordering we can define the leading term of a polynomial:

Definition. Fix a monomial ordering on the polynomial ring $F[x_1, x_2, \ldots, x_n]$.

(1) The *leading term* of a nonzero polynomial f in $F[x_1, x_2, \ldots, x_n]$, denoted $LT(f)$, is the monomial term of maximal order in f and the leading term of $f = 0$ is 0. Define the *multidegree of* f, denoted $\partial(f)$, to be the multidegree of the leading term of f.

(2) If I is an ideal in $F[x_1, x_2, \ldots, x_n]$, the *ideal of leading terms*, denoted $LT(I)$, is the ideal generated by the leading terms of all the elements in the ideal, i.e., $LT(I) = (LT(f) \mid f \in I)$.

The leading term and the multidegree of a polynomial clearly depend on the choice of the ordering. For example $LT(2xy + y^3) = 2xy$ with multidegree $(1, 1)$ if $x > y$, but $LT(2xy + y^3) = y^3$ with multidegree $(0, 3)$ if $y > x$. In particular, the leading term of a polynomial need not be the term of largest total degree. Similarly, the ideal of leading terms $LT(I)$ of an ideal I in general depends on the ordering used. Note also that the multidegree of a polynomial satisfies $\partial(fg) = \partial f + \partial g$ when f and g are nonzero, and that in this case $LT(fg) = LT(f) + LT(g)$ (cf. Exercise 2).

The ideal $LT(I)$ is by definition generated by monomials. Such ideals are called *monomial ideals* and are typically much easier to work with than generic ideals. For example, a polynomial is contained in a monomial ideal if and only if each of its monomial terms is a multiple of one of the generators for the ideal (cf. Exercise 10).

It was important in the proof of Hilbert's Basis Theorem to have *all* of the leading terms of the ideal I. If $I = (f_1, \ldots, f_m)$, then $LT(I)$ contains the leading terms $LT(f_1), \ldots, LT(f_m)$ of the generators for I by definition. Since $LT(I)$ is an ideal, it contains the ideal generated by these leading terms:

$$(LT(f_1), \ldots, LT(f_m)) \subseteq LT(I).$$

The first of the following examples shows that the ideal $LT(I)$ of leading terms can in general be strictly larger than the ideal generated just by the leading terms of some generators for I.

Examples

(1) Choose the lexicographic ordering $x > y$ on $F[x, y]$. The leading terms of the polynomials $f_1 = x^3y - xy^2 + 1$ and $f_2 = x^2y^2 - y^3 - 1$ are $LT(f_1) = x^3y$ (so the multidegree of f_1 is $\partial(f_1) = (3, 1)$) and $LT(f_2) = x^2y^2$ (so $\partial(f_2) = (2, 2)$). If $I = (f_1, f_2)$ is the ideal generated by f_1 and f_2 then the leading term ideal $LT(I)$ contains $LT(f_1) = x^3y$ and $LT(f_2) = x^2y^2$, so $(x^3y, x^2y^2) \subseteq LT(I)$. Since

$$yf_1 - xf_2 = y(x^3y - xy^2 + 1) - x(x^2y^2 - y^3 - 1) = x + y$$

we see that $g = x + y$ is an element of I and so the ideal $LT(I)$ also contains the leading term $LT(g) = x$. This shows that $LT(I)$ is strictly larger than $(LT(f_1), LT(f_2))$, since every element in $(LT(f_1), LT(f_2)) = (x^3y, x^2y^2)$ has total degree at least 4. We shall see later that in this case $LT(I) = (x, y^4)$.

(2) With respect to the lexicographic ordering $y > x$, the leading terms of f_1 and f_2 in the previous example are $LT(f_1) = -xy^2$ (which one could write as $-y^2x$ to emphasize the chosen ordering) and $LT(f_2) = -y^3$. We shall see later that in this ordering $LT(I) = (x^4, y)$, which is a different ideal than the ideal $LT(I)$ obtained in the previous example using the ordering $x > y$, and is again strictly larger than $(LT(f_1), LT(f_2))$.

(3) Choose any ordering on $F[x, y]$ and let $f = f(x, y)$ be any nonzero polynomial. The leading term of every element of the principal ideal $I = (f)$ is then a multiple of the leading term of f, so in this case $LT(I) = (LT(f))$.

In the case of one variable, leading terms are used in the Division Algorithm to reduce one polynomial g modulo another polynomial f to get a unique remainder r, and this remainder is 0 if and only if g is contained in the ideal (f). Since $F[x_1, x_2, \ldots, x_n]$ is not a Euclidean Domain if $n \geq 2$ (since it is not a P.I.D.), the situation is more complicated for polynomials in more than one variable. In the first example above, neither f_1 nor f_2 divides g in $F[x, y]$ (by degree considerations, for example), so attempting to first divide g by one of f_1 or f_2 and then by the other to try to reduce g modulo the ideal I would produce a (nonzero) "remainder" of g itself. In particular, this would suggest that $g = yf_1 - xf_2$ is not an element of the ideal I even though it is. The reason the polynomial g of degree 1 can be a linear combination of the two polynomials f_1 and f_2 of degree 4 is that the leading terms in yf_1 and xf_2 cancel in the difference, and this is reflected in the fact that $LT(f_1)$ and $LT(f_2)$ are not sufficient to generate $LT(I)$. A set of generators for an ideal I in $F[x_1, \ldots, x_n]$ whose leading terms generate the leading terms of *all* the elements in I is given a special name.

Definition. A *Gröbner basis* for an ideal I in the polynomial ring $F[x_1, \ldots, x_n]$ is a finite set of generators $\{g_1, \ldots, g_m\}$ for I whose leading terms generate the ideal of all leading terms in I, i.e.,

$$I = (g_1, \ldots, g_m) \quad \text{and} \quad LT(I) = (LT(g_1), \ldots, LT(g_m)).$$

Remark: Note that a Gröbner "basis" is in fact a set of *generators* for I (that depends on the choice of ordering), i.e., every element in I is a linear combination of the generators, and not a basis in the sense of vector spaces (where the linear combination would be *unique*, cf. Sections 10.3 and 11.1). Although potentially misleading, the terminology "Gröbner basis" has been so widely adopted that it would be hazardous to introduce a different nomenclature.

One of the most important properties of a Gröbner basis (proved in Theorem 23 following) is that every polynomial g can be written *uniquely* as the sum of an element in I and a remainder r obtained by a general polynomial division. In particular, we shall see that g is an element of I if and only if this remainder r is 0. While there is a similar decomposition in general, we shall see that if we do not use a Gröbner basis the uniqueness is lost (and we cannot detect membership in I by checking whether the remainder is 0) because there are leading terms not accounted for by the leading terms of the generators.

We first use the leading terms of polynomials defined by a monomial ordering on $F[x_1, \ldots, x_n]$ to extend the one variable Division Algorithm to a noncanonical polynomial division in several variables. Recall that for polynomials in one variable, the usual Division Algorithm determines the quotient $q(x)$ and remainder $r(x)$ in the equation $f(x) = q(x)g(x) + r(x)$ by successively testing whether the leading term of the dividend $f(x)$ is divisible by the leading term of $g(x)$: if $LT(f) = a(x)LT(g)$, the monomial term $a(x)$ is added to the quotient and the process is iterated with $f(x)$ replaced by the dividend $f(x) - a(x)g(x)$, which is of smaller degree since the leading terms cancel (by the choice of $a(x)$). The process terminates when the leading term of the divisor $g(x)$ no longer divides the leading term of the dividend, leaving the remainder $r(x)$. We can extend this to division by a finite number of polynomials in several variables simply by allowing successive divisions, resulting in a remainder and several quotients, as follows.

General Polynomial Division

Fix a monomial ordering on $F[x_1, \ldots, x_n]$, and suppose $g_1, \ldots, g_m$ is a set of nonzero polynomials in $F[x_1, \ldots, x_n]$. If f is any polynomial in $F[x_1, \ldots, x_n]$, start with a set of quotients $q_1, \ldots, q_m$ and a remainder r initially all equal to 0 and successively test whether the leading term of the dividend f is divisible by the leading terms of the divisors $g_1, \ldots, g_m$, in that order. Then

i. If $LT(f)$ is divisible by $LT(g_i)$, say, $LT(f) = a_i LT(g_i)$, add a_i to the quotient q_i, replace f by the dividend $f - a_i g_i$ (a polynomial with lower order leading term), and reiterate the entire process.

ii. If the leading term of the dividend f is not divisible by any of the leading terms $LT(g_1), \ldots, LT(g_m)$, add the leading term of f to the remainder r, replace f by the dividend $f - LT(f)$ (i.e., remove the leading term of f), and reiterate the entire process.

The process terminates (cf. Exercise 3) when the dividend is 0 and results in a set of quotients $q_1, \ldots, q_m$ and a remainder r with

$$f = q_1 g_1 + \cdots + q_m g_m + r.$$

Each $q_i g_i$ has multidegree less than or equal to the multidegree of f and the remainder r has the property that no nonzero term in r is divisible by any of the leading terms $LT(g_1), \ldots, LT(g_m)$ (since only terms with this property are added to r in (ii)).

Examples

Fix the lexicographic ordering $x > y$ on $F[x, y]$.

(1) Suppose $f = x^3y^3 + 3x^2y^4$ and $g = xy^4$. The leading term of f is x^3y^3, which is not divisible by (the leading term of) g, so x^3y^3 is added to the remainder r (so now $r = x^3y^3$) and f is replaced by $f - LT(f) = 3x^2y^4$ and we start over. Since $3x^2y^4$ is divisible by $LT(g) = xy^4$, with quotient $a = 3x$, we add $3x$ to the quotient q (so $q = 3x$), and replace $3x^2y^4$ by $3x^2y^4 - aLT(g) = 0$, at which point the process terminates. The result is the quotient $q = 3x$ and remainder $r = x^3y^3$ and

$$x^3y^3 + 3x^2y^4 = f = qg + r = (3x)(xy^4) + x^3y^3.$$

Note that if we had terminated at the first step because the leading term of f is not divisible by the leading term of g (which terminates the Division Algorithm for polynomials in one variable), then we would have been left with a 'remainder' of f itself, even though 'more' of f is divisible by g. This is the reason for step 2 in the division process (which is not necessary for polynomials in one variable).

(2) Let $f = x^2+x-y^2+y$, and suppose $g_1 = xy+1$ and $g_2 = x+y$. In the first iteration, the leading term x^2 of f is not divisible by the leading term of g_1, but is divisible by the leading term of g_2, so the quotient q_2 is x and the dividend f is replaced by the dividend $f - xg_2 = -xy + x - y^2 + y$. In the second iteration, the leading term of $-xy + x - y^2 + y$ is divisible by $LT(g_1)$, with quotient -1, so $q_1 = -1$ and the dividend is replaced by $(-xy + x - y^2 + y) - (-1)g_1 = x - y^2 + y + 1$. In the third iteration, the leading term of $x - y^2 + y + 1$ is not divisible by the leading term of g_1, but is divisible by the leading term of g_2, with quotient 1, so 1 is added to q_2 (which is now $q_2 = x+1$) and the dividend becomes $(x - y^2 + y + 1) - (1)(g_2) = -y^2 + 1$. The leading term is now $-y^2$, which is not divisible by either $LT(g_1) = xy$ or $LT(g_2) = x$, so $-y^2$ is added to the remainder r (which is now $-y^2$) and the dividend becomes simply 1. Finally, 1 is not divisible by either $LT(g_1)$ or $LT(g_2)$, so is added to the remainder (so r is now $-y^2 + 1$), and the process terminates. The result is

$$q_1 = -1, \qquad q_2 = x + 1, \qquad r = -y^2 + 1 \quad \text{and}$$

$$\begin{aligned} f = x^2 + x - y^2 + y &= (-1)(xy + 1) + (x + 1)(x + y) + (-y^2 + 1) \\ &= q_1 g_1 + q_2 g_2 + r. \end{aligned}$$

(3) Let $f = x^2 + x - y^2 + y$ as in the previous example and interchange the divisors g_1 and g_2: $g_1 = x + y$ and $g_2 = xy + 1$. In this case an easy computation gives

$$q_1 = x - y + 1, \qquad q_2 = 0, \qquad r = 0 \quad \text{and}$$

$$f = x^2 + x - y^2 + y = (x - y + 1)(x + y) = q_1 g_1 + q_2 g_2 + r,$$

showing that the quotients q_i and the remainder r are in general not unique and depend on the order of the divisors $g_1, \ldots, g_m$.

The computation in Example 3 shows that the polynomial $f = x^2 + x - y^2 + y$ is an element of the ideal $I = (x + y, xy + 1)$ since the remainder obtained in this case was 0 (in fact f is just a multiple of the first generator). In Example 2, however, the same polynomial resulted in a nonzero remainder $-y^2 + 1$ when divided by $xy + 1$ and $x + y$, and it was not at all clear from that computation that f was an element of I.

The next theorem shows that if we use a Gröbner basis for the ideal I then these difficulties do not arise: we obtain a *unique* remainder, which in turn can be used to determine whether a polynomial f is an element of the ideal I.

Theorem 23. Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and suppose $\{g_1, \ldots, g_m\}$ is a Gröbner basis for the nonzero ideal I in R. Then

(1) Every polynomial $f \in R$ can be written uniquely in the form

$$f = f_I + r$$

where $f_I \in I$ and no nonzero monomial term of the 'remainder' r is divisible by any of the leading terms $LT(g_1), \ldots, LT(g_m)$.

(2) Both f_I and r can be computed by general polynomial division by $g_1, \ldots, g_m$ and are independent of the order in which these polynomials are used in the division.

(3) The remainder r provides a unique representative for the coset of f in the quotient ring $F[x_1, \ldots, x_n]/I$. In particular, $f \in I$ if and only if $r = 0$.

Proof: Letting $f_I = \sum_{i=1}^m q_i g_i \in I$ in the general polynomial division of f by $g_1, \ldots, g_m$ immediately gives a decomposition $f = f_I + r$ for any generators $g_1, \ldots, g_m$. Suppose now that $\{g_1, \ldots, g_m\}$ is a Gröbner basis, and $f = f_I + r = f_I' + r'$. Then $r - r' = f_I' - f_I \in I$, so its leading term $LT(r - r')$ is an element of $LT(I)$, which is the ideal $(LT(g_1), \ldots, LT(g_m))$ since $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I. Every element in this ideal is a sum of multiples of the monomial terms $LT(g_1), \ldots, LT(g_m)$, so is a sum of terms each of which is divisible by one of the $LT(g_i)$. But both r and r', hence also $r - r'$, are sums of monomial terms none of which is divisible by $LT(g_1), \ldots, LT(g_m)$, which is a contradiction unless $r - r' = 0$. It follows that $r = r'$ is unique, hence so is $f_I = f - r$, which proves (1).

We have already seen that f_I and r can be computed algorithmically by polynomial division, and the uniqueness in (1) implies that r is independent of the order in which the polynomials $g_1, \ldots, g_m$ are used in the division. Similarly $f_I = \sum_{i=1}^m q_i g_i$ is uniquely determined (even though the individual quotients q_i are not in general unique), which gives (2).

The first statement in (3) is immediate from the uniqueness in (1). If $r = 0$, then $f = f_I \in I$. Conversely, if $f \in I$, then $f = f + 0$ together with the uniqueness of r implies that $r = 0$, and the final statement of the theorem follows.

As previously mentioned, the importance of Theorem 23, and one of the principal uses of Gröbner bases, is the uniqueness of the representative r, which allows effective computation in the quotient ring $F[x_1, \ldots, x_n]/I$.

We next prove that a set of polynomials in an ideal whose leading terms generate all the leading terms of an ideal is in fact a set of generators for the ideal itself (and so is a Gröbner basis—in some works this is taken as the definition of a Gröbner basis), and this shows in particular that a Gröbner basis always exists.

Proposition 24. Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and let I be a nonzero ideal in R.

(1) If $g_1, \ldots, g_m$ are any elements of I such that $LT(I) = (LT(g_1), \ldots, LT(g_m))$, then $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I.

(2) The ideal I has a Gröbner basis.

Proof: Suppose $g_1, \ldots, g_m \in I$ with $LT(I) = (LT(g_1), \ldots, LT(g_m))$. We need to see that $g_1, \ldots, g_m$ generate the ideal I. If $f \in I$, use general polynomial division to write $f = \sum_{i=1}^m q_i g_i + r$ where no nonzero term in the remainder r is divisible by any $LT(g_i)$. Since $f \in I$, also $r \in I$, which means $LT(r)$ is in $LT(I)$. But then $LT(r)$ would be divisible by one of $LT(g_1), \ldots, LT(g_m)$, which is a contradiction unless $r = 0$. Hence $f = \sum_{i=1}^m q_i g_i$ and $g_1, \ldots, g_m$ generate I, so are a Gröbner basis for I, which proves (1).

For (2), note that the ideal $LT(I)$ of leading terms of any ideal I is a monomial ideal generated by all the leading terms of the polynomials in I. By Exercise 1 a finite number of those leading terms suffice to generate $LT(I)$, say $LT(I) = (LT(h_1), \ldots, LT(h_k))$ for some $h_1, \ldots, h_k \in I$. By (1), the polynomials $h_1, \ldots, h_k$ are a Gröbner basis of I, completing the proof.

Proposition 24 proves that Gröbner bases always exist. We next prove a criterion that determines whether a given set of generators of an ideal I is a Gröbner basis, which we then use to provide an algorithm to find a Gröbner basis. The basic idea is very simple: additional elements in $LT(I)$ can arise by taking linear combinations of generators that cancel leading terms, as we saw in taking $yf_1 - xf_2$ in the first example in this section. We shall see that obtaining new leading terms from generators in this simple manner is the only obstruction to a set of generators being a Gröbner basis.

In general, if f_1, f_2 are two polynomials in $F[x_1, \ldots, x_n]$ and M is the monic least common multiple of the monomial terms $LT(f_1)$ and $LT(f_2)$ then we can cancel the leading terms by taking the difference

$$S(f_1, f_2) = \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2. \tag{9.1}$$

The next lemma shows that these elementary linear combinations account for all cancellation in leading terms of polynomials of the same multidegree.

Lemma 25. Suppose $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ are polynomials with the same multidegree α and that the linear combination $h = a_1 f_1 + \cdots + a_m f_m$ with constants $a_i \in F$ has strictly smaller multidegree. Then

$$h = \sum_{i=2}^{m} b_i S(f_{i-1}, f_i), \quad \text{for some constants } b_i \in F.$$

Proof: Write $f_i = c_i f_i'$ where $c_i \in F$ and f_i' is a monic polynomial of multidegree α. We have

$$h = \sum a_i c_i f_i' = a_1 c_1 (f_1' - f_2') + (a_1 c_1 + a_2 c_2)(f_2' - f_3') + \cdots$$
$$+ (a_1 c_1 + \cdots + a_{m-1} c_{m-1})(f_{m-1}' - f_m') + (a_1 c_1 + \cdots + a_m c_m) f_m'.$$

Note that $f_{i-1}' - f_i' = S(f_{i-1}, f_i)$. Then since h and each $f_{i-1}' - f_i'$ has multidegree strictly smaller than α, we have $a_1 c_1 + \cdots + a_m c_m = 0$, so the last term on the right hand side is 0 and the lemma follows.

The next proposition shows that a set of generators $g_1, \ldots, g_m$ is a Gröbner basis if there are no new leading terms among the differences $S(g_i, g_j)$ not already accounted for by the g_i. This result provides the principal ingredient in an algorithm to construct a Gröbner basis.

For a fixed monomial ordering on $R = F[x_1, \ldots, x_n]$ and ordered set of polynomials $G = \{g_1, \ldots, g_m\}$ in R, write $f \equiv r \bmod G$ if r is the remainder obtained by general polynomial division of $f \in R$ by $g_1, \ldots, g_m$ (in that order).

Proposition 26. *(Buchberger's Criterion)* Let $R = F[x_1, \ldots, x_n]$ and fix a monomial ordering on R. If $I = (g_1, \ldots, g_m)$ is a nonzero ideal in R, then $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I if and only if $S(g_i, g_j) \equiv 0 \bmod G$ for $1 \leq i < j \leq m$.

Proof: If $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I, then $S(g_i, g_j) \equiv 0 \bmod G$ by Theorem 23 since each $S(g_i, g_j)$ is an element of I.

Suppose now that $S(g_i, g_j) \equiv 0 \bmod G$ for $1 \leq i < j \leq m$ and take any element $f \in I$. To see that G is a Gröbner basis we need to see that $(LT(g_1), \ldots, LT(g_m))$ contains $LT(f)$. Since $f \in I$, we can write $f = \sum_{i=1}^{m} h_i g_i$ for some polynomials $h_1, \ldots, h_m$. Such a representation is not unique. Among all such representations choose one for which the largest multidegree of any summand (i.e., $\max_{i=1,\ldots,m} \partial(h_i g_i)$) is minimal, say α. It is clear that the multidegree of f is no worse than the largest multidegree of all the summands $h_i g_i$, so $\partial(f) \leq \alpha$. Write

$$\begin{aligned} f = \sum_{i=1}^{m} h_i g_i &= \sum_{\partial(h_i g_i)=\alpha} h_i g_i + \sum_{\partial(h_i g_i)<\alpha} h_i g_i \\ &= \sum_{\partial(h_i g_i)=\alpha} LT(h_i) g_i + \sum_{\partial(h_i g_i)=\alpha} (h_i - LT(h_i)) g_i + \sum_{\partial(h_i g_i)<\alpha} h_i g_i. \end{aligned} \tag{9.2}$$

Suppose that $\partial(f) < \alpha$. Then since the multidegree of the second two sums is also strictly smaller than α it follows that the multidegree of the first sum is strictly smaller than α. If $a_i \in F$ denotes the constant coefficient of the monomial term $LT(h_i)$ then $LT(h_i) = a_i h_i'$ where h_i' is a monomial. We can apply Lemma 25 to $\sum a_i(h_i' g_i)$ to write the first sum above as $\sum b_i S(h_{i-1}' g_{i-1}, h_i' g_i)$ with $\partial(h_{i-1}' g_{i-1}) = \partial(h_i' g_i) = \alpha$. Let $\beta_{i-1,i}$ be the multidegree of the monic least common multiple of $LT(g_{i-1})$ and $LT(g_i)$. Then an easy computation shows that $S(h_{i-1}' g_{i-1}, h_i' g_i)$ is just $S(g_{i-1}, g_i)$ multiplied by the monomial of multidegree $\alpha - \beta_{i-1,i}$. The polynomial $S(g_{i-1}, g_i)$ has multidegree less than $\beta_{i-1,i}$ and, by assumption, $S(g_{i-1}, g_i) \equiv 0 \bmod G$. This means that after general polynomial division of $S(g_{i-1}, g_i)$ by $g_1, \ldots, g_m$, each $S(g_{i-1}, g_i)$ can be written as a sum $\sum q_j g_j$ with $\partial(q_j g_j) < \beta_{i-1,i}$. It follows that each $S(h_{i-1}' g_{i-1}, h_i' g_i)$ is a sum $\sum q_j' g_j$ with $\partial(q_j' g_j) < \alpha$. But then all the sums on the right hand side of equation (2) can be written as a sum of terms of the form $p_i g_i$ with polynomials p_i satisfying $\partial(p_i g_i) < \alpha$. This contradicts the minimality of α and shows that in fact $\partial(f) = \alpha$, i.e., the leading term of f has multidegree α.

If we now take the terms in equation (2) of multidegree α we see that

$$LT(f) = \sum_{\partial(h_i g_i)=\alpha} LT(h_i) LT(g_i),$$

so indeed $LT(f) \in (LT(g_1), \ldots, LT(g_m))$. It follows that $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis.

Buchberger's Algorithm

Buchberger's Criterion can be used to provide an algorithm to find a Gröbner basis for an ideal I, as follows. If $I = (g_1, \ldots, g_m)$ and each $S(g_i, g_j)$ leaves a remainder of 0 when divided by $G = \{g_1, \ldots, g_m\}$ using general polynomial division then G

is a Gröbner basis. Otherwise $S(g_i, g_j)$ has a nonzero remainder r. Increase G by appending the polynomial $g_{m+1} = r$: $G' = \{g_1, \ldots, g_m, g_{m+1}\}$ and begin again (note that this is again a set of generators for I since $g_{m+1} \in I$). It is not hard to check that this procedure terminates after a finite number of steps in a generating set G that satisfies Buchberger's Criterion, hence is a Gröbner basis for I (cf. Exercise 16). Note that once an $S(g_i, g_j)$ yields a remainder of 0 after division by the polynomials in G it also yields a remainder of 0 when additional polynomials are appended to G.

If $\{g_1, \ldots, g_m\}$ is a Gröbner basis for the ideal I and $LT(g_j)$ is divisible by $LT(g_i)$ for some $j \neq i$, then $LT(g_j)$ is not needed as a generator for $LT(I)$. By Proposition 24 we may therefore delete g_j and still retain a Gröbner basis for I. We may also assume without loss that the leading term of each g_i is monic. A Gröbner basis $\{g_1, \ldots, g_m\}$ for I where each $LT(g_i)$ is monic and where $LT(g_j)$ is not divisible by $LT(g_i)$ for $i \neq j$ is called a *minimal Gröbner basis.* While a minimal Gröbner basis is not unique, the number of elements and their leading terms are unique (cf. Exercise 15).

Examples

(1) Choose the lexicographic ordering $x > y$ on $F[x, y]$ and consider the ideal I generated by $f_1 = x^3y - xy^2 + 1$ and $f_2 = x^2y^2 - y^3 - 1$ as in Example 1 at the beginning of this section. To test whether $G = \{f_1, f_2\}$ is a Gröbner basis we compute $S(f_1, f_2) = yf_1 - xf_2 = x + y$, which is its own remainder when divided by $\{f_1, f_2\}$, so G is not a Gröbner basis for I. Set $f_3 = x + y$, and increase the generating set: $G' = \{f_1, f_2, f_3\}$. Now $S(f_1, f_2) \equiv 0 \bmod G'$, and a brief computation yields

$$S(f_1, f_3) = f_1 - x^2yf_3 = -x^2y^2 - xy^2 + 1 \equiv 0 \bmod G'$$

$$S(f_2, f_3) = f_2 - xy^2f_3 = -xy^3 - y^3 - 1 \equiv y^4 - y^3 - 1 \bmod G'.$$

Let $f_4 = y^4 - y^3 - 1$ and increase the generating set to $G'' = \{f_1, f_2, f_3, f_4\}$. The previous 0 remainder is still 0, and now $S(f_2, f_3) \equiv 0 \bmod G''$ by the choice of f_4. Some additional computation yields

$$S(f_1, f_4) \equiv S(f_2, f_4) \equiv S(f_3, f_4) \equiv 0 \bmod G''$$

and so $\{x^3y - xy^2 + 1, x^2y^2 - y^3 - 1, x + y, y^4 - y^3 - 1\}$ is a Gröbner basis for I. In particular, $LT(I)$ is generated by the leading terms of these four polynomials, so $LT(I) = (x^3y, x^2y^2, x, y^4) = (x, y^4)$, as previously mentioned. Then $x + y$ and $y^4 - y^3 - 1$ in I have leading terms generating $LT(I)$, so by Proposition 24, $\{x + y, y^4 - y^3 - 1\}$ gives a minimal Gröbner basis for I:

$$I = (x + y, y^4 - y^3 - 1).$$

This description of I is much simpler than $I = (x^3y - xy^2 + 1, x^2y^2 - y^3 - 1)$.

(2) Choose the lexicographic ordering $y > x$ on $F[x, y]$ and consider the ideal I in the previous example. In this case, $S(f_1, f_2)$ produces a remainder of $f_3 = -x - y$; then $S(f_1, f_3)$ produces a remainder of $f_4 = -x^4 - x^3 + 1$, and then all remainders are 0 with respect to the Gröbner basis $\{x^3y - xy^2 + 1, x^2y^2 - y^3 - 1, -x - y, -x^4 - x^3 + 1\}$. Here $LT(I) = (-xy^2, -y^3, -y, -x^4) = (y, x^4)$, as previously mentioned, and $\{x + y, x^4 + x^3 - 1\}$ gives a minimal Gröbner basis for I with respect to this ordering:

$$I = (x + y, x^4 + x^3 - 1),$$

a different simpler description of I.

In Example 1 above it is easy to check that $\{x+y^4-y^3+y-1,\ y^4-y^3-1\}$ is again a minimal Gröbner basis for I (this is just $\{f_3+f_4,\ f_4\}$), so even with a fixed monomial ordering on $F[x_1, \ldots, x_n]$ a minimal Gröbner basis for an ideal I is not unique. We can obtain an important uniqueness property by strengthening the condition on divisibility by the leading terms of the basis.

Definition. Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$. A Gröbner basis $\{g_1, \ldots, g_m\}$ for the nonzero ideal I in R is called a *reduced Gröbner basis* if

(a) each g_i has monic leading term, i.e., $LT(g_i)$ is monic, $i = 1, \ldots, m$, and

(b) no term in g_j is divisible by $LT(g_i)$ for $j \neq i$.

Note that a reduced Gröbner basis is, in particular, a minimal Gröbner basis. If $G = \{g_1, \ldots, g_m\}$ is a minimal Gröbner basis for I, then the leading term $LT(g_j)$ is not divisible by $LT(g_i)$ for any $i \neq j$. As a result, if we use polynomial division to divide g_j by the other polynomials in G we obtain a remainder g_j' in the ideal I with the same leading term as g_j (the remainder g_j' does not depend on the order of the polynomials used in the division by (2) of Theorem 23). By Proposition 24, replacing g_j by g_j' in G again gives a minimal Gröbner basis for I, and in this basis no term of g_j' is divisible by $LT(g_i)$ for any $i \neq j$. Replacing each element in G by its remainder after division by the other elements in G therefore results in a reduced Gröbner basis for I. The importance of reduced Gröbner bases is that they are unique (for a given monomial ordering), as the next result shows.

Theorem 27. Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$. Then there is a unique reduced Gröbner basis for every nonzero ideal I in R.

Proof: By Exercise 15, two reduced bases have the same number of elements and the same leading terms since reduced bases are also minimal bases. If $G = \{g_1, \ldots, g_m\}$ and $G' = \{g_1', \ldots, g_m'\}$ are two reduced bases for the same nonzero ideal I, then after a possible rearrangement we may assume $LT(g_i) = LT(g_i') = h_i$ for $i = 1, \ldots, m$. For any fixed i, consider the polynomial $f_i = g_i - g_i'$. If f_i is nonzero, then since $f_i \in I$, its leading term must be divisible by some h_j. By definition of a reduced basis, h_j for $j \neq i$ does not divide any of the terms in either g_i or g_i', hence does not divide $LT(f_i)$. But h_i also does not divide $LT(f_i)$ since all the terms in f_i have strictly smaller multidegree. This forces $f_i = 0$, i.e., $g_i = g_i'$ for every i, so $G = G'$.

One application of the uniqueness of the reduced Gröbner basis is a computational method to determine when two ideals in a polynomial ring are equal.

Corollary 28. Let I and J be two ideals in $F[x_1, \ldots, x_n]$. Then $I = J$ if and only if I and J have the same reduced Gröbner basis with respect to any fixed monomial ordering on $F[x_1, \ldots, x_n]$.

Examples

(1) Consider the ideal $I = (h_1, h_2, h_3)$ with $h_1 = x^2+xy^5+y^4$, $h_2 = xy^6-xy^3+y^5-y^2$, and $h_3 = xy^5 - xy^2$ in $F[x, y]$. Using the lexicographic ordering $x > y$ we find

$S(h_1, h_2) \equiv S(h_1, h_3) \equiv 0 \bmod \{h_1, h_2, h_3\}$ and $S(h_2, h_3) \equiv y^5 - y^2 \bmod \{h_1, h_2, h_3\}$. Setting $h_4 = y^5 - y^2$ we find $S(h_i, h_j) \equiv 0 \bmod \{h_1, h_2, h_3, h_4\}$ for $1 \leq i < j \leq 4$, so

$$x^2 + xy^5 + y^4, \quad xy^6 - xy^3 + y^5 - y^2, \quad xy^5 - xy^2, \quad y^5 - y^2$$

is a Gröbner basis for I. The leading terms of this basis are x^2, xy^6, xy^5, y^5. Since y^5 divides both xy^6 and xy^5, we may remove the second and third generators to obtain a minimal Gröbner basis $\{x^2 + xy^5 + y^4, y^5 - y^2\}$ for I. The second term in the first generator is divisible by the leading term y^5 of the second generator, so this is not a reduced Gröbner basis. Replacing $x^2 + xy^5 + y^4$ by its remainder $x^2 + xy^2 + y^4$ after division by the other polynomials in the basis (which in this case is only the polynomial $y^5 - y^2$), we are left with the reduced Gröbner basis $\{x^2 + xy^2 + y^4, y^5 - y^2\}$ for I.

(2) Consider the ideal $J = (h_1, h_2, h_3)$ with $h_1 = xy^3 + y^3 + 1$, $h_2 = x^3y - x^3 + 1$, and $h_3 = x + y$ in $F[x, y]$. Using the lexicographic monomial ordering $x > y$ we find $S(h_1, h_2) \equiv 0 \bmod \{h_1, h_2, h_3\}$ and $S(h_1, h_3) \equiv y^4 - y^3 - 1 \bmod \{h_1, h_2, h_3\}$. Setting $h_4 = y^4 - y^3 - 1$ we find $S(h_i, h_j) \equiv 0 \bmod \{h_1, h_2, h_3, h_4\}$ for $1 \leq i < j \leq 4$, so

$$xy^3 + y^3 + 1, \quad x^3y - x^3 + 1, \quad x + y, \quad y^4 - y^3 - 1$$

is a Gröbner basis for J. The leading terms of this basis are xy^3, x^3y, x, and y^4, so $\{x + y, y^4 - y^3 - 1\}$ is a minimal Gröbner basis for J. In this case none of the terms in $y^4 - y^3 - 1$ are divisible by the leading term of $x + y$ and none of the terms in $x + y$ are divisible by the leading term in $y^4 - y^3 - 1$, so $\{x + y, y^4 - y^3 - 1\}$ is the reduced Gröbner basis for J. This is the basis for the ideal I in Example 1 following Proposition 26, so these two ideals are equal:

$$(x^3y - xy^2 + 1, x^2y^2 - y^3 - 1) = (xy^3 + y^3 + 1, x^3y - x^3 + 1, x + y)$$

(and both are equal to the ideal $(x + y, y^4 - y^3 - 1)$).

Gröbner Bases and Solving Algebraic Equations: Elimination

The theory of Gröbner bases is very useful in explicitly solving systems of algebraic equations, and is the basis by which computer algebra programs attempt to solve systems of equations. Suppose $S = \{f_1, \ldots, f_m\}$ is a collection of polynomials in n variables $x_1, \ldots, x_n$ and we are trying to find the solutions of the system of equations $f_1 = 0$, $f_2 = 0, \ldots, f_m = 0$ (i.e., the common set of zeros of the polynomials in S). If $(a_1, \ldots, a_n)$ is any solution to this system, then every element f of the ideal I generated by S also satisfies $f(a_1, \ldots, a_n) = 0$. Furthermore, it is an easy exercise to see that if $S' = \{g_1, \ldots, g_s\}$ is *any* set of generators for the ideal I then the set of solutions to the system $g_1 = 0, \ldots, g_s = 0$ is the *same* as the original solution set.

In the situation where $f_1, \ldots, f_m$ are *linear* polynomials, a solution to the system of equations can be obtained by successively eliminating the variables $x_1, x_2, \ldots$ by elementary means—using linear combinations of the original equations to eliminate the variable x_1, then using these equations to eliminate x_2, etc., producing a system of equations that can be easily solved (this is "Gauss-Jordan elimination" in linear algebra, cf. the exercises in Section 11.2).

The situation for polynomial equations that are nonlinear is naturally more complicated, but the basic principle is the same. If there is a nonzero polynomial in the

ideal I involving only one of the variables, say $p(x_n)$, then the last coordinate a_n is a solution of $p(x_n) = 0$. If now there is a polynomial in I involving only x_{n-1} and x_n, say $q(x_{n-1}, x_n)$, then the coordinate a_{n-1} would be a solution of $q(x_{n-1}, a_n) = 0$, etc. If we can successively find polynomials in I that eliminate the variables $x_1, x_2, \ldots$ then we will be able to determine all the solutions $(a_1, \ldots, a_n)$ to our original system of equations explicitly.

Finding equations that follow from the system of equations in S, i.e., finding elements of the ideal I that do not involve some of the variables, is referred to as *elimination theory*. The polynomials in I that do not involve the variables $x_1, \ldots, x_i$, i.e., $I \cap F[x_{i+1}, \ldots, x_n]$, is easily seen to be an ideal in $F[x_{i+1}, \ldots, x_n]$ and is given a name.

Definition. If I is an ideal in $F[x_1, \ldots, x_n]$ then $I_i = I \cap F[x_{i+1}, \ldots, x_n]$ is called the i^{th} *elimination ideal* of I with respect to the ordering $x_1 > \cdots > x_n$.

The success of using elimination to solve a system of equations depends on being able to determine the elimination ideals (and, ultimately, on whether these elimination ideals are nonzero).

The following fundamental proposition shows that if the lexicographic monomial ordering $x_1 > \cdots > x_n$ is used to compute a Gröbner basis for I then the elements in the resulting basis not involving the variables $x_1, \ldots, x_i$ not only determine the i^{th} elimination ideal, but in fact give a Gröbner basis for the i^{th} elimination ideal of I.

Proposition 29. (*Elimination*) Suppose $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for the nonzero ideal I in $F[x_1, \ldots, x_n]$ with respect to the lexicographic monomial ordering $x_1 > \cdots > x_n$. Then $G \cap F[x_{i+1}, \ldots, x_n]$ is a Gröbner basis of the i^{th} elimination ideal $I_i = I \cap F[x_{i+1}, \ldots, x_n]$ of I. In particular, $I \cap F[x_{i+1}, \ldots, x_n] = 0$ if and only if $G \cap F[x_{i+1}, \ldots, x_n] = \emptyset$.

Proof: Denote $G_i = G \cap F[x_{i+1}, \ldots, x_n]$. Then $G_i \subseteq I_i$, so by Proposition 24, to see that G_i is a Gröbner basis of I_i it suffices to see that $LT(G_i)$, the leading terms of the elements in G_i, generate $LT(I_i)$ as an ideal in $F[x_{i+1}, \ldots, x_n]$. Certainly $(LT(G_i)) \subseteq LT(I_i)$ as ideals in $F[x_{i+1}, \ldots, x_n]$. To show the reverse containment, let f be any element in I_i. Then $f \in I$ and since G is a Gröbner basis for I we have

$$LT(f) = a_1(x_1, \ldots, x_n)LT(g_1) + \cdots + a_m(x_1, \ldots, x_n)LT(g_m)$$

for some polynomials $a_1, \ldots, a_m \in F[x_1, \ldots, x_n]$. Writing each polynomial a_i as a sum of monomial terms we see that $LT(f)$ is a sum of monomial terms of the form $ax_1^{s_1} \ldots x_n^{s_n} LT(g_i)$. Since $LT(f)$ involves only the variables $x_{i+1}, \ldots, x_n$, the sum of all such terms containing any of the variables $x_1, \ldots, x_i$ must be 0, so $LT(f)$ is also the sum of those monomial terms only involving $x_{i+1}, \ldots, x_n$. It follows that $LT(f)$ can be written as a $F[x_{i+1}, \ldots, x_n]$-linear combination of some monomial terms $LT(g_t)$ where $LT(g_t)$ does not involve the variables $x_1, \ldots, x_i$. But by the choice of the ordering, if $LT(g_t)$ does not involve $x_1, \ldots, x_i$, then neither do any of the other terms in g_t, i.e., $g_t \in G_i$. Hence $LT(f)$ can be written as a $F[x_{i+1}, \ldots, x_n]$-linear combination of elements $LT(G_i)$, completing the proof.

Note also that Gröbner bases can be used to eliminate any variables simply by using an appropriate monomial ordering.

Examples

(1) The ellipse $2x^2 + 2xy + y^2 - 2x - 2y = 0$ intersects the circle $x^2 + y^2 = 1$ in two points. To find them we compute a Gröbner basis for the ideal $I = (2x^2 + 2xy + y^2 - 2x - 2y, x^2 + y^2 - 1) \subset \mathbb{R}[x, y]$ using the lexicographic monomial order $x > y$ to eliminate x, obtaining $g_1 = 2x + y^2 + 5y^3 - 2$ and $g_2 = 5y^4 - 4y^3$. Hence $5y^4 = 4y^3$ and $y = 0$ or $y = 4/5$. Substituting these values into $g_1 = 0$ and solving for x we find the two intersection points are $(1, 0)$ and $(-3/5, 4/5)$.

Instead using the lexicographic monomial order $y > x$ to eliminate y results in the Gröbner basis $\{y^2 + x^2 - 1, 2yx - 2y + x^2 - 2x + 1, 5x^3 - 7x^2 - x + 3\}$. Then $5x^3 - 7x^2 - x + 3 = (x - 1)^2(5x + 3)$ shows that x is 1 or $-3/5$ and we obtain the same solutions as before, although with more effort.

(2) In the previous example the solutions could also have been found by elementary means. Consider now the solutions in $\mathbb{C}$ to the system of two equations

$$x^3 - 2xy + y^3 = 0 \quad \text{and} \quad x^5 - 2x^2y^2 + y^5 = 0.$$

Computing a Gröbner basis for the ideal generated by $f_1 = x^3 - 2xy + y^3$ and $f_2 = x^5 - 2x^2y^2 + y^5$ with respect to the lexicographic monomial order $x > y$ we obtain the basis

$$\begin{aligned} g_1 &= x^3 - 2xy + y^3 \\ g_2 &= 200xy^2 + 193y^9 + 158y^8 - 45y^7 - 456y^6 + 50y^5 - 100y^4 \\ g_3 &= y^{10} - y^8 - 2y^7 + 2y^6. \end{aligned}$$

Any solution to our original equations would satisfy $g_1 = g_2 = g_3 = 0$. Since $g_3 = y^6(y - 1)^2(y^2 + 2y + 2)$, we have $y = 0$, $y = 1$ or $y = -1 \pm i$. Since $g_1(x, 0) = x^3$ and $g_2(x, 0) = 0$, we see that $(0, 0)$ is the only solution with $y = 0$. Since $g_1(x, 1) = x^3 - 2x + 1$ and $g_2(x, 1) = 200(x - 1)$ have only $x = 1$ as a common zero, the only solution with $y = 1$ is $(1, 1)$. Finally,

$$\begin{aligned} g_1(x, -1 \pm i) &= x^3 + (2 \mp 2i)x + (2 \pm 2i) \\ g_2(x, -1 \pm i) &= -400i(x + 1 \pm i), \end{aligned}$$

and a quick check shows the common zero $x = -1 \mp i$ when $y = -1 \pm i$, respectively. Hence, there are precisely four solutions to the original pair of equations, namely

$$(x, y) = (0, 0), \quad (1, 1), \quad (-1 + i, -1 - i), \quad \text{or} \quad (-1 - i, -1 + i).$$

(3) Consider the solutions in $\mathbb{C}$ to the system of equations

$$\begin{aligned} x + y + z &= 1 \\ x^2 + y^2 + z^2 &= 2 \\ x^3 + y^3 + z^3 &= 3. \end{aligned}$$

The reduced Gröbner basis with respect to the lexicographic ordering $x > y > z$ is

$$\{x + y + z - 1, \ y^2 + yz - y + z^2 - z - (1/2), \ z^3 - z^2 - (1/2)z - (1/6)\}$$

and so z is a root of the polynomial $t^3 - t^2 - (1/2)t - (1/6)$ (by symmetry, also x and y are roots of this same polynomial). For each of the three roots of this polynomial, there are two values of y and one corresponding value of x making the first two polynomials in the Gröbner basis equal to 0. The resulting six solutions are quickly checked to be the three distinct roots of the polynomial $t^3 - t^2 - (1/2)t - (1/6)$ (which is irreducible over $\mathbb{Q}$) in some order.

As the previous examples show, the study of solutions to systems of polynomial equations $f_1 = 0, f_2 = 0, \ldots, f_m = 0$ is intimately related to the study of the ideal $I = (f_1, f_2, \ldots, f_m)$ the polynomials generate in $F[x_1, \ldots, x_n]$. This fundamental connection is the starting point for the important and active branch of mathematics called "algebraic geometry", introduced in Chapter 15, where additional applications of Gröbner bases are given.

We close this section by showing how to compute the basic set-theoretic operations of sums, products and intersections of ideals in polynomial rings. Suppose $I = (f_1, \ldots, f_s)$ and $J = (h_1, \ldots, h_t)$ are two ideals in $F[x_1, \ldots, x_n]$. Then $I + J = (f_1, \ldots, f_s, h_1, \ldots, h_t)$ and $IJ = (f_1h_1, \ldots, f_ih_j, \ldots, f_sh_t)$. The following proposition shows how to compute the intersection of any two ideals.

Proposition 30. If I and J are any two ideals in $F[x_1, \ldots, x_n]$ then $tI + (1 - t)J$ is an ideal in $F[t, x_1, \ldots, x_n]$ and $I \cap J = (tI + (1 - t)J) \cap F[x_1, \ldots, x_n]$. In particular, $I \cap J$ is the first elimination ideal of $tI + (1 - t)J$ with respect to the ordering $t > x_1 > \cdots > x_n$.

Proof: First, tI and $(1-t)J$ are clearly ideals in $F[x_1, \ldots, x_n, t]$, so also their sum $tI + (1-t)J$ is an ideal in $F[x_1, \ldots, x_n, t]$. If $f \in I \cap J$, then $f = tf + (1-t)f$ shows $I \cap J \subseteq (tI + (1-t)J) \cap F[x_1, \ldots, x_n]$. Conversely, suppose $f = tf_1 + (1-t)f_2$ is an element of $F[x_1, \ldots, x_n]$, where $f_1 \in I$ and $f_2 \in J$. Then $t(f_1 - f_2) = f - f_2 \in F[x_1, \ldots, x_n]$ shows that $f_1 - f_2 = 0$ and $f = f_2$, so $f = f_1 = f_2 \in I \cap J$. Since $I \cap J = (tI + (1 - t)J) \cap F[x_1, \ldots, x_n]$, $I \cap J$ is the first elimination ideal of $tI + (1 - t)J$ with respect to the ordering $t > x_1 > \cdots > x_n$.

We have $tI + (1-t)J = (tf_1, \ldots, tf_s, (1-t)h_1, \ldots, (1-t)h_t)$ if $I = (f_1, \ldots, f_s)$ and $J = (h_1, \ldots, h_t)$. By Proposition 29, the elements not involving t in a Gröbner basis for this ideal in $F[t, x_1, \ldots, x_n]$, computed for the lexicographic monomial ordering $t > x_1 > \cdots > x_n$, give a Gröbner basis for the ideal $I \cap J$ in $F[x_1, \ldots, x_n]$.

Example

Let $I = (x, y)^2 = (x^2, xy, y^2)$ and let $J = (x)$. For the lexicographic monomial ordering $t > x > y$ the reduced Gröbner basis for $tI + (1-t)J$ in $F[t, x, y]$ is $\{tx - x, ty^2, x^2, xy\}$ and so $I \cap J = (x^2, xy)$.

EXERCISES

1. Suppose I is an ideal in $F[x_1, \ldots, x_n]$ generated by a (possibly infinite) set $\mathcal{S}$ of polynomials. Prove that a finite subset of the polynomials in $\mathcal{S}$ suffice to generate I. [Use Theorem 21 to write $I = (f_1, \ldots, f_m)$ and then write each $f_i \in I$ using polynomials in $\mathcal{S}$.]
2. Let $\geq$ be any monomial ordering.
   (a) Prove that $LT(fg) = LT(f)LT(g)$ and $\partial(fg) = \partial(f) + \partial(g)$ for any nonzero polynomials f and g.
   (b) Prove that $\partial(f + g) \leq \max(\partial(f), \partial(g))$ with equality if $\partial(f) \neq \partial(g)$.

(c) Prove that $m \geq 1$ for every monomial m.

(d) Prove that if m_1 divides m_2 then $m_2 \geq m_1$. Deduce that the leading term of a polynomial does not divide any of its lower order terms.

3. Prove that if $\geq$ is any total or partial ordering on a nonempty set then the following are equivalent:

(i) Every nonempty subset contains a minimum element.

(ii) There is no infinite strictly decreasing sequence $a_1 > a_2 > a_3 > \cdots$ (this is called the *descending chain condition* or *D.C.C.*).

Deduce that General Polynomial Division always terminates in finitely many steps.

4. Let $\geq$ be a monomial ordering, and for monomials m_1, m_2 define $m_1 \geq_g m_2$ if either $\deg m_1 > \deg m_2$, or $\deg m_1 = \deg m_2$ and $m_1 \geq m_2$.

(a) Prove that $\geq_g$ is also a monomial ordering. (The relation $\geq_g$ is called the *grading* of $\geq$. An ordering in which the most important criterion for comparison is degree is sometimes called a *graded* or a *degree* ordering, so this exercise gives a method for constructing graded orderings.)

(b) The grading of the lexicographic ordering $x_1 > \cdots > x_n$ is called the *grlex* monomial ordering. Show that $x_2^4 > x_1^2x_2 > x_1x_2^2 > x_2^2 > x_1$ with respect to the grlex ordering and $x_1^2x_2 > x_1x_2^2 > x_1 > x_2^4 > x_2^2$ with respect to the lexicographic ordering.

5. The *grevlex* monomial ordering is defined by first choosing an ordering of the variables $\{x_1, x_2, \ldots, x_n\}$, then defining $m_1 \geq m_2$ for monomials m_1, m_2 if either $\deg m_1 > \deg m_2$ or $\deg m_1 = \deg m_2$ and the first exponent of $x_n, x_{n-1}, \ldots, x_1$ (in that order) where m_1 and m_2 differ is *smaller* in m_1.

(a) Prove that grevlex is a monomial ordering that satisfies $x_1 > x_2 > \cdots > x_n$.

(b) Prove that the grevlex ordering on $F[x_1, x_2]$ with respect to $\{x_1, x_2\}$ is the graded lexicographic ordering with $x_1 > x_2$, but that the grevlex ordering on $F[x_1, x_2, x_3]$ is not the grading of any lexicographic ordering.

(c) Show that $x_1x_2^2x_3 > x_1^2x_3^2 > x_2^2x_3^2 > x_2x_3^2 > x_1x_2 > x_2^2 > x_1x_3 > x_3^2 > x_1 > x_2$ for the grevlex monomial ordering with respect to $\{x_1, x_2, x_3\}$.

6. Show that $x^3y > x^3z^2 > x^3z > x^2y^2z > x^2y > xz^2 > y^2z^2 > y^2z$ with respect to the lexicographic monomial ordering $x > y > z$. Show that for the corresponding grlex monomial ordering $x^3z^2 > x^2y^2z > x^3y > x^3z > y^2z^2 > x^2y > xz^2 > y^2z$, and that $x^2y^2z > x^3z^2 > x^3y > x^3z > y^2z^2 > x^2y > y^2z > xz^2$ for the grevlex monomial ordering with respect to $\{x, y, z\}$.

7. Order the monomials $x^2z, x^2y^2z, xy^2z, x^3y, x^3z^2, x^2, x^2yz^2, x^2z^2$ for the lexicographic monomial ordering $x > y > z$, for the corresponding grlex monomial order, and for the grevlex monomial ordering with respect to $\{x, y, z\}$.

8. Show there are $n!$ distinct lexicographic monomial orderings on $F[x_1, \ldots, x_n]$. Show similarly that there are $n!$ distinct grlex and grevlex monomial orderings.

9. It can be shown that any monomial ordering on $F[x_1, \ldots, x_n]$ may be obtained as follows. For $k \leq n$ let $v_1, v_2, \ldots, v_k$ be nonzero vectors in Euclidean n-space, $\mathbb{R}^n$, that are pairwise orthogonal: $v_i \cdot v_j = 0$ for all $i \neq j$, where $\cdot$ is the usual dot product, and suppose also that all the coordinates of v_1 are nonnegative. Define an order, $\geq$, on monomials by $m_1 > m_2$ if and only if for some $t \leq k$ we have $v_i \cdot \partial(m_1) = v_i \cdot \partial(m_2)$ for all $i \in \{1, 2, \ldots, t-1\}$ and $v_t \cdot \partial(m_1) > v_t \cdot \partial(m_2)$.

(a) Let $k = n$ and let $v_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in the i^{th} position. Show that $\geq$ defines the lexicographic order with $x_1 > x_2 > \cdots > x_n$.

(b) Let $k = n$ and define $v_1 = (1, 1, \ldots, 1)$ and $v_i = (1, 1, \ldots, 1, -n+i-1, 0, \ldots, 0)$,

where there are $i-2$ trailing zeros, $2 \le i \le n$. Show that $\ge$ defines the grlex order with respect to $\{x_1, \ldots, x_n\}$.

10. Suppose I is a monomial ideal generated by monomials $m_1, \ldots, m_k$. Prove that the polynomial $f \in F[x_1, \ldots, x_n]$ is in I if and only if every monomial term f_i of f is a multiple of one of the m_j. [For polynomials $a_1, \ldots, a_k \in F[x_1, \ldots, x_n]$ expand the polynomial $a_1m_1 + \cdots + a_km_k$ and note that every monomial term is a multiple of at least one of the m_j.] Show that $x^2yz+3xy^2$ is an element of the ideal $I = (xyz, y^2) \subset F[x, y, z]$ but is not an element of the ideal $I' = (xz^2, y^2)$.

11. Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and suppose $\{g_1, \ldots, g_m\}$ is a Gröbner basis for the ideal I in R. Prove that $h \in LT(I)$ if and only if h is a sum of monomial terms each divisible by some $LT(g_i)$, $1 \le i \le m$. [Use the previous exercise.]

12. Suppose I is a monomial ideal with monomial generators $g_1, \ldots, g_m$. Use the previous exercise to prove directly that $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I.

13. Suppose I is a monomial ideal with monomial generators $g_1, \ldots, g_m$. Use Buchberger's Criterion to prove that $\{g_1, \ldots, g_m\}$ is a Gröbner basis for I.

14. Suppose I is a monomial ideal in $R = F[x_1, \ldots, x_n]$ and suppose $\{m_1, \ldots, m_k\}$ is a minimal set of monomials generating I, i.e., each m_i is a monomial and no proper subset of $\{m_1, \ldots, m_k\}$ generates I. Prove that the m_i, $1 \le i \le k$ are unique. [Use Exercise 10.]

15. Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$.

(a) Prove that $\{g_1, \ldots, g_m\}$ is a minimal Gröbner basis for the ideal I in R if and only if $\{LT(g_1), \ldots, LT(g_m)\}$ is a minimal generating set for $LT(I)$.

(b) Prove that the leading terms of a minimal Gröbner basis for I are uniquely determined and the number of elements in any two minimal Gröbner bases for I is the same. [Use (a) and the previous exercise.]

16. Fix a monomial ordering on $F[x_1, \ldots, x_n]$ and suppose $G = \{g_1, \ldots, g_m\}$ is a set of generators for the nonzero ideal I. Show that if $S(g_i, g_j) \not\equiv 0 \bmod G$ then the ideal $(LT(g_1), \ldots, LT(g_m), LT(S(g_i, g_j))$ is strictly larger than the ideal $(LT(g_1), \ldots, LT(g_m))$. Conclude that the algorithm for computing a Gröbner basis described following Proposition 26 terminates after a finite number of steps. [Use Exercise 1.]

17. Fix the lexicographic ordering $x > y$ on $F[x, y]$. Use Buchberger's Criterion to show that $\{x^2y - y^2, x^3 - xy\}$ is a Gröbner basis for the ideal $I = (x^2y - y^2, x^3 - xy)$.

18. Show $\{x - y^3, y^5 - y^6\}$ is the reduced Gröbner basis for the ideal $I = (x - y^3, -x^2 + xy^2)$ with respect to the lexicographic ordering defined by $x > y$ in $F[x, y]$.

19. Fix the lexicographic ordering $x > y$ on $F[x, y]$.

(a) Show that $\{x^3 - y, x^2y - y^2, xy^2 - y^2, y^3 - y^2\}$ is the reduced Gröbner basis for the ideal $I = (-x^3 + y, x^2y - y^2)$.

(b) Determine whether the polynomial $f = x^6 - x^5y$ is an element of the ideal I.

20. Fix the lexicographic ordering $x > y > z$ on $F[x, y, z]$. Show that $\{x^2 + xy + z, xyz + z^2, xz^2, z^3\}$ is the reduced Gröbner basis for the ideal $I = (x^2 + xy + z, xyz + z^2)$ and in particular conclude that the leading term ideal $LT(I)$ requires four generators.

21. Fix the lexicographic ordering $x > y$ on $F[x, y]$. Use Buchberger's Criterion to show that $\{x^2y - y^2, x^3 - xy\}$ is a Gröbner basis for the ideal $I = (x^2y - y^2, x^3 - xy)$.

22. Let $I = (x^2 - y, x^2y - z)$ in $F[x, y, z]$.

(a) Show that $\{x^2 - y, y^2 - z\}$ is the reduced Gröbner basis for I with respect to the lexicographic ordering defined by $x > y > z$.

(b) Show that $\{x^2 - y, z - y^2\}$ is the reduced Gröbner basis for I with respect to the

lexicographic ordering defined by $z > x > y$ (note these are essentially the same polynomials as in (a)).

(c) Show that $\{y - x^2, z - x^4\}$ is the reduced Gröbner basis for I with respect to the lexicographic ordering defined by $z > y > x$.

23. Show that the ideals $I = (x^2y + xy^2 - 2y, x^2 + xy - x + y^2 - 2y, xy^2 - x - y + y^3)$ and $J = (x - y^2, xy - y, x^2 - y)$ in $F[x, y]$ are equal.

24. Use reduced Gröbner bases to show that the ideal $I = (x^3 - yz, yz + y)$ and the ideal $J = (x^3z + x^3, x^3 + y)$ in $F[x, y, z]$ are equal.

25. Show that the reduced Gröbner basis using the lexicographic ordering $x > y$ for the ideal $I = (x^2 + xy^2, x^2 - y^3, y^3 - y^2)$ is $\{x^2 - y^2, y^3 - y^2, xy^2 + y^2\}$.

26. Show that the reduced Gröbner basis for the ideal $I = (xy + y^2, x^2y + xy^2 + x^2)$ is $\{x^2, xy + y^2, y^3\}$ with respect to the lexicographic ordering $x > y$ and is $\{y^2 + yx, x^2\}$ with respect to the lexicographic ordering $y > x$.

There are generally substantial differences in computational complexity when using different monomial orders. The grevlex monomial ordering often provides the most efficient computation and produces simpler polynomials.

27. Show that $\{x^3 - y^3, x^2 + xy^2 + y^4, x^2y + xy^3 + y^2\}$ is a reduced Gröbner basis for the ideal I in the example following Corollary 28 with respect to the grlex monomial ordering. (Note that while this gives three generators for I rather than two for the lexicographic ordering as in the example, the degrees are smaller.)

28. Let $I = (x^4 - y^4 + z^3 - 1, x^3 + y^2 + z^2 - 1)$. Show that there are five elements in a reduced Gröbner basis for I with respect to the lexicographic ordering with $x > y > z$ (the maximum degree among the five generators is 12 and the maximum number of monomial terms among the five generators is 35), that there are two elements for the lexicographic ordering $y > z > x$ (maximum degree is 6 and maximum number of terms is 8), and that $\{x^3 + y^2 + z^2 - 1, xy^2 + xz^2 - x + y^4 - z^3 + 1\}$ is the reduced Gröbner basis for the grevlex monomial ordering.

29. Solve the system of equations $x^2 - yz = 3$, $y^2 - xz = 4$, $z^2 - xy = 5$ over $\mathbb{C}$.

30. Find a Gröbner basis for the ideal $I = (x^2 + xy + y^2 - 1, x^2 + 4y^2 - 4)$ for the lexicographic ordering $x > y$ and use it to find the four points of intersection of the ellipse $x^2 + xy + y^2 = 1$ with the ellipse $x^2 + 4y^2 = 4$ in $\mathbb{R}^2$.

31. Use Gröbner bases to find all six solutions to the system of equations $2x^3 + 2x^2y^2 + 3y^3 = 0$ and $3x^5 + 2x^3y^3 + 2y^5 = 0$ over $\mathbb{C}$.

32. Use Gröbner bases to show that $(x, z) \cap (y^2, x - yz) = (xy, x - yz)$ in $F[x, y, z]$.

33. Use Gröbner bases to compute the intersection of the ideals $(x^3y - xy^2 + 1, x^2y^2 - y^3 - 1)$ and $(x^2 - y^2, x^3 + y^3)$ in $F[x, y]$.

The following four exercises deal with the *ideal quotient* of two ideals I and J in a ring R.

Definition. The *ideal quotient* $(I : J)$ of two ideals I, J in a ring R is the ideal

$$(I : J) = \{r \in R \mid rJ \in I\}.$$

34. (a) Suppose R is an integral domain, $0 \neq f \in R$ and I is an ideal in R. Show that if $\{g_1, \ldots, g_s\}$ are generators for the ideal $I \cap (f)$, then $\{g_1/f, \ldots, g_s/f\}$ are generators for the ideal quotient $(I : (f))$.

(b) If I is an ideal in the commutative ring R and $f_1, \ldots, f_s \in R$, show that the ideal quotient $(I : (f_1, \ldots f_s))$ is the ideal $\cap_{i=1}^{s} (I : (f_i))$.

35. If $I = (x^2y + z^3, x + y^3 - z, 2y^4z - yz^2 - z^3)$ and $J = (x^2y^5, x^3z^4, y^3z^7)$ in $\mathbb{Q}[x, y, z]$ show $(I : J)$ is the ideal $(z^2, y + z, x - z)$. [Use the previous exercise and Proposition 30.]

36. Suppose that K is an ideal in R, that I is an ideal containing K, and J is any ideal. If $\overline{I}$ and $\overline{J}$ denote the images of I and J in the quotient ring R/K, show that $\overline{(I : J)} = (\overline{I} : \overline{J})$ where $\overline{(I : J)}$ is the image in R/K of the ideal quotient $(I : J)$.

37. Let K be the ideal $(y^5 - z^4)$ in $R = \mathbb{Q}[y, z]$. For each of the following pairs of ideals I and J, use the previous two exercises together with Proposition 30 to verify the ideal quotients $(\overline{I} : \overline{J})$ in the ring R/K:

i. $I = (y^3, y^5 - z^4)$, $J = (z)$, $(\overline{I} : \overline{J}) = (\bar{y}^3, \bar{z}^3)$.

ii. $I = (y^3, z, y^5 - z^4)$, $J = (y)$, $(\overline{I} : \overline{J}) = (\bar{y}^2, \bar{z})$.

iii. $I = (y, y^3, z, y^5 - z^4)$, $J = (1)$, $(\overline{I} : \overline{J}) = (\bar{y}, \bar{z})$.

Exercises 38 to 44 develop some additional elementary properties of monomial ideals in $F[x_1, \ldots, x_n]$. It follows from Hilbert's Basis Theorem that ideals are finitely generated, however one need not assume this in these exercises—the arguments are the same for finitely or infinitely generated ideals. These exercises may be used to give an independent proof of Hilbert's Basis Theorem (Exercise 44). In these exercises, M and N are monomial ideals with monomial generators $\{m_i \mid i \in I\}$ and $\{n_j \mid j \in J\}$ for some index sets I and J respectively.

38. Prove that the sum and product of two monomial ideals is a monomial ideal by showing that $M + N = (m_i,\ n_j \mid i \in I,\ j \in J)$, and $MN = (m_i n_j \mid i \in I,\ j \in J)$.

39. Show that if $\{M_s \mid s \in S\}$ is any nonempty collection of monomial ideals that is totally ordered under inclusion then $\cup_{s \in S} M_s$ is a monomial ideal. (In particular, the union of any increasing sequence of monomial ideals is a monomial ideal, cf. Exercise 19, Section 7.3.)

40. Prove that the intersection of two monomial ideals is a monomial ideal by showing that $M \cap N = (e_{i,j} \mid i \in I,\ j \in J)$, where $e_{i,j}$ is the least common multiple of m_i and n_j. [Use Exercise 10.]

41. Prove that for any monomial n, the ideal quotient $(M : (n))$ is $(m_i/d_i \mid i \in I)$, where d_i is the greatest common divisor of m_i and n (cf. Exercise 34). Show that if N is finitely generated, then the ideal quotient $(M : N)$ of two monomial ideals is a monomial ideal.

42. **(a)** Show that M is a monomial prime ideal if and only if $M = (S)$ for some subset of S of $\{x_1, x_2, \ldots, x_n\}$. (In particular, there are only finitely many monomial prime ideals, and each is finitely generated.)

(b) Show that $(x_1, \ldots, x_n)$ is the only monomial maximal ideal.

43. *(Dickson's Lemma*—a special case of Hilbert's Basis Theorem) Prove that every monomial ideal in $F[x_1, \ldots, x_n]$ is finitely generated as follows.
Let $\mathcal{S} = \{N \mid N$ is a monomial ideal that is not finitely generated$\}$, and assume by way of contradiction $\mathcal{S} \neq \emptyset$.

(a) Show that $\mathcal{S}$ contains a maximal element M. [Use Exercise 30 and Zorn's Lemma.]

(b) Show that there are monomials x, y not in M with $xy \in M$. [Use Exercise 33(a).]

(c) For x as in (b), show that M contains a finitely generated monomial ideal M_0 such that $M_0 + (x) = M + (x)$ and $M = M_0 + (x)(M : (x))$, where $(M : (x))$ is the (monomial) ideal defined in Exercise 32, and $(x)(M : (x))$ is the product of these two ideals. Deduce that M is finitely generated, a contradiction which proves $\mathcal{S} = \emptyset$. [Use the maximality of M and previous exercises.]

44. If I is a nonzero ideal in $F[x_1, \ldots, x_n]$, use Dickson's Lemma to prove that $LT(I)$ is finitely generated. Conclude that I has a Gröbner basis and deduce Hilbert's Basis Theorem. [cf. Proposition 24.]

45. *(n-colorings of graphs)* A finite *graph* $\mathcal{G}$ of size N is a set of vertices $i \in \{1, 2, \ldots, N\}$ and a collection of edges (i, j) connecting vertex i with vertex j. An *n-coloring* of $\mathcal{G}$ is an assignment of one of n colors to each vertex in such a way that vertices connected by an edge have distinct colors. Let F be any field containing at least n elements. If we introduce a variable x_i for each vertex i and represent the n colors by choosing a set S of n distinct elements from F, then an n-coloring of $\mathcal{G}$ is equivalent to assigning a value $x_i = \alpha_i$ for each $i = 1, 2, \ldots, N$ where $\alpha_i \in S$ and $\alpha_i \neq \alpha_j$ if (i, j) is an edge in $\mathcal{G}$. If $f(x) = \prod_{\alpha \in S}(x - \alpha)$ is the polynomial in $F[x]$ of degree n whose roots are the elements in S, then $x_i = \alpha_i$ for some $\alpha_i \in S$ is equivalent to the statement that x_i is a solution to the equation $f(x_i) = 0$. The statement $\alpha_i \neq \alpha_j$ is then the statement that $f(x_i) = f(x_j)$ but $x_i \neq x_j$, so x_i and x_j satisfy the equation $g(x_i, x_j) = 0$, where $g(x_i, x_j)$ is the polynomial $(f(x_i) - f(x_j))/(x_i - x_j)$ in $F[x_i, x_j]$. It follows that finding an *n-coloring* of $\mathcal{G}$ is equivalent to solving the system of equations

$$\begin{cases} f(x_i) = 0, & \text{for } i = 1, 2, \ldots, N, \\ g(x_i, x_j) = 0, & \text{for all edges } (i, j) \text{ in } \mathcal{G} \end{cases}$$

(note also we may use any polynomial g satisfying $\alpha_i \neq \alpha_j$ if $g(\alpha_i, \alpha_j) = 0$). It follows by "Hilbert's Nullstellensatz" (cf. Corollary 33 in Section 15.3) that this system of equations has a solution, hence $\mathcal{G}$ has an n-coloring, unless the ideal I in $F[x_1, x_2, \ldots, x_N]$ generated by the polynomials $f(x_i)$ for $i = 1, 2, \ldots, N$, together with the polynomials $g(x_i, x_j)$ for all the edges (i, j) in the graph $\mathcal{G}$, is not a proper ideal. This in turn is equivalent to the statement that the reduced Gröbner basis for I (with respect to any monomial ordering) is simply $\{1\}$. Further, when an n-coloring does exist, solving this system of equations as in the examples following Proposition 29 provides an explicit coloring for $\mathcal{G}$.

There are many possible choices of field F and set S. For example, use any field F containing a set S of distinct n^{th} roots of unity, in which case $f(x) = x^n - 1$ and we may take $g(x_i, x_j) = (x_i^n - x_j^n)/(x_i - x_j) = x_i^{n-1} + x_i^{n-2}x_j + \cdots + x_i x_j^{n-2} + x_j^{n-1}$, or use any subset S of $F = \mathbb{F}_p$ with a prime $p \geq n$ (in the special case $n = p$, then, by Fermat's Little Theorem, we have $f(x) = x^p - x$ and $g(x_i, x_j) = (x_i - x_j)^{p-1} - 1$).

(a) Consider a possible 3-coloring of the graph $\mathcal{G}$ with eight vertices and 14 edges $(1, 3)$, $(1, 4)$, $(1, 5)$, $(2, 4)$, $(2, 7)$, $(2, 8)$, $(3, 4)$, $(3, 6)$, $(3, 8)$, $(4, 5)$, $(5, 6)$, $(6, 7)$, $(6, 8)$, $(7, 8)$. Take $F = \mathbb{F}_3$ with 'colors' $0, 1, 2 \in \mathbb{F}_3$ and suppose vertex 1 is colored by 0. In this case $f(x) = x(x - 1)(x - 2) = x^3 - x \in \mathbb{F}_3[x]$ and $g(x_i, x_j) = x_i^2 + x_i x_j + x_j^2 - 1$. If I is the ideal generated by x_1, $x_i^3 - x_i$, $2 \leq i \leq 8$ and $g(x_i, x_j)$ for the edges (i, j) in $\mathcal{G}$, show that the reduced Gröbner basis for I with respect to the lexicographic monomial ordering $x_1 > x_2 > \cdots > x_8$ is $\{x_1, x_2, x_3 + x_8, x_4 + 2x_8, x_5 + x_8, x_6, x_7 + x_8, x_8^2 + 2\}$. Deduce that $\mathcal{G}$ has two distinct 3-colorings, determined by the coloring of vertex 8 (which must be colored by a nonzero element in $\mathbb{F}_3$), and exhibit the colorings of $\mathcal{G}$.

Show that if the edge $(3, 7)$ is added to $\mathcal{G}$ then the graph cannot be 3-colored.

(b) Take $F = \mathbb{F}_5$ with four 'colors' $1, 2, 3, 4 \in \mathbb{F}_5$, so $f(x) = x^4 - 1$ and we may use $g(x_i, x_j) = x_i^3 + x_i^2 x_j + x_i x_j^2 + x_j^3$. Show that the graph $\mathcal{G}$ with five vertices having 9 edges $(1, 3)$, $(1, 4)$, $(1, 5)$, $(2, 3)$, $(2, 4)$, $(2, 5)$, $(3, 4)$, $(3, 5)$, $(4, 5)$ (the "complete graph on five vertices" with one edge removed) can be 4-colored but cannot be 3-colored.

(c) Use Gröbner bases to show that the graph $\mathcal{G}$ with nine vertices and 22 edges $(1, 4)$, $(1, 6)$, $(1, 7)$, $(1, 8)$, $(2, 3)$, $(2, 4)$, $(2, 6)$, $(2, 7)$, $(3, 5)$, $(3, 7)$, $(3, 9)$, $(4, 5)$, $(4, 6)$, $(4, 7)$, $(4, 9)$, $(5, 6)$, $(5, 7)$, $(5, 8)$, $(5, 9)$, $(6, 7)$, $(6, 9)$, $(7, 8)$ has precisely four 4-colorings up to a permutation of the colors (so a total of 96 total 4-colorings). Show that if the edge $(1, 5)$ is added then $\mathcal{G}$ cannot be 4-colored.

Part III

MODULES AND VECTOR SPACES

In Part III we study the mathematical objects called modules. The use of modules was pioneered by one of the most prominent mathematicians of the first part of this century, Emmy Noether, who led the way in demonstrating the power and elegance of this structure. We shall see that vector spaces are just special types of modules which arise when the underlying ring is a field. If R is a ring, the definition of an R-module M is closely analogous to the definition of a group action where R plays the role of the group and M the role of the set. The additional axioms for a module require that M itself have more structure (namely that M be an abelian group). Modules are the "representation objects" for rings, i.e., they are, by definition, algebraic objects on which rings act. As the theory develops it will become apparent how the structure of the ring R (in particular, the structure and wealth of its ideals) is reflected by the structure of its modules and vice versa in the same way that the structure of the collection of normal subgroups of a group was reflected by its permutation representations.

CHAPTER 10

Introduction to Module Theory

10.1 BASIC DEFINITIONS AND EXAMPLES

We start with the definition of a module.

Definition. Let R be a ring (not necessarily commutative nor with 1). A *left R-module* or a *left module over R* is a set M together with

(1) a binary operation $+$ on M under which M is an abelian group, and

(2) an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies

(a) $(r+s)m = rm + sm$, for all $r, s \in R, m \in M$,

(b) $(rs)m = r(sm)$, for all $r, s \in R, m \in M$, and

(c) $r(m+n) = rm + rn$, for all $r \in R, m, n \in M$.

If the ring R has a 1 we impose the additional axiom:

(d) $1m = m$, for all $m \in M$.

The descriptor "left" in the above definition indicates that the ring elements appear on the left; "right" R-modules can be defined analogously. If the ring R is *commutative* and M is a left R-module we can make M into a right R-module by defining $mr = rm$ for $m \in M$ and $r \in R$. If R is not commutative, axiom 2(b) in general will not hold with this definition (so not every left R-module is also a right R-module). Unless explicitly mentioned otherwise the term "module" will always mean "left module." Modules satisfying axiom 2(d) are called *unital* modules and in this book all our modules will be unital (this is to avoid "pathologies" such as having $rm = 0$ for all $r \in R$ and $m \in M$).

When R is a field F the axioms for an R-module are precisely the same as those for a vector space over F, so that

modules over a field F and vector spaces over F are the same.

Before giving other examples of R-modules we record the obvious definition of submodules.

Definition. Let R be a ring and let M be an R-module. An *R-submodule* of M is a subgroup N of M which is closed under the action of ring elements, i.e., $rn \in N$, for all $r \in R, n \in N$.

Submodules of M are therefore just subsets of M which are themselves modules under the restricted operations. In particular, if $R = F$ is a field, submodules are the same as subspaces. Every R-module M has the two submodules M and 0 (the latter is called the *trivial submodule*).

Examples

(1) Let R be any ring. Then $M = R$ is a left R-module, where the action of a ring element on a module element is just the usual multiplication in the ring R (similarly, R is a right module over itself). In particular, every field can be considered as a (1-dimensional) vector space over itself. When R is considered as a left module over itself in this fashion, the submodules of R are precisely the left ideals of R (and if R is considered as a right R-module over itself, its submodules are the right ideals). Thus if R is not commutative it has a left and right module structure over itself and these structures may be different (e.g., the submodules may be different) — Exercise 21 at the end of this section gives a specific example of this.

(2) Let $R = F$ be a field. As noted above, every vector space over F is an F-module and vice versa. Let $n \in \mathbb{Z}^+$ and let

$$F^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in F, \text{ for all } i\}$$

(called *affine n-space over F*). Make F^n into a vector space by defining addition and scalar multiplication componentwise:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$
$$\alpha(a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n), \qquad \alpha \in F.$$

As in the case of Euclidean n-space (i.e., when $F = \mathbb{R}$), affine n-space is a vector space of dimension n over F (we shall discuss the notion of dimension more thoroughly in the next chapter).

(3) Let R be a ring with 1 and let $n \in \mathbb{Z}^+$. Following Example 2 define

$$R^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R, \text{ for all } i\}.$$

Make R^n into an R-module by componentwise addition and multiplication by elements of R in the same manner as when R was a field. The module R^n is called *the free module of rank n over R*. (We shall see shortly that free modules have the same "universal property" in the context of R-modules that free groups were seen to have in Section 6.3. We shall also soon discuss direct products of R-modules.) An obvious submodule of R^n is given by the i^{th} component, namely the set of n-tuples with arbitrary ring elements in the i^{th} component and zeros in the j^{th} component for all $j \neq i$.

(4) The same abelian group may have the structure of an R-module for a number of different rings R and each of these module structures may carry useful information. Specifically, if M is an R-module and S is a subring of R with $1_S = 1_R$, then M is automatically an S-module as well. For instance the field $\mathbb{R}$ is an $\mathbb{R}$-module, a $\mathbb{Q}$-module and a $\mathbb{Z}$-module.

(5) If M is an R-module and for some (2-sided) ideal I of R, $am = 0$, for all $a \in I$ and all $m \in M$, we say M is *annihilated by I*. In this situation we can make M into an (R/I)-module by defining an action of the quotient ring R/I on M as follows: for each $m \in M$ and coset $r + I$ in R/I let

$$(r + I)m = rm.$$

Since $am = 0$ for all $a \in I$ and all $m \in M$ this is well defined and one easily checks that it makes M into an (R/I)-module. In particular, when I is a maximal ideal in the commutative ring R and $IM = 0$, then M is a vector space over the field R/I (cf. the following example).

The next example is of sufficient importance as to be singled out. It will form the basis for our proof of the Fundamental Theorem of Finitely Generated Abelian Groups in Chapter 12.

Example: ($\mathbb{Z}$-modules)

Let R = $\mathbb{Z}$, let A be *any* abelian group (finite or infinite) and write the operation of A as $+$. Make A into a $\mathbb{Z}$-module as follows: for any $n \in \mathbb{Z}$ and $a \in A$ define

$$na = \begin{cases} a + a + \cdots + a \quad (n \text{ times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -a - a - \cdots - a \quad (-n \text{ times}) & \text{if } n < 0 \end{cases}$$

(here 0 is the identity of the additive group A). This definition of an action of the integers on A makes A into a $\mathbb{Z}$-module, and the module axioms show that this is the only possible action of $\mathbb{Z}$ on A making it a (unital) $\mathbb{Z}$-module. Thus every abelian group is a $\mathbb{Z}$-module. Conversely, if M is any $\mathbb{Z}$-module, a fortiori M is an abelian group, so

$\mathbb{Z}$-modules are the same as abelian groups.

Furthermore, it is immediate from the definition that

$\mathbb{Z}$-submodules are the same as subgroups.

Note that for the cyclic group $\langle a \rangle$ written multiplicatively the additive notation na becomes a^n, that is, we have all along been using the fact that $\langle a \rangle$ is a right $\mathbb{Z}$-module (checking that this "exponential" notation satisfies the usual laws of exponents is equivalent to checking the $\mathbb{Z}$-module axioms — this was given as an exercise at the end of Section 1.1). Note that since $\mathbb{Z}$ is commutative these definitions of left and right actions by ring elements give the same module structure.

If A is an abelian group containing an element x of finite order n then $nx = 0$. Thus, in contrast to vector spaces, a $\mathbb{Z}$-module may have nonzero elements x such that $nx = 0$ for some nonzero ring element n. In particular, if A has order m, then by Lagrange's Theorem (Corollary 9, Section 3.2) $mx = 0$, for *all* $x \in A$. Note that then A is a module over $\mathbb{Z}/m\mathbb{Z}$.

In particular, if p is a prime and A is an abelian group (written additively) such that $px = 0$, for all $x \in A$, then (as noted in Example 5) A is a $\mathbb{Z}/p\mathbb{Z}$-module, i.e., can be considered as a vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. For instance, the Klein 4-group is a (2-dimensional) vector space over $\mathbb{F}_2$. These groups are the *elementary abelian p-groups* discussed in Section 4.4 (see, in particular, Proposition 17(3)).

The next example is also of fundamental importance and will form the basis for our study of canonical forms of matrices in Sections 12.2 and 12.3.

Example: ($F[x]$-modules)

Let F be a field, let x be an indeterminate and let R be the polynomial ring $F[x]$. Let V be a vector space over F and let T be a linear transformation from V to V (we shall review the theory of linear transformations in the next chapter — for the purposes of this example one only needs to know the definition of a linear transformation). We have already seen that V is an F-module; the linear map T will enable us to make V into an $F[x]$-module.

First, for the nonnegative integer n, define

$$T^0 = I,$$

$$\vdots$$

$$T^n = T \circ T \circ \cdots \circ T \qquad (n \text{ times})$$

where I is the identity map from V to V and $\circ$ denotes function composition (which makes sense because the domain and codomain of T are the same). Also, for any two linear transformations A, B from V to V and elements $\alpha, \beta \in F$, let $\alpha A + \beta B$ be defined by

$$(\alpha A + \beta B)(v) = \alpha(A(v)) + \beta(B(v))$$

(i.e., addition and scalar multiplication of linear transformations are defined pointwise). Then $\alpha A + \beta B$ is easily seen to be a linear transformation from V to V, so that linear combinations of linear transformations are again linear transformations.

We now define the action of any polynomial in x on V. Let $p(x)$ be the polynomial

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

where $a_0, \ldots, a_n \in F$. For each $v \in V$ define an action of the ring element $p(x)$ on the module element v by

$$\begin{aligned} p(x)v &= (a_n T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0)(v) \\ &= a_n T^n(v) + a_{n-1}T^{n-1}(v) + \cdots + a_1 T(v) + a_0 v \end{aligned}$$

(i.e., $p(x)$ acts by substituting the linear transformation T for x in $p(x)$ and applying the resulting linear transformation to v). Put another way, x acts on V as the linear transformation T and we extend this to an action of all of $F[x]$ on V in a natural way. It is easy to check that this definition of an action of $F[x]$ on V satisfies all the module axioms and makes V into an $F[x]$-module.

The field F is naturally a subring of $F[x]$ (the constant polynomials) and the action of these field elements is by definition the same as their action when viewed as constant polynomials. In other words, the definition of the $F[x]$ action on V is consistent with the given action of the field F on the vector space V, i.e., the definition *extends* the action of F to an action of the larger ring $F[x]$.

The way $F[x]$ acts on V depends on the choice of T so that there are in general many different $F[x]$-module structures on the same vector space V. For instance, if $T = 0$, and $p(x)$, v are as above, then $p(x)v = a_0 v$, that is, the polynomial $p(x)$ acts on v simply by multiplying by the constant term of $p(x)$, so that the $F[x]$-module structure is just the F-module structure. If, on the other hand, T is the identity transformation (so $T^n(v) = v$, for all n and v), then $p(x)v = a_n v + a_{n-1}v + \cdots + a_0 v = (a_n + \cdots + a_0)v$, so that now $p(x)$ multiplies v by the sum of the coefficients of $p(x)$.

To give another specific example, let V be affine n-space F^n and let T be the "shift operator"

$$T(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, 0).$$

Let e_i be the usual i^{th} basis vector $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is in position i. Then

$$T^k(e_i) = \begin{cases} e_{i-k} & \text{if } i > k \\ 0 & \text{if } i \leq k \end{cases}$$

so for example, if $m < n$,

$$(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0)e_n = (0, \ldots, 0, a_m, a_{m-1}, \ldots, a_0).$$

From this we can determine the action of any polynomial on any vector.

The construction of an $F[x]$-module from a vector space V over F and a linear transformation T from V to V in fact describes *all* $F[x]$-modules; namely, an $F[x]$-module is a vector space together with a linear transformation which specifies the action of x. This is because if V is any $F[x]$-module, then V is an F-module and the action of the ring element x on V is a linear transformation from V to V. The axioms for a module ensure that the actions of F and x on V uniquely determine the action of any element of $F[x]$ on V. Thus there is a bijection between the collection of $F[x]$-modules and the collection of pairs V, T

$$\left\{ V \text{ an } F[x]\text{-module} \right\} \quad \longleftrightarrow \quad \left\{ \begin{array}{c} V \text{ a vector space over } F \\ \text{and} \\ T : V \to V \text{ a linear transformation} \end{array} \right\}$$

given by

the element x acts on V as the linear transformation T.

Now we consider $F[x]$-submodules of V where, as above, V is any $F[x]$-module and T is the linear transformation from V to V given by the action of x. An $F[x]$-submodule W of V must first be an F-submodule, i.e., W must be a vector subspace of V. Secondly, W must be sent to itself under the action of the ring element x, i.e., we must have $T(w) \in W$, for all $w \in W$. Any vector subspace U of V such that $T(U) \subseteq U$ is called *T-stable* or *T-invariant*. If U is any T-stable subspace of V it follows that $T^n(U) \subseteq U$, for all $n \in \mathbb{Z}^+$ (for example, $T(U) \subseteq U$ implies $T^2(U) = T(T(U)) \subseteq T(U) \subseteq U$). Moreover any linear combination of powers of T then sends U into U so that U is also stable by the action of *any* polynomial in T. Thus U is an $F[x]$-submodule of V. This shows that

the $F[x]$-submodules of V are precisely the T-stable subspaces of V.

In terms of the bijection above,

$$\left\{ W \text{ an } F[x]\text{-submodule} \right\} \quad \longleftrightarrow \quad \left\{ \begin{array}{c} W \text{ a subspace of } V \\ \text{and} \\ W \text{ is } T\text{-stable} \end{array} \right\}$$

which gives a complete dictionary between $F[x]$-modules V and vector spaces V together with a given linear transformation T from V to V.

For instance, if T is the shift operator defined on affine n-space above and k is any integer in the range $0 \leq k \leq n$, then the subspace

$$U_k = \{ (x_1, x_2, \ldots, x_k, 0, \ldots, 0) \mid x_i \in F \}$$

is clearly T-stable so is an $F[x]$-submodule of V.

We emphasize that an abelian group M may have many different R-module structures, even if the ring R does not vary (in the same way that a given group G may act in many ways as a permutation group on some fixed set Ω). We shall see that the structure of an R-module is reflected by the ideal structure of R. When R is a field (the subject of the next chapter) all R-modules will be seen to be products of copies of R (as in Example 3 above).

We shall see in Chapter 12 that the relatively simple ideal structure of the ring $F[x]$ (recall that $F[x]$ is a Principal Ideal Domain) forces the $F[x]$-module structure of V to be correspondingly uncomplicated, and this in turn provides a great deal of information about the linear transformation T (in particular, gives some nice matrix representations for T: its *rational canonical form* and its *Jordan canonical form*). Moreover, the same arguments which *classify* finitely generated $F[x]$-modules apply to any Principal Ideal Domain R, and when these are invoked for $R = \mathbb{Z}$, we obtain the Fundamental Theorem of Finitely Generated Abelian Groups. These results generalize the theorem that every finite dimensional vector space has a basis.

In Part VI of the book we shall study modules over certain noncommutative rings (group rings) and see that this theory in some sense generalizes both the study of $F[x]$-modules in Chapter 12 and the notion of a permutation representation of a finite group.

We establish a submodule criterion analogous to that for subgroups of a group in Section 2.1.

Proposition 1. *(The Submodule Criterion)* Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if

(1) $N \neq \emptyset$, and

(2) $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$.

Proof: If N is a submodule, then $0 \in N$ so $N \neq \emptyset$. Also N is closed under addition and is sent to itself under the action of elements of R. Conversely, suppose (1) and (2) hold. Let $r = -1$ and apply the subgroup criterion (in additive form) to see that N is a subgroup of M. In particular, $0 \in N$. Now let $x = 0$ and apply hypothesis (2) to see that N is sent to itself under the action of R. This establishes the proposition.

We end this section with an important definition and some examples.

Definition. Let R be a commutative ring with identity. An *R-algebra* is a ring A with identity together with a ring homomorphism $f : R \to A$ mapping 1_R to 1_A such that the subring $f(R)$ of A is contained in the center of A.

If A is an R-algebra then it is easy to check that A has a natural left and right (unital) R-module structure defined by $r \cdot a = a \cdot r = f(r)a$ where $f(r)a$ is just the multiplication in the ring A (and this is the same as $af(r)$ since by assumption $f(r)$ lies in the center of A). In general it is possible for an R-algebra A to have other left (or right) R-module structures, but unless otherwise stated, this natural module structure on an algebra will be assumed.

Definition. If A and B are two R-algebras, an *R-algebra homomorphism* (or isomorphism) is a ring homomorphism (isomorphism, respectively) $\varphi : A \to B$ mapping 1_A to 1_B such that $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R$ and $a \in A$.

Examples

Let R be a commutative ring with 1.

(1) Any ring with identity is a $\mathbb{Z}$-algebra.

(2) For any ring A with identity, if R is a subring of the center of A containing the identity of A then A is an R-algebra. In particular, a commutative ring A containing 1 is an R-algebra for any subring R of A containing 1. For example, the polynomial ring $R[x]$ is an R-algebra, the polynomial ring over R in any number of variables is an R-algebra, and the group ring RG for a finite group G is an R-algebra (cf. Section 7.2).

(3) If A is an R-algebra then the R-module structure of A depends only on the subring $f(R)$ contained in the center of A as in the previous example. If we replace R by its image $f(R)$ we see that "up to a ring homomorphism" every algebra A arises from a subring of the center of A that contains 1_A.

(4) A special case of the previous example occurs when $R = F$ is a *field*. In this case F is *isomorphic* to its image under f, so we can identify F itself as a subring of A. Hence, saying that A is an algebra over a field F is the same as saying that the ring A contains the field F in its center and the identity of A and of F are the same (this last condition is necessary, cf. Exercise 23).

Suppose that A is an R-algebra. Then A is a ring with identity that is a (unital) left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$ (these are all equal to the product $f(r)ab$ in the ring A—recall that $f(R)$ is contained in the center of A). Conversely, these conditions on a ring A define an R-algebra, and are sometimes used as the definition of an R-algebra (cf. Exercise 22).

EXERCISES

In these exercises R is a ring with 1 and M is a left R-module.

1. Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

2. Prove that $R^\times$ and M satisfy the two axioms in Section 1.7 for a *group action* of the multiplicative group $R^\times$ on the set M.

3. Assume that $rm = 0$ for some $r \in R$ and some $m \in M$ with $m \neq 0$. Prove that r does not have a left inverse (i.e., there is no $s \in R$ such that $sr = 1$).

4. Let M be the module R^n described in Example 3 and let $I_1, I_2, \ldots, I_n$ be left ideals of R. Prove that the following are submodules of M:

(a) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in I_i\}$

(b) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in R \text{ and } x_1 + x_2 + \cdots + x_n = 0\}$.

5. For any left ideal I of R define

$$IM = \{\sum_{\text{finite}} a_i m_i \mid a_i \in I,\ m_i \in M\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

6. Show that the intersection of any nonempty collection of submodules of an R-module is a submodule.

7. Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules of M. Prove that $\cup_{i=1}^{\infty} N_i$ is a submodule of M.

8. An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted

$$\text{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

   (a) Prove that if R is an integral domain then $\text{Tor}(M)$ is a submodule of M (called the *torsion* submodule of M).
   (b) Give an example of a ring R and an R-module M such that $\text{Tor}(M)$ is not a submodule. [Consider the torsion elements in the R-module R.]
   (c) If R has zero divisors show that every nonzero R-module has nonzero torsion elements.

9. If N is a submodule of M, the *annihilator of N in R* is defined to be $\{r \in R \mid rn = 0 \text{ for all } n \in N\}$. Prove that the annihilator of N in R is a 2-sided ideal of R.

10. If I is a right ideal of R, the *annihilator of I in M* is defined to be $\{m \in M \mid am = 0 \text{ for all } a \in I\}$. Prove that the annihilator of I in M is a submodule of M.

11. Let M be the abelian group (i.e., $\mathbb{Z}$-module) $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.
   (a) Find the annihilator of M in $\mathbb{Z}$ (i.e., a generator for this principal ideal).
   (b) Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups.

12. In the notation of the preceding exercises prove the following facts about annihilators.
   (a) Let N be a submodule of M and let I be its annihilator in R. Prove that the annihilator of I in M contains N. Give an example where the annihilator of I in M does not equal N.
   (b) Let I be a right ideal of R and let N be its annihilator in M. Prove that the annihilator of N in R contains I. Give an example where the annihilator of N in R does not equal I.

13. Let I be an ideal of R. Let M' be the subset of elements a of M that are annihilated by some power, I^k, of the ideal I, where the power may depend on a. Prove that M' is a submodule of M. [Use Exercise 7.]

14. Let z be an element of the center of R, i.e., $zr = rz$ for all $r \in R$. Prove that zM is a submodule of M, where $zM = \{zm \mid m \in M\}$. Show that if R is the ring of 2×2 matrices over a field and e is the matrix with a 1 in position 1,1 and zeros elsewhere then eR is *not* a left R-submodule (where $M = R$ is considered as a left R-module as in Example 1) — in this case the matrix e is not in the center of R.

15. If M is a finite abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?

16. Prove that the submodules U_k described in the example of $F[x]$-modules are all of the $F[x]$-submodules for the shift operator.

17. Let T be the shift operator on the vector space V and let $e_1, \ldots, e_n$ be the usual basis vectors described in the example of $F[x]$-modules. If $m \geq n$ find $(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0)e_n$.

18. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by $\pi/2$ radians. Show that V and 0 are the only $F[x]$-submodules for this T.

19. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is projection onto the y-axis. Show that V, 0, the x-axis and the y-axis are the only $F[x]$-submodules for this T.

20. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by π radians. Show that *every* subspace of V is an

$F[x]$-submodule for this T.

21. Let $n \in \mathbb{Z}^+$, $n > 1$ and let R be the ring of $n \times n$ matrices with entries from a field F. Let M be the set of $n \times n$ matrices with arbitrary elements of F in the first column and zeros elsewhere. Show that M is a submodule of R when R is considered as a left module over itself, but M is not a submodule of R when R is considered as a right R-module.

22. Suppose that A is a ring with identity 1_A that is a (unital) left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$. Prove that the map $f : R \to A$ defined by $f(r) = r \cdot 1_A$ is a ring homomorphism mapping 1_R to 1_A and that $f(R)$ is contained in the center of A. Conclude that A is an R-algebra and that the R-module structure on A induced by its algebra structure is precisely the original R-module structure.

23. Let A be the direct product ring $\mathbb{C} \times \mathbb{C}$ (cf. Section 7.6). Let τ_1 denote the identity map on $\mathbb{C}$ and let τ_2 denote complex conjugation. For any pair $p, q \in \{1, 2\}$ (not necessarily distinct) define

$$f_{p,q} : \mathbb{C} \to \mathbb{C} \times \mathbb{C} \qquad \text{by} \qquad f_{p,q}(z) = (\tau_p(z), \tau_q(z)).$$

So, for example, $f_{2,1} : z \mapsto (\bar{z}, z)$, where $\bar{z}$ is the complex conjugate of z, i.e., $\tau_2(z)$.

(a) Prove that each $f_{p,q}$ is an injective ring homomorphism, and that they all agree on the subfield $\mathbb{R}$ of $\mathbb{C}$. Deduce that A has four distinct $\mathbb{C}$-algebra structures. Explicitly give the action $z \cdot (u, v)$ of a complex number z on an ordered pair in A in each case.

(b) Prove that if $f_{p,q} \neq f_{p',q'}$ then the identity map on A is *not* a $\mathbb{C}$-algebra homomorphism from A considered as a $\mathbb{C}$-algebra via $f_{p,q}$ to A considered a $\mathbb{C}$-algebra via $f_{p',q'}$ (although the identity is an $\mathbb{R}$-algebra isomorphism).

(c) Prove that for any pair p, q there is some ring isomorphism from A to itself such that A is isomorphic as a $\mathbb{C}$-algebra via $f_{p,q}$ to A considered as $\mathbb{C}$-algebra via $f_{1,1}$ (the "natural" $\mathbb{C}$-algebra structure on A).

Remark: In the preceding exercise $A = \mathbb{C} \times \mathbb{C}$ is not a $\mathbb{C}$-algebra over either of the direct factor component copies of $\mathbb{C}$ (for example the subring $\mathbb{C} \times 0 \cong \mathbb{C}$) since it is not a unital module over these copies of $\mathbb{C}$ (the 1 of these subrings is not the same as the 1 of A).

10.2 QUOTIENT MODULES AND MODULE HOMOMORPHISMS

This section contains the basic theory of quotient modules and module homomorphisms.

Definition. Let R be a ring and let M and N be R-modules.

(1) A map $\varphi : M \to N$ is an *R-module homomorphism* if it respects the R-module structures of M and N, i.e.,

(a) $\varphi(x + y) = \varphi(x) + \varphi(y)$, for all $x, y \in M$ and

(b) $\varphi(rx) = r\varphi(x)$, for all $r \in R$, $x \in M$.

(2) An R-module homomorphism is an *isomorphism (of R-modules)* if it is both injective and surjective. The modules M and N are said to be *isomorphic*, denoted $M \cong N$, if there is some R-module isomorphism $\varphi : M \to N$.

(3) If $\varphi : M \to N$ is an R-module homomorphism, let $\ker \varphi = \{m \in M \mid \varphi(m) = 0\}$ (the *kernel* of φ) and let $\varphi(M) = \{n \in N \mid n = \varphi(m) \text{ for some } m \in M\}$ (the *image* of φ, as usual).

(4) Let M and N be R-modules and define $\text{Hom}_R(M, N)$ to be the set of all R-module homomorphisms from M into N.

Any R-module homomorphism is also a homomorphism of the additive groups, but not every group homomorphism need be a module homomorphism (because condition (b) may not be satisfied). The unqualified term "isomorphism" when applied to R-modules will always mean R-module isomorphism. When the symbol $\cong$ is used without qualification it will denote an isomorphism of the respective structures (which will be evident from the context).

It is an easy exercise using the submodule criterion (Proposition 1) to show that kernels and images of R-module homomorphisms are submodules.

Examples

(1) If R is a ring and $M = R$ is a module over itself, then R-module homomorphisms (even from R to itself) need not be ring homomorphisms and ring homomorphisms need not be R-module homomorphisms. For example, when $R = \mathbb{Z}$ the $\mathbb{Z}$-module homomorphism $x \mapsto 2x$ is not a ring homomorphism (1 does not map to 1). When $R = F[x]$ the ring homomorphism $\varphi : f(x) \mapsto f(x^2)$ is not an $F[x]$-module homomorphism (if it were, we would have $x^2 = \varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = x$).

(2) Let R be a ring, let $n \in \mathbb{Z}^+$ and let $M = R^n$. One easily checks that for each $i \in \{1, \ldots, n\}$ the projection map

$$\pi_i : R^n \to R \quad \text{by} \quad \pi_i(x_1, \ldots, x_n) = x_i$$

is a surjective R-module homomorphism with kernel equal to the submodule of n-tuples which have a zero in position i.

(3) If R is a field, R-module homomorphisms are called *linear transformations*. These will be studied extensively in Chapter 11.

(4) For the ring $R = \mathbb{Z}$ the action of ring elements (integers) on any $\mathbb{Z}$-module amounts to just adding and subtracting within the (additive) abelian group structure of the module so that in this case condition (b) of a homomorphism is implied by condition (a). For example, $\varphi(2x) = \varphi(x + x) = \varphi(x) + \varphi(x) = 2\varphi(x)$, etc. It follows that

$\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms.

(5) Let R be a ring, let I be a 2-sided ideal of R and suppose M and N are R-modules annihilated by I (i.e., $am = 0$ and $an = 0$ for all $a \in I$, $n \in N$ and $m \in M$). Any R-module homomorphism from N to M is then automatically a homomorphism of (R/I)-modules (see Example 5 of Section 1). In particular, if A is an additive abelian group such that for some prime p, $px = 0$ for all $x \in A$, then any group homomorphism from A to itself is a $\mathbb{Z}/p\mathbb{Z}$-module homomorphism, i.e., is a linear transformation over the field $\mathbb{F}_p$. In particular, the group of all (group) automorphisms of A is the group of invertible linear transformations from A to itself: $GL(A)$.

Proposition 2. Let M, N and L be R-modules.

(1) A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $x, y \in M$ and all $r \in R$.

(2) Let φ, ψ be elements of $\mathrm{Hom}_R(M, N)$. Define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \qquad \text{for all } m \in M.$$

Then $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ and with this operation $\mathrm{Hom}_R(M, N)$ is an abelian group. If R is a commutative ring then for $r \in R$ define $r\varphi$ by

$$(r\varphi)(m) = r(\varphi(m)) \qquad \text{for all } m \in M.$$

Then $r\varphi \in \mathrm{Hom}_R(M, N)$ and with this action of the commutative ring R the abelian group $\mathrm{Hom}_R(M, N)$ is an R-module.

(3) If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$ then $\psi \circ \varphi \in \mathrm{Hom}_R(L, N)$.

(4) With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M, M)$ is a ring with 1. When R is commutative $\mathrm{Hom}_R(M, M)$ is an R-algebra.

Proof: (1) Certainly $\varphi(rx+y) = r\varphi(x)+\varphi(y)$ if φ is an R-module homomorphism. Conversely, if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$, take $r = 1$ to see that φ is additive and take $y = 0$ to see that φ commutes with the action of R on M (i.e., is *homogeneous*).

(2) It is straightforward to check that all the abelian group and R-module axioms hold with these definitions — the details are left as an exercise. We note that the commutativity of R is used to show that $r\varphi$ satisfies the second axiom of an R-module homomorphism, namely,

$$\begin{aligned}
(r_1\varphi)(r_2m) &= r_1\varphi(r_2m) && \text{(by definition of } r_1\varphi) \\
&= r_1r_2(\varphi(m)) && \text{(since } \varphi \text{ is a homomorphism)} \\
&= r_2r_1\varphi(m) && \text{(since } R \text{ is commutative)} \\
&= r_2(r_1\varphi)(m) && \text{(by definition of } r_1\varphi).
\end{aligned}$$

Verification of the axioms relies ultimately on the hypothesis that N is an R-module. The domain M could in fact be any set — it does not have to be an R-module nor an abelian group.

(3) Let φ and ψ be as given and let $r \in R$, $x, y \in L$. Then

$$\begin{aligned}
(\psi \circ \varphi)(rx + y) &= \psi(\varphi(rx + y)) \\
&= \psi(r\varphi(x) + \varphi(y)) && \text{(by (1) applied to } \varphi) \\
&= r\psi(\varphi(x)) + \psi(\varphi(y)) && \text{(by (1) applied to } \psi) \\
&= r(\psi \circ \varphi)(x) + (\psi \circ \varphi)(y)
\end{aligned}$$

so, by (1), $\psi \circ \varphi$ is an R-module homomorphism.

(4) Note that since the domain and codomain of the elements of $\mathrm{Hom}_R(M, M)$ are the same, function composition is defined. By (3), it is a binary operation on $\mathrm{Hom}_R(M, M)$. As usual, function composition is associative. The remaining ring axioms are straightforward to check — the details are left as an exercise. The identity function, I, (as usual, $I(x) = x$, for all $x \in M$) is seen to be the multiplicative identity of $\mathrm{Hom}_R(M, M)$. If R is commutative, then (2) shows that the ring $\mathrm{Hom}_R(M, M)$ is a left R-module and defining $\varphi r = r\varphi$ for all $\varphi \in \mathrm{Hom}_R(M, M)$ and $r \in R$ makes $\mathrm{Hom}_R(M, M)$ into an R-algebra.

Definition. The ring $\mathrm{Hom}_R(M, M)$ is called the *endomorphism ring of* M and will often be denoted by $\mathrm{End}_R(M)$, or just $\mathrm{End}(M)$ when the ring R is clear from the context. Elements of $\mathrm{End}(M)$ are called *endomorphisms*.

When R is commutative there is a natural map from R into End(M) given by $r \mapsto rI$, where the latter endomorphism of M is just multiplication by r on M (cf. Exercise 7). The image of R is contained in the center of End(M) so if R has an identity, End(M) is an R-algebra. The ring homomorphism (cf. Exercise 7) from R to $\text{End}_R(M)$ may not be injective since for some r we may have $rm = 0$ for all $m \in M$ (e.g., $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$, and $r = 2$). When R is a field, however, this map is injective (in general, no unit is in the kernel of this map) and the copy of R in $\text{End}_R(M)$ is called the (subring of) *scalar transformations*.

Next we prove that every submodule N of an R-module M is "normal" in the sense that we can *always* form the quotient module M/N, and the natural projection $\pi : M \to M/N$ is an R-module homomorphism with kernel N. The proof of this fact and, more generally, the subsequent proofs of the isomorphism theorems for modules follow easily from the corresponding facts for groups. The reason for this is because a module is first of all an *abelian* group and so *every* submodule is automatically a normal subgroup and any module homomorphism is, in particular, a homomorphism of abelian groups, all of which we have already considered in Chapter 3. What remains to be proved in order to extend results on abelian groups to corresponding results on modules is to check that the action of R is compatible with these group quotients and homomorphisms. For example, the map π above was shown to be a group homomorphism in Chapter 3 but the abelian group M/N must be shown to be an R-module (i.e., to have an action by R) and property (b) in the definition of a module homomorphism must be checked for π.

Proposition 3. Let R be a ring, let M be an R-module and let N be a submodule of M. The (additive, abelian) quotient group M/N can be made into an R-module by defining an action of elements of R by

$$r(x + N) = (rx) + N, \qquad \text{for all } r \in R,\ x + N \in M/N.$$

The natural projection map $\pi : M \to M/N$ defined by $\pi(x) = x + N$ is an R-module homomorphism with kernel N.

Proof: Since M is an abelian group under $+$ the quotient group M/N is defined and is an abelian group. To see that the action of the ring element r on the coset $x+N$ is well defined, suppose $x+N = y+N$, i.e., $x-y \in N$. Since N is a (left) R-submodule, $r(x - y) \in N$. Thus $rx - ry \in N$ and $rx + N = ry + N$, as desired. Now since the operations in M/N are "compatible" with those of M, the axioms for an R-module are easily checked in the same way as was done for quotient groups. For example, axiom 2(b) holds as follows: for all $r_1, r_2 \in R$ and $x + N \in M/N$, by definition of the action of ring elements on elements of M/N

$$\begin{aligned}(r_1r_2)(x + N) &= (r_1r_2x) + N \\ &= r_1(r_2x + N) \\ &= r_1(r_2(x + N)).\end{aligned}$$

The other axioms are similarly checked — the details are left as an exercise. Finally, the natural projection map π described above is, in particular, the natural projection of the abelian group M onto the abelian group M/N hence is a group homomorphism with kernel N. The kernel of any module homomorphism is the same as its kernel when viewed as a homomorphism of the abelian group structures. It remains only to show π is a module homomorphism, i.e., $\pi(rm) = r\pi(m)$. But

$$\begin{aligned}\pi(rm) &= rm + N \\ &= r(m + N) \qquad \text{(by definition of the action of } R \text{ on } M/N) \\ &= r\pi(m).\end{aligned}$$

This completes the proof.

All the isomorphism theorems stated for groups also hold for R-modules. The proofs are similar to that of Proposition 3 above in that they begin by invoking the corresponding theorem for groups and then prove that the group homomorphisms are also R-module homomorphisms. To state the Second Isomorphism Theorem we need the following.

Definition. Let A, B be submodules of the R-module M. The *sum* of A and B is the set

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

One can easily check that the sum of two submodules A and B is a submodule and is the smallest submodule which contains both A and B.

Theorem 4. (Isomorphism Theorems)

(1) *(The First Isomorphism Theorem for Modules)* Let M, N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then $\ker\varphi$ is a submodule of M and $M/\ker\varphi \cong \varphi(M)$.

(2) *(The Second Isomorphism Theorem)* Let A, B be submodules of the R-module M. Then $(A + B)/B \cong A/(A \cap B)$.

(3) *(The Third Isomorphism Theorem)* Let M be an R-module, and let A and B be submodules of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.

(4) *(The Fourth or Lattice Isomorphism Theorem)* Let N be a submodule of the R-module M. There is a bijection between the submodules of M which contain N and the submodules of M/N. The correspondence is given by $A \leftrightarrow A/N$, for all $A \supseteq N$. This correspondence commutes with the processes of taking sums and intersections (i.e., is a lattice isomorphism between the lattice of submodules of M/N and the lattice of submodules of M which contain N).

Proof: Exercise.

EXERCISES

In these exercises R is a ring with 1 and M is a left R-module.

1. Use the submodule criterion to show that kernels and images of R-module homomorphisms are submodules.
2. Show that the relation "is R-module isomorphic to" is an equivalence relation on any set of R-modules.
3. Give an explicit example of a map from one R-module to another which is a group homomorphism but not an R-module homomorphism.
4. Let A be any $\mathbb{Z}$-module, let a be any element of A and let n be a positive integer. Prove that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi(\bar{k}) = ka$ is a well defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, where $A_n = \{a \in A \mid na = 0\}$ (so A_n is the annihilator in A of the ideal (n) of $\mathbb{Z}$ — cf. Exercise 10, Section 1).
5. Exhibit all $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$.
6. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n, m)\mathbb{Z}$.
7. Let z be a fixed element of the center of R. Prove that the map $m \mapsto zm$ is an R-module homomorphism from M to itself. Show that for a commutative ring R the map from R to $\mathrm{End}_R(M)$ given by $r \mapsto rI$ is a ring homomorphism (where I is the identity endomorphism).
8. Let $\varphi : M \to N$ be an R-module homomorphism. Prove that $\varphi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$ (cf. Exercise 8 in Section 1).
9. Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, M)$ and M are isomorphic as left R-modules. [Show that each element of $\mathrm{Hom}_R(R, M)$ is determined by its value on the identity of R.]
10. Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, R)$ and R are isomorphic as rings.
11. Let $A_1, A_2, \ldots, A_n$ be R-modules and let B_i be a submodule of A_i for each $i = 1, 2, \ldots, n$. Prove that
$$(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong (A_1/B_1) \times \cdots \times (A_n/B_n).$$
[Recall Exercise 14 in Section 5.1.]
12. Let I be a left ideal of R and let n be a positive integer. Prove
$$R^n/IR^n \cong R/IR \times \cdots \times R/IR \quad (n \text{ times})$$
where IR^n is defined as in Exercise 5 of Section 1. [Use the preceding exercise.]
13. Let I be a nilpotent ideal in a commutative ring R (cf. Exercise 37, Section 7.3), let M and N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Show that if the induced map $\overline{\varphi} : M/IM \to N/IN$ is surjective, then φ is surjective.
14. Let $R = \mathbb{Z}[x]$ be the ring of polynomials in x and let $A = \mathbb{Z}[t_1, t_2, \ldots]$ be the ring of polynomials in the independent indeterminates $t_1, t_2, \ldots$. Define an action of R on A as follows: 1) let $1 \in R$ act on A as the identity, 2) for $n \geq 1$ let $x^n \circ 1 = t_n$, let $x^n \circ t_i = t_{n+i}$ for $i = 1, 2, \ldots$, and let x^n act as 0 on monomials in A of (total) degree at least two, and 3) extend $\mathbb{Z}$-linearly, i.e., so that the module axioms 2(a) and 2(c) are satisfied.
   (a) Show that $x^{p+q} \circ t_i = x^p \circ (x^q \circ t_i) = t_{p+q+i}$ and use this to show that under this action the ring A is a (unital) R-module.
   (b) Show that the map $\varphi : R \to A$ defined by $\varphi(r) = r \circ 1_A$ is an R-module homomorphism of the ring R into the ring A mapping 1_R to 1_A, but is not a ring homomorphism from R to A.

10.3 GENERATION OF MODULES, DIRECT SUMS, AND FREE MODULES

Let R be a ring with 1. As in the preceding sections the term "module" will mean "left module." We first extend the notion of the sum of two submodules to sums of any finite number of submodules and define the submodule generated by a subset.

Definition. Let M be an R-module and let $N_1, \ldots, N_n$ be submodules of M.

(1) The *sum* of $N_1, \ldots, N_n$ is the set of all finite sums of elements from the sets N_i: $\{a_1 + a_2 + \cdots + a_n \mid a_i \in N_i \text{ for all } i\}$. Denote this sum by $N_1 + \cdots + N_n$.

(2) For any subset A of M let

$$RA = \{r_1a_1 + r_2a_2 + \cdots + r_ma_m \mid r_1, \ldots, r_m \in R,\ a_1, \ldots, a_m \in A,\ m \in \mathbb{Z}^+\}$$

(where by convention $RA = \{0\}$ if $A = \emptyset$). If A is the finite set $\{a_1, a_2, \ldots, a_n\}$ we shall write $Ra_1 + Ra_2 + \cdots + Ra_n$ for RA. Call RA the *submodule of M generated by A*. If N is a submodule of M (possibly $N = M$) and $N = RA$, for some subset A of M, we call A a *set of generators* or *generating set* for N, and we say N *is generated by* A.

(3) A submodule N of M (possibly $N = M$) is *finitely generated* if there is some finite subset A of M such that $N = RA$, that is, if N is generated by some finite subset.

(4) A submodule N of M (possibly $N = M$) is *cyclic* if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element:

$$N = Ra = \{ra \mid r \in R\}.$$

Note that these definitions do not require that the ring R contain a 1, however this condition ensures that A is contained in RA. It is easy to see using the Submodule Criterion that for any subset A of M, RA is indeed a submodule of M and is the smallest submodule of M which contains A (i.e., any submodule of M which contains A also contains RA). In particular, for submodules $N_1, \ldots, N_n$ of M, $N_1 + \cdots + N_n$ is just the submodule generated by the set $N_1 \cup \cdots \cup N_n$ and is the smallest submodule of M containing N_i, for all i. If $N_1, \ldots, N_n$ are generated by sets $A_1, \ldots, A_n$ respectively, then $N_1 + \cdots + N_n$ is generated by $A_1 \cup \cdots \cup A_n$. Note that cyclic modules are, a fortiori, finitely generated.

A submodule N of an R-module M may have many different generating sets (for instance the set N itself always generates N). If N is finitely generated, then there is a smallest nonnegative integer d such that N is generated by d elements (and no fewer). Any generating set consisting of d elements will be called a *minimal set of generators for N* (it is not unique in general). If N is not finitely generated, it need not have a minimal generating set.

The process of generating submodules of an R-module M by taking subsets A of M and forming all finite "R-linear combinations" of elements of A will be our primary way of producing submodules (this notion is perhaps familiar from vector space theory where it is referred to as taking the *span* of A). The obstruction which made the analogous process so difficult for groups in general was the noncommutativity of group

operations. For abelian groups, G, however, it was much simpler to control the subgroup $\langle A \rangle$ generated by A, for a subset A of G (see Section 2.4 for the complete discussion of this). The situation for R-modules is similar to that of abelian groups (even if R is a noncommutative ring) because we can always collect "like terms" in elements of A, i.e., terms such as $r_1a_1 + r_2a_2 + s_1a_1$ can always be simplified to $(r_1 + s_1)a_1 + r_2a_2$. This again reflects the underlying abelian group structure of modules.

Examples

(1) Let $R = \mathbb{Z}$ and let M be any R-module, that is, any abelian group. If $a \in M$, then $\mathbb{Z}a$ is just the cyclic subgroup of M generated by a: $\langle a \rangle$ (compare Definition 4 above with the definition of a cyclic group). More generally, M is generated as a $\mathbb{Z}$-module by a set A if and only if M is generated as a group by A (that is, the action of ring elements in this instance produces no elements that cannot already be obtained from A by addition and subtraction). The definition of finitely generated for $\mathbb{Z}$-modules is identical to that for abelian groups found in Chapter 5.

(2) Let R be a ring with 1 and let M be the (left) R-module R itself. Note that R is a finitely generated, in fact cyclic, R-module because $R = R1$ (i.e., we can take $A = \{1\}$). Recall that the submodules of R are precisely the left ideals of R, so saying I is a cyclic R-submodule of the left R-module R is the same as saying I is a principal ideal of R (usually the term "principal ideal" is used in the context of commutative rings). Also, saying I is a finitely generated R-submodule of R is the same as saying I is a finitely generated ideal. When R is a commutative ring we often write AR or aR for the submodule (ideal) generated by A or a respectively, as we have been doing for $\mathbb{Z}$ when we wrote $n\mathbb{Z}$. In this situation $AR = RA$ and $aR = Ra$ (elementwise as well). Thus a Principal Ideal Domain is a (commutative) integral domain R with identity in which every R-submodule of R is cyclic.

Submodules of a finitely generated module need not be finitely generated: take M to be the cyclic R-module R itself where R is the polynomial ring in infinitely many variables $x_1, x_2, x_3, \ldots$ with coefficients in some field F. The submodule (i.e., 2-sided ideal) generated by $\{x_1, x_2, \ldots\}$ cannot be generated by any finite set (note that one must show that *no* finite subset of this ideal will generate it).

(3) Let R be a ring with 1 and let M be the free module of rank n over R, as described in the first section. For each $i \in \{1, 2, \ldots, n\}$ let $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 appears in position i. Since

$$(s_1, s_2, \ldots, s_n) = \sum_{i=1}^{n} s_i e_i$$

it is clear that M is generated by $\{e_1, \ldots, e_n\}$. If R is commutative then this is a *minimal* generating set (cf. Exercises 2 and 27).

(4) Let F be a field, let x be an indeterminate, let V be a vector space over F and let T be a linear transformation from V to V. Make V into an $F[x]$-module via T. Then V is a *cyclic* $F[x]$-module (with generator v) if and only if $V = \{p(x)v \mid p(x) \in F[x]\}$, that is, if and only if every element of V can be written as an F-linear combination of elements of the set $\{T^n(v) \mid n \geq 0\}$. This in turn is equivalent to saying $\{v, T(v), T^2(v), \ldots\}$ span V as a vector space over F.

For instance if T is the identity linear transformation from V to V or the zero linear transformation, then for every $v \in V$ and every $p(x) \in F[x]$ we have $p(x)v = \alpha v$ for some $\alpha \in F$. Thus if V has dimension > 1, V cannot be a cyclic $F[x]$-module.

For another example suppose V is affine n-space and T is the "shift operator" described in Section 1. Let e_i be the i^{th} basis vector (as usual) numbered so that T is defined by $T^k(e_n) = e_{n-k}$ for $1 \leq k < n$. Thus V is spanned by the elements $e_n, T(e_n), \ldots, T^{n-1}(e_n)$, that is, V is a cyclic $F[x]$-module with generator e_n. For $n > 1$, V is not, however, a cyclic F-module (i.e., is not a 1-dimensional vector space over F).

Definition. Let $M_1, \ldots, M_k$ be a collection of R-modules. The collection of k-tuples $(m_1, m_2, \ldots, m_k)$ where $m_i \in M_i$ with addition and action of R defined componentwise is called the *direct product* of $M_1, \ldots, M_k$, denoted $M_1 \times \cdots \times M_k$.

It is evident that the direct product of a collection of R-modules is again an R-module. The direct product of $M_1, \ldots, M_k$ is also referred to as the *(external) direct sum* of $M_1, \ldots, M_k$ and denoted $M_1 \oplus \cdots \oplus M_k$. The direct product and direct sum of an infinite number of modules (which are different in general) are defined in Exercise 20.

The next proposition indicates when a module is isomorphic to the direct product of some of its submodules and is the analogue for modules of Theorem 9 in Section 5.4 (which determines when a group is the direct product of two of its subgroups).

Proposition 5. Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Then the following are equivalent:

(1) The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ defined by

$$\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$$

is an isomorphism (of R-modules): $N_1 + N_2 + \cdots + N_k \cong N_1 \times N_2 \times \cdots \times N_k$.

(2) $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all $j \in \{1, 2, \ldots, k\}$.

(3) Every $x \in N_1 + \cdots + N_k$ can be written *uniquely* in the form $a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i$.

Proof: To prove (1) implies (2), suppose for some j that (2) fails to hold and let $a_j \in (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) \cap N_j$, with $a_j \neq 0$. Then

$$a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k$$

for some $a_i \in N_i$, and $(a_1, \ldots, a_{j-1}, -a_j, a_{j+1}, \ldots, a_k)$ would be a nonzero element of $\ker \pi$, a contradiction.

Assume now that (2) holds. If for some module elements $a_i, b_i \in N_i$ we have

$$a_1 + a_2 + \cdots + a_k = b_1 + b_2 + \cdots + b_k$$

then for each j we have

$$a_j - b_j = (b_1 - a_1) + \cdots + (b_{j-1} - a_{j-1}) + (b_{j+1} - a_{j+1}) + \cdots + (b_k - a_k).$$

The left hand side is in N_j and the right side belongs to $N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k$. Thus

$$a_j - b_j \in N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0.$$

This shows $a_j = b_j$ for all j, and so (2) implies (3).

Finally, to see that (3) implies (1) observe first that the map π is clearly a surjective R-module homomorphism. Then (3) simply implies π is injective, hence is an isomorphism, completing the proof.

If an R-module $M = N_1 + N_2 + \cdots + N_k$ is the sum of submodules $N_1, N_2, \ldots, N_k$ of M satisfying the equivalent conditions of the proposition above, then M is said to be the *(internal) direct sum* of $N_1, N_2, \ldots, N_k$, written

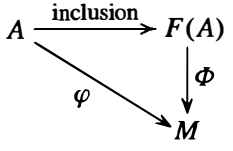
$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

By the proposition, this is equivalent to the assertion that every element m of M can be written *uniquely* as a sum of elements $m = n_1 + n_2 + \cdots + n_k$ with $n_i \in N_i$. (Note that part (1) of the proposition is the statement that the internal direct sum of $N_1, N_2, \ldots, N_k$ is isomorphic to their external direct sum, which is the reason we identify them and use the same notation for both.)

Definition. An R-module F is said to be *free* on the subset A of F if for every nonzero element x of F, there exist unique nonzero elements $r_1, r_2, \ldots, r_n$ of R and unique $a_1, a_2, \ldots, a_n$ in A such that $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, for some $n \in \mathbb{Z}^+$. In this situation we say A is a *basis* or *set of free generators* for F. If R is a commutative ring the cardinality of A is called the *rank* of F (cf. Exercise 27).

One should be careful to note the difference between the uniqueness property of direct sums (Proposition 5(3)) and the uniqueness property of free modules. Namely, in the direct sum of two modules, say $N_1 \oplus N_2$, each element can be written uniquely as $n_1 + n_2$; here the uniqueness refers to the *module elements* n_1 and n_2. In the case of free modules, the uniqueness is on the *ring elements as well as the module elements.* For example, if $R = \mathbb{Z}$ and $N_1 = N_2 = \mathbb{Z}/2\mathbb{Z}$, then each element of $N_1 \oplus N_2$ has a unique representation in the form $n_1 + n_2$ where each $n_i \in N_i$, however n_1 (for instance) can be expressed as n_1 or $3n_1$ or $5n_1 \ldots$ etc., so each element does not have a unique representation in the form $r_1a_1 + r_2a_2$, where $r_1, r_2 \in R$, $a_1 \in N_1$ and $a_2 \in N_2$. Thus $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module on the set $\{(1, 0), (0, 1)\}$. Similarly, it is not free on any set.

Theorem 6. For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following *universal property:* if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$, for all $a \in A$, that is, the following diagram commutes.



When A is the finite set $\{a_1, a_2, \ldots, a_n\}$, $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$. (Compare: Section 6.3, free groups.)

Proof: Let $F(A) = \{0\}$ if $A = \emptyset$. If A is nonempty let $F(A)$ be the collection of all set functions $f : A \to R$ such that $f(a) = 0$ for all but finitely many $a \in A$. Make

$F(A)$ into an R-module by pointwise addition of functions and pointwise multiplication of a ring element times a function, i.e.,

$$(f+g)(a) = f(a) + g(a) \quad \text{and}$$
$$(rf)(a) = r(f(a)), \qquad \text{for all } a \in A,\ r \in R \text{ and } f, g \in F(A).$$

It is an easy matter to check that all the R-module axioms hold (the details are omitted). Identify A as a subset of $F(A)$ by $a \mapsto f_a$, where f_a is the function which is 1 at a and zero elsewhere. We can, in this way, think of $F(A)$ as all finite R-linear combinations of elements of A by identifying each function f with the sum $r_1a_1 + r_2a_2 + \cdots + r_na_n$, where f takes on the value r_i at a_i and is zero at all other elements of A. Moreover, each element of $F(A)$ has a unique expression as such a formal sum. To establish the universal property of $F(A)$ suppose $\varphi : A \to M$ is a map of the set A into the R-module M. Define $\Phi : F(A) \to M$ by

$$\Phi : \sum_{i=1}^{n} r_i a_i \mapsto \sum_{i=1}^{n} r_i \varphi(a_i).$$

By the uniqueness of the expression for the elements of $F(A)$ as linear combinations of the a_i we see easily that Φ is a well defined R-module homomorphism (the details are left as an exercise). By definition, the restriction of Φ to A equals φ. Finally, since $F(A)$ is generated by A, once we know the values of an R-module homomorphism on A its values on every element of $F(A)$ are uniquely determined, so Φ is the unique extension of φ to all of $F(A)$.

When A is the finite set $\{a_1, a_2, \ldots, a_n\}$ Proposition 5(3) shows that $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$. Since $R \cong Ra_i$ for all i (under the map $r \mapsto ra_i$) Proposition 5(1) shows that the direct sum is isomorphic to R^n.

Corollary 7.

(1) If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.

(2) If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ does in Theorem 6.

Proof: Exercise.

If F is a free R-module with basis A, we shall often (particularly in the case of vector spaces) define R-module homomorphisms from F into other R-modules simply by specifying their values on the elements of A and then saying "*extend by linearity.*" Corollary 7(2) ensures that this is permissible.

When $R = \mathbb{Z}$, the free module on a set A is called the *free abelian group on A*. If $|A| = n$, $F(A)$ is called the free abelian group of *rank n* and is isomorphic to $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n times). These definitions agree with the ones given in Chapter 5.

EXERCISES

In these exercises R is a ring with 1 and M is a left R-module.

1. Prove that if A and B are sets of the same cardinality, then the free modules $F(A)$ and $F(B)$ are isomorphic.
2. Assume R is commutative. Prove that $R^n \cong R^m$ if and only if $n = m$, i.e., two free R-modules of finite rank are isomorphic if and only if they have the same rank. [Apply Exercise 12 of Section 2 with I a maximal ideal of R. You may assume that if F is a field, then $F^n \cong F^m$ if and only if $n = m$, i.e., two finite dimensional vector spaces over F are isomorphic if and only if they have the same dimension — this will be proved later in Section 11.1.]
3. Show that the $F[x]$-modules in Exercises 18 and 19 of Section 1 are both cyclic.
4. An R-module M is called a *torsion* module if for each $m \in M$ there is a nonzero element $r \in R$ such that $rm = 0$, where r may depend on m (i.e., $M = \mathrm{Tor}(M)$ in the notation of Exercise 8 of Section 1). Prove that every finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module.
5. Let R be an integral domain. Prove that every finitely generated torsion R-module has a nonzero annihilator i.e., there is a nonzero element $r \in R$ such that $rm = 0$ for all $m \in M$ — here r does not depend on m (the annihilator of a module was defined in Exercise 9 of Section 1). Give an example of a torsion R-module whose annihilator is the zero ideal.
6. Prove that if M is a finitely generated R-module that is generated by n elements then every quotient of M may be generated by n (or fewer) elements. Deduce that quotients of cyclic modules are cyclic.
7. Let N be a submodule of M. Prove that if both M/N and N are finitely generated then so is M.
8. Let S be the collection of sequences $(a_1, a_2, a_3, \ldots)$ of integers $a_1, a_2, a_3, \ldots$ where all but finitely many of the a_i are 0 (called the *direct sum* of infinitely many copies of $\mathbb{Z}$). Recall that S is a ring under componentwise addition and multiplication and S does not have a multiplicative identity — cf. Exercise 20, Section 7.1. Prove that S is not finitely generated as a module over itself.
9. An R-module M is called *irreducible* if $M \neq 0$ and if 0 and M are the only submodules of M. Show that M is irreducible if and only if $M \neq 0$ and M is a cyclic module with any nonzero element as generator. Determine all the irreducible $\mathbb{Z}$-modules.
10. Assume R is commutative. Show that an R-module M is irreducible if and only if M is isomorphic (as an R-module) to R/I where I is a maximal ideal of R. [By the previous exercise, if M is irreducible there is a natural map $R \to M$ defined by $r \mapsto rm$, where m is any fixed nonzero element of M.]
11. Show that if M_1 and M_2 are irreducible R-modules, then any nonzero R-module homomorphism from M_1 to M_2 is an isomorphism. Deduce that if M is irreducible then $\mathrm{End}_R(M)$ is a division ring (this result is called *Schur's Lemma*). [Consider the kernel and the image.]
12. Let R be a commutative ring and let A, B and M be R-modules. Prove the following isomorphisms of R-modules:
    (a) $\mathrm{Hom}_R(A \times B, M) \cong \mathrm{Hom}_R(A, M) \times \mathrm{Hom}_R(B, M)$
    (b) $\mathrm{Hom}_R(M, A \times B) \cong \mathrm{Hom}_R(M, A) \times \mathrm{Hom}_R(M, B)$.
13. Let R be a commutative ring and let F be a free R-module of finite rank. Prove the following isomorphism of R-modules: $\mathrm{Hom}_R(F, R) \cong F$.

14. Let R be a commutative ring and let F be the free R-module of rank n. Prove that $\mathrm{Hom}_R(F, M) \cong M \times \cdots \times M$ (n times). [Use Exercise 9 in Section 2 and Exercise 12.]

15. An element $e \in R$ is called a *central idempotent* if $e^2 = e$ and $er = re$ for all $r \in R$. If e is a central idempotent in R, prove that $M = eM \oplus (1-e)M$. [Recall Exercise 14 in Section 1.]

The next two exercises establish the Chinese Remainder Theorem for modules (cf. Section 7.6).

16. For any ideal I of R let IM be the submodule defined in Exercise 5 of Section 1. Let $A_1, \ldots, A_k$ be any ideals in the ring R. Prove that the map

$$M \to M/A_1M \times \cdots \times M/A_kM \quad \text{defined by} \quad m \mapsto (m + A_1M, \ldots, m + A_kM)$$

is an R-module homomorphism with kernel $A_1M \cap A_2M \cap \cdots \cap A_kM$.

17. In the notation of the preceding exercise, assume further that the ideals $A_1, \ldots, A_k$ are pairwise comaximal (i.e., $A_i + A_j = R$ for all $i \neq j$). Prove that

$$M/(A_1 \cdots A_k)M \cong M/A_1M \times \cdots \times M/A_kM.$$

[See the proof of the Chinese Remainder Theorem for rings in Section 7.6.]

18. Let R be a Principal Ideal Domain and let M be an R-module that is annihilated by the nonzero, proper ideal (a). Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the unique factorization of a into distinct prime powers in R. Let M_i be the annihilator of $p_i^{\alpha_i}$ in M, i.e., M_i is the set $\{m \in M \mid p_i^{\alpha_i} m = 0\}$ — called the *p_i-primary component of M*. Prove that

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_k.$$

19. Show that if M is a finite abelian group of order $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then, considered as a $\mathbb{Z}$-module, M is annihilated by (a), the p_i-primary component of M is the unique Sylow p_i-subgroup of M and M is isomorphic to the direct product of its Sylow subgroups.

20. Let I be a nonempty index set and for each $i \in I$ let M_i be an R-module. The *direct product* of the modules M_i is defined to be their direct product as abelian groups (cf. Exercise 15 in Section 5.1) with the action of R componentwise multiplication. The *direct sum* of the modules M_i is defined to be the restricted direct product of the abelian groups M_i (cf. Exercise 17 in Section 5.1) with the action of R componentwise multiplication. In other words, the direct sum of the M_i's is the subset of the direct product, $\prod_{i \in I} M_i$, which consists of all elements $\prod_{i \in I} m_i$ such that only finitely many of the components m_i are nonzero; the action of R on the direct product or direct sum is given by $r \prod_{i \in I} m_i = \prod_{i \in I} rm_i$ (cf. Appendix I for the definition of Cartesian products of infinitely many sets). The direct sum will be denoted by $\oplus_{i \in I} M_i$.

- **(a)** Prove that the direct product of the M_i's is an R-module and the direct sum of the M_i's is a submodule of their direct product.
- **(b)** Show that if $R = \mathbb{Z}$, $I = \mathbb{Z}^+$ and M_i is the cyclic group of order i for each i, then the direct sum of the M_i's is not isomorphic to their direct product. [Look at torsion.]

21. Let I be a nonempty index set and for each $i \in I$ let N_i be a submodule of M. Prove that the following are equivalent:

- **(i)** the submodule of M generated by all the N_i's is isomorphic to the direct sum of the N_i's
- **(ii)** if $\{i_1, i_2, \ldots, i_k\}$ is any finite subset of I then $N_{i_1} \cap (N_{i_2} + \cdots + N_{i_k}) = 0$
- **(iii)** if $\{i_1, i_2, \ldots, i_k\}$ is any finite subset of I then $N_1 + \cdots + N_k = N_1 \oplus \cdots \oplus N_k$
- **(iv)** for every element x of the submodule of M generated by the N_i's there are unique elements $a_i \in N_i$ for all $i \in I$ such that all but a finite number of the a_i are zero and x is the (finite) sum of the a_i.

22. Let R be a Principal Ideal Domain, let M be a torsion R-module (cf. Exercise 4) and let p be a prime in R (do not assume M is finitely generated, hence it need not have a nonzero annihilator — cf. Exercise 5). The *p-primary component* of M is the set of all elements of M that are annihilated by some positive power of p.

(a) Prove that the p-primary component is a submodule. [See Exercise 13 in Section 1.]

(b) Prove that this definition of p-primary component agrees with the one given in Exercise 18 when M has a nonzero annihilator.

(c) Prove that M is the (possibly infinite) direct sum of its p-primary components, as p runs over all primes of R.

23. Show that any direct sum of free R-modules is free.

24. *(An arbitrary direct product of free modules need not be free)* For each positive integer i let M_i be the free $\mathbb{Z}$-module $\mathbb{Z}$, and let M be the direct product $\prod_{i\in\mathbb{Z}^+} M_i$ (cf. Exercise 20). Each element of M can be written uniquely in the form $(a_1, a_2, a_3, \dots)$ with $a_i \in \mathbb{Z}$ for all i. Let N be the submodule of M consisting of all such tuples with only finitely many nonzero a_i. Assume M is a free $\mathbb{Z}$-module with basis $\mathcal{B}$.

(a) Show that N is countable.

(b) Show that there is some countable subset $\mathcal{B}_1$ of $\mathcal{B}$ such that N is contained in the submodule, N_1, generated by $\mathcal{B}_1$. Show also that N_1 is countable.

(c) Let $\overline{M} = M/N_1$. Show that $\overline{M}$ is a free $\mathbb{Z}$-module. Deduce that if $\overline{x}$ is any nonzero element of $\overline{M}$ then there are only finitely many distinct positive integers k such that $\overline{x} = k\overline{m}$ for some $m \in M$ (depending on k).

(d) Let $\mathcal{S} = \{(b_1, b_2, b_3, \dots) \mid b_i = \pm i! \text{ for all } i\}$. Prove that $\mathcal{S}$ is uncountable. Deduce that there is some $s \in \mathcal{S}$ with $s \notin N_1$.

(e) Show that the assumption M is free leads to a contradiction: By (d) we may choose $s \in \mathcal{S}$ with $s \notin N_1$. Show that for each positive integer k there is some $m \in M$ with $\overline{s} = k\overline{m}$, contrary to (c). [Use the fact that $N \subseteq N_1$.]

25. In the construction of direct limits, Exercise 8 of Section 7.6, show that if all A_i are R-modules and the maps ρ_{ij} are R-module homomorphisms, then the direct limit $A = \varinjlim A_i$ may be given the structure of an R-module in a natural way such that the maps $\rho_i : A_i \to A$ are all R-module homomorphisms. Verify the corresponding universal property (part (e)) for R-module homomorphisms $\varphi_i : A_i \to C$ commuting with the ρ_{ij}.

26. Carry out the analysis of the preceding exercise corresponding to inverse limits to show that an inverse limit of R-modules is an R-module satisfying the appropriate universal property (cf. Exercise 10 of Section 7.6).

27. *(Free modules over noncommutative rings need not have a unique rank)* Let M be the $\mathbb{Z}$-module $\mathbb{Z} \times \mathbb{Z} \times \cdots$ of Exercise 24 and let R be its endomorphism ring, $R = \mathrm{End}_{\mathbb{Z}}(M)$ (cf. Exercises 29 and 30 in Section 7.1). Define $\varphi_1, \varphi_2 \in R$ by

$$\varphi_1(a_1, a_2, a_3, \dots) = (a_1, a_3, a_5, \dots)$$
$$\varphi_2(a_1, a_2, a_3, \dots) = (a_2, a_4, a_6, \dots)$$

(a) Prove that $\{\varphi_1, \varphi_2\}$ is a free basis of the left R-module R. [Define the maps ψ_1 and ψ_2 by $\psi_1(a_1, a_2, \dots) = (a_1, 0, a_2, 0, \dots)$ and $\psi_2(a_1, a_2, \dots) = (0, a_1, 0, a_2, \dots)$. Verify that $\varphi_i\psi_i = 1$, $\varphi_1\psi_2 = 0 = \varphi_2\psi_1$ and $\psi_1\varphi_1 + \psi_2\varphi_2 = 1$. Use these relations to prove that φ_1, φ_2 are independent and generate R as a left R-module.]

(b) Use (a) to prove that $R \cong R^2$ and deduce that $R \cong R^n$ for all $n \in \mathbb{Z}^+$.

10.4 TENSOR PRODUCTS OF MODULES

In this section we study the tensor product of two modules M and N over a ring (not necessarily commutative) containing 1. Formation of the tensor product is a general construction that, loosely speaking, enables one to form another module in which one can take "products" mn of elements $m \in M$ and $n \in N$. The general construction involves various left- and right- module actions, and it is instructive, by way of motivation, to first consider an important special case: the question of "extending scalars" or "changing the base."

Suppose that the ring R is a subring of the ring S. Throughout this section, we always assume that $1_R = 1_S$ (this ensures that S is a unital R-module).

If N is a left S-module, then N can also be naturally considered as a left R-module since the elements of R (being elements of S) act on N by assumption. The S-module axioms for N include the relations

$$(s_1 + s_2)n = s_1n + s_2n \quad \text{and} \quad s(n_1 + n_2) = sn_1 + sn_2 \tag{10.1}$$

for all $s, s_1, s_2 \in S$ and all $n, n_1, n_2 \in N$, and the relation

$$(s_1s_2)n = s_1(s_2n) \quad \text{for all } s_1, s_2 \in S, \text{ and all } n \in N. \tag{10.2}$$

A particular case of the latter relation is

$$(sr)n = s(rn) \quad \text{for all } s \in S, r \in R \text{ and } n \in N. \tag{10.2'}$$

More generally, if $f : R \to S$ is a ring homomorphism from R into S with $f(1_R) = 1_S$ (for example the injection map if R is a subring of S as above) then it is easy to see that N can be considered as an R-module with $rn = f(r)n$ for $r \in R$ and $n \in N$. In this situation S can be considered as an *extension* of the ring R and the resulting R-module is said to be obtained from N by *restriction of scalars* from S to R.

Suppose now that R is a subring of S and we try to reverse this, namely we start with an R-module N and attempt to define an S-module structure on N that extends the action of R on N to an action of S on N (hence "extending the scalars" from R to S). In general this is impossible, even in the simplest situation: the ring R itself is an R-module but is usually not an S-module for the larger ring S. For example, $\mathbb{Z}$ is a $\mathbb{Z}$-module but it cannot be made into a $\mathbb{Q}$-module (if it could, then $\frac{1}{2} \circ 1 = z$ would be an element of $\mathbb{Z}$ with $z + z = 1$, which is impossible). Although $\mathbb{Z}$ itself cannot be made into a $\mathbb{Q}$-module it is *contained* in a $\mathbb{Q}$-module, namely $\mathbb{Q}$ itself. Put another way, there is an injection (also called an *embedding*) of the $\mathbb{Z}$-module $\mathbb{Z}$ into the $\mathbb{Q}$-module $\mathbb{Q}$ (and similarly the ring R can always be embedded as an R-submodule of the S-module S). This raises the question of whether an arbitrary R-module N can be embedded as an R-submodule of some S-module, or more generally, the question of what R-module homomorphisms exist from N to S-modules. For example, suppose N is a nontrivial *finite* abelian group, say $N = \mathbb{Z}/2\mathbb{Z}$, and consider possible $\mathbb{Z}$-module homomorphisms (i.e., abelian group homomorphisms) of N into some $\mathbb{Q}$-module. A $\mathbb{Q}$-module is just a vector space over $\mathbb{Q}$ and every nonzero element in a vector space over $\mathbb{Q}$ has infinite (additive) order. Since every element of N has finite order, every element of N must map to 0 under such a homomorphism. In other words there are *no* nonzero $\mathbb{Z}$-module homomorphisms from this N to *any* $\mathbb{Q}$-module, much less embeddings of N identifying

N as a submodule of a $\mathbb{Q}$-module. The two $\mathbb{Z}$-modules $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ exhibit extremely different behaviors when we try to "extend scalars" from $\mathbb{Z}$ to $\mathbb{Q}$: the first module maps injectively into some $\mathbb{Q}$-module, the second always maps to 0 in a $\mathbb{Q}$-module.

We now construct for a general R-module N an S-module that is the "best possible" target in which to try to embed N. We shall also see that this module determines *all* of the possible R-module homomorphisms of N into S-modules, in particular determining when N is contained in some S-module (cf. Corollary 9). In the case of $R = \mathbb{Z}$ and $S = \mathbb{Q}$ this construction will give us $\mathbb{Q}$ when applied to the module $N = \mathbb{Z}$, and will give us 0 when applied to the module $N = \mathbb{Z}/2\mathbb{Z}$ (Examples 2 and 3 following Corollary 9).

If the R-module N were already an S-module then of course there is no difficulty in "extending" the scalars from R to S, so we begin the construction by returning to the basic module axioms in order to examine whether we can define "products" of the form sn, for $s \in S$ and $n \in N$. These axioms start with an abelian group N together with a map from $S \times N$ to N, where the image of the pair (s, n) is denoted by sn. It is therefore natural to consider the free $\mathbb{Z}$-module (i.e., , the free abelian group) on the set $S \times N$, i.e., the collection of all finite commuting sums of elements of the form (s_i, n_i) where $s_i \in S$ and $n_i \in N$. This is an abelian group where there are no relations between any distinct pairs (s, n) and (s', n'), i.e., no relations between the "formal products" sn, and in this abelian group the original module N has been thoroughly distinguished from the new "coefficients" from S. To satisfy the relations necessary for an S-module structure imposed in equation (1) and the compatibility relation with the action of R on N in (2′), we must take the quotient of this abelian group by the subgroup H generated by all elements of the form

$$\begin{gathered}(s_1 + s_2, n) - (s_1, n) - (s_2, n), \\ (s, n_1 + n_2) - (s, n_1) - (s, n_2), \text{ and} \\ (sr, n) - (s, rn),\end{gathered} \tag{10.3}$$

for $s, s_1, s_2 \in S$, $n, n_1, n_2 \in N$ and $r \in R$, where rn in the last element refers to the R-module structure already defined on N.

The resulting quotient group is denoted by $S \otimes_R N$ (or just $S \otimes N$ if R is clear from the context) and is called the *tensor product of S and N over R*. If $s \otimes n$ denotes the coset containing (s, n) in $S \otimes_R N$ then by definition of the quotient we have forced the relations

$$\begin{gathered}(s_1 + s_2) \otimes n = s_1 \otimes n + s_2 \otimes n, \\ s \otimes (n_1 + n_2) = s \otimes n_1 + s \otimes n_2, \text{ and} \\ sr \otimes n = s \otimes rn.\end{gathered} \tag{10.4}$$

The elements of $S \otimes_R N$ are called *tensors* and can be written (non-uniquely in general) as finite sums of "simple tensors" of the form $s \otimes n$ with $s \in S$, $n \in N$.

We now show that the tensor product $S \otimes_R N$ is naturally a left S-module under the action defined by

$$s\left(\sum_{\text{finite}} s_i \otimes n_i\right) = \sum_{\text{finite}} (ss_i) \otimes n_i. \tag{10.5}$$

We first check this is well defined, i.e., independent of the representation of the element of $S \otimes_R N$ as a sum of simple tensors. Note first that if s' is any element of S then

$$(s'(s_1 + s_2), n) - (s's_1, n) - (s's_2, n) \quad \big(= (s's_1 + s's_2, n) - (s's_1, n) - (s's_2, n)\big),$$
$$(s's, n_1 + n_2) - (s's, n_1) - (s's, n_2), \text{ and}$$
$$(s'(sr), n) - (s's, rn) \quad \big(= ((s's)r, n) - (s's, rn)\big)$$

each belongs to the set of generators in (3), so in particular each lies in the subgroup H. This shows that multiplying the first entries of the generators in (3) on the left by s' gives another element of H (in fact another generator). Since any element of H is a sum of elements as in (3), it follows that for any element $\sum(s_i, n_i)$ in H also $\sum(s's_i, n_i)$ lies in H. Suppose now that $\sum s_i \otimes n_i = \sum s_i' \otimes n_i'$ are two representations for the same element in $S \otimes_R N$. Then $\sum(s_i, n_i) - \sum(s_i', n_i')$ is an element of H, and by what we have just seen, for any $s \in S$ also $\sum(ss_i, n_i) - \sum(ss_i', n_i')$ is an element of H. But this means that $\sum ss_i \otimes n_i = \sum ss_i' \otimes n_i'$ in $S \otimes_R N$, so the expression in (5) is indeed well defined.

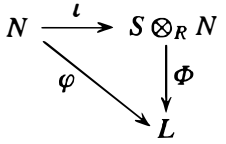
It is now straightforward using the relations in (4) to check that the action defined in (5) makes $S \otimes_R N$ into a left S-module. For example, on the simple tensor $s_i \otimes n_i$,

$$\begin{aligned}
(s + s')(s_i \otimes n_i) &= ((s + s')s_i) \otimes n_i && \text{by definition (5)} \\
&= (ss_i + s's_i) \otimes n_i \\
&= ss_i \otimes n_i + s's_i \otimes n_i && \text{by the first relation in (4)} \\
&= s(s_i \otimes n_i) + s'(s_i \otimes n_i) && \text{by definition (5)}.
\end{aligned}$$

The module $S \otimes_R N$ is called *the (left) S-module obtained by extension of scalars from the (left) R-module N.*

There is a natural map $\iota : N \to S \otimes_R N$ defined by $n \mapsto 1 \otimes n$ (i.e., first map $n \in N$ to the element $(1, n)$ in the free abelian group and then pass to the quotient group). Since $1 \otimes rn = r \otimes n = r(1 \otimes n)$ by (4) and (5), it is easy to check that ι is an R-module homomorphism from N to $S \otimes_R N$. Since we have passed to a quotient group, however, ι is not injective in general. Hence, while there is a natural R-module homomorphism from the original left R-module N to the left S-module $S \otimes_R N$, in general $S \otimes_R N$ need not contain (an isomorphic copy of) N. On the other hand, the relations in equation (3) were the *minimal* relations that we had to impose in order to obtain an S-module, so it is reasonable to expect that the tensor product $S \otimes_R N$ is the "best possible" S-module to serve as target for an R-module homomorphism from N. The next theorem makes this more precise by showing that any other R-module homomorphism from N factors through this one, and is referred to as the *universal property* for the tensor product $S \otimes_R N$. The analogous result for the general tensor product is given in Theorem 10.

Theorem 8. Let R be a subring of S, let N be a left R-module and let $\iota : N \to S \otimes_R N$ be the R-module homomorphism defined by $\iota(n) = 1 \otimes n$. Suppose that L is any left S-module (hence also an R-module) and that $\varphi : N \to L$ is an R-module homomorphism from N to L. Then there is a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ such that φ factors through Φ, i.e., $\varphi = \Phi \circ \iota$ and the diagram



commutes. Conversely, if $\Phi : S \otimes_R N \to L$ is an S-module homomorphism then $\varphi = \Phi \circ \iota$ is an R-module homomorphism from N to L.

Proof: Suppose $\varphi : N \to L$ is an R-module homomorphism to the S-module L. By the universal property of free modules (Theorem 6 in Section 3) there is a $\mathbb{Z}$-module homomorphism from the free $\mathbb{Z}$-module F on the set $S \times N$ to L that sends each generator (s, n) to $s\varphi(n)$. Since φ is an R-module homomorphism, the generators of the subgroup H in equation (3) all map to zero in L. Hence this $\mathbb{Z}$-module homomorphism factors through H, i.e., there is a well defined $\mathbb{Z}$-module homomorphism Φ from $F/H = S \otimes_R N$ to L satisfying $\Phi(s \otimes n) = s\varphi(n)$. Moreover, on simple tensors we have

$$s'\Phi(s \otimes n) = s'(s\varphi(n)) = (s's)\varphi(n) = \Phi((s's) \otimes n) = \Phi(s'(s \otimes n)).$$

for any $s' \in S$. Since Φ is additive it follows that Φ is an S-module homomorphism, which proves the existence statement of the theorem. The module $S \otimes_R N$ is generated as an S-module by elements of the form $1 \otimes n$, so any S-module homomorphism is uniquely determined by its values on these elements. Since $\Phi(1 \otimes n) = \varphi(n)$, it follows that the S-module homomorphism Φ is uniquely determined by φ, which proves the uniqueness statement of the theorem. The converse statement is immediate.

The universal property of $S \otimes_R N$ in Theorem 8 shows that R-module homomorphisms of N into S-modules arise from S-module homomorphisms from $S \otimes_R N$. In particular this determines when it is possible to map N injectively into some S-module:

Corollary 9. Let $\iota : N \to S \otimes_R N$ be the R-module homomorphism in Theorem 8. Then $N/\ker \iota$ is the unique largest quotient of N that can be embedded in any S-module. In particular, N can be embedded as an R-submodule of some left S-module if and only if ι is injective (in which case N is isomorphic to the R-submodule $\iota(N)$ of the S-module $S \otimes_R N$).

Proof: The quotient $N/\ker \iota$ is mapped injectively (by ι) into the S-module $S \otimes_R N$. Suppose now that φ is an R-module homomorphism injecting the quotient $N/\ker \varphi$ of N into an S-module L. Then, by Theorem 8, $\ker \iota$ is mapped to 0 by φ, i.e., $\ker \iota \subseteq \ker \varphi$. Hence $N/\ker \varphi$ is a quotient of $N/\ker \iota$ (namely, the quotient by the submodule $\ker \varphi/\ker \iota$). It follows that $N/\ker \iota$ is the unique largest quotient of N that can be embedded in any S-module. The last statement in the corollary follows immediately.

Examples

(1) For any ring R and any left R-module N we have $R \otimes_R N \cong N$ (so "extending scalars from R to R" does not change the module). This follows by taking φ to be the identity map from N to itself (and $S = R$) in Theorem 8: ι is then an isomorphism with inverse isomorphism given by Φ. In particular, if A is any abelian group (i.e., a $\mathbb{Z}$-module), then $\mathbb{Z} \otimes_{\mathbb{Z}} A = A$.

(2) Let $R = \mathbb{Z}$, $S = \mathbb{Q}$ and let A be a finite abelian group of order n. In this case the $\mathbb{Q}$-module $\mathbb{Q} \otimes_{\mathbb{Z}} A$ obtained by extension of scalars from the $\mathbb{Z}$-module A is 0. To see this, observe first that in any tensor product $1 \otimes 0 = 1 \otimes (0 + 0) = 1 \otimes 0 + 1 \otimes 0$, by the second relation in (4), so

$$1 \otimes 0 = 0.$$

Now, for any simple tensor $q \otimes a$ we can write the rational number q as $(q/n)n$. Then since $na = 0$ in A by Lagrange's Theorem, we have

$$q \otimes a = (\frac{q}{n} \cdot n) \otimes a = \frac{q}{n} \otimes (na) = (q/n) \otimes 0 = (q/n)(1 \otimes 0) = 0.$$

It follows that $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$. In particular, the map $\iota : A \to S \otimes_R A$ is the zero map. By Theorem 8, we see again that any homomorphism of a finite abelian group into a rational vector space is the zero map. In particular, if A is nontrivial, then the original $\mathbb{Z}$-module A is not contained in the $\mathbb{Q}$-module obtained by extension of scalars.

(3) *Extension of scalars for free modules:* If $N \cong R^n$ is a free module of rank n over R then $S \otimes_R N \cong S^n$ is a free module of rank n over S. We shall prove this shortly (Corollary 18) when we discuss tensor products of direct sums. For example, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q}^n$. In this case the module obtained by extension of scalars contains (an isomorphic copy of) the original R-module N. For example, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q}^n$ and $\mathbb{Z}^n$ is a subgroup of the abelian group $\mathbb{Q}^n$.

(4) *Extension of scalars for vector spaces:* As a special case of the previous example, let F be a subfield of the field K and let V be an n-dimensional vector space over F (i.e., $V \cong F^n$). Then $K \otimes_F V \cong K^n$ is a vector space over the larger field K of the same dimension, and the original vector space V is contained in $K \otimes_F V$ as an F-vector subspace.

(5) *Induced modules for finite groups:* Let R be a commutative ring with 1, let G be a finite group and let H be a subgroup of G. As in Section 7.2 we may form the group ring RG and its subring RH. For any RH-module N define the *induced module* $RG \otimes_{RH} N$. In this way we obtain an RG-module for each RH-module N. We shall study properties of induced modules and some of their important applications to group theory in Chapters 17 and 19.

The general tensor product construction follows along the same lines as the extension of scalars above, but before describing it we make two observations from this special case. The first is that the construction of $S \otimes_R N$ as an *abelian group* involved only the elements in equation (3), which in turn only required S to be a *right* R-module and N to be a *left* R-module. In a similar way we shall construct an *abelian group* $M \otimes_R N$ for *any right* R-module M and *any left* R-module N. The second observation is that the *S-module* structure on $S \otimes_R N$ defined by equation (5) required only a *left* S-module structure on S together with a "compatibility relation"

$$s'(sr) = (s's)r \qquad \text{for } s, s' \in S, r \in R,$$

between this left S-module structure and the right R-module structure on S (this was needed in order to deduce that (5) was well defined). We first consider the general construction of $M \otimes_R N$ as an abelian group, after which we shall return to the question of when this abelian group can be given a module structure.

Suppose then that N is a left R-module and that M is a right R-module. The quotient of the free $\mathbb{Z}$-module on the set $M \times N$ by the subgroup generated by all elements of the form

$$\begin{gathered}(m_1 + m_2, n) - (m_1, n) - (m_2, n), \\ (m, n_1 + n_2) - (m, n_1) - (m, n_2), \text{ and} \\ (mr, n) - (m, rn),\end{gathered} \tag{10.6}$$

for $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$ is an abelian group, denoted by $M \otimes_R N$, or simply $M \otimes N$ if the ring R is clear from the context, and is called the *tensor product of M and N over R*. The elements of $M \otimes_R N$ are called *tensors*, and the coset, $m \otimes n$, of (m, n) in $M \otimes_R N$ is called a simple tensor. We have the relations

$$\begin{gathered}(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \\ m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \text{ and} \\ mr \otimes n = m \otimes rn.\end{gathered} \tag{10.7}$$

Every tensor can be written (non-uniquely in general) as a finite sum of simple tensors.

Remark: We emphasize that care must be taken when working with tensors, since each $m \otimes n$ represents a *coset* in some quotient group, and so we may have $m \otimes n = m' \otimes n'$ where $m \neq m'$ or $n \neq n'$. More generally, an element of $M \otimes N$ may be expressible in many different ways as a sum of simple tensors. In particular, care must be taken when defining maps from $M \otimes_R N$ to another group or module, since a map from $M \otimes N$ which is described on the generators $m \otimes n$ in terms of m and n is not well defined unless it is shown to be independent of the particular choice of $m \otimes n$ as a coset representative.

Another point where care must be exercised is in reference to the element $m \otimes n$ when the modules M and N or the ring R are not clear from the context. The first two examples of extension of scalars give an instance where M is a submodule of a larger module M', and for some $m \in M$ and $n \in N$ we have $m \otimes n = 0$ in $M' \otimes_R N$ but $m \otimes n$ is *nonzero* in $M \otimes_R N$. This is possible because the symbol "$m \otimes n$" represents different cosets, hence possibly different elements, in the two tensor products. In particular, these two examples show that $M \otimes_R N$ need not be a subgroup of $M' \otimes_R N$ even when M is a submodule of M' (cf. also Exercise 2).

Mapping $M \times N$ to the free $\mathbb{Z}$-module on $M \times N$ and then passing to the quotient defines a map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$. This map is in general not a group homomorphism, but it is additive in both m and n separately and satisfies $\iota(mr, n) = mr \otimes n = m \otimes rn = \iota(m, rn)$. Such maps are given a name:

Definition. Let M be a right R-module, let N be a left R-module and let L be an abelian group (written additively). A map $\varphi : M \times N \to L$ is called *R-balanced* or *middle linear with respect to R* if

$$\varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$$
$$\varphi(m, n_1 + n_2) = \varphi(m, n_1) + \varphi(m, n_2)$$
$$\varphi(m, rn) = \varphi(mr, n)$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$.

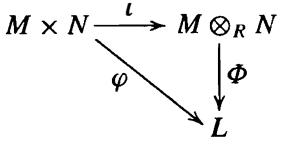
With this terminology, it follows immediately from the relations in (7) that the map $\iota : M \times N \to M \otimes_R N$ is R-balanced. The next theorem proves the extremely useful *universal property of the tensor product* with respect to balanced maps.

Theorem 10. Suppose R is a ring with 1, M is a right R-module, and N is a left R-module. Let $M \otimes_R N$ be the tensor product of M and N over R and let $\iota : M \times N \to M \otimes_R N$ be the R-balanced map defined above.

(1) If $\Phi : M \otimes_R N \to L$ is any group homomorphism from $M \otimes_R N$ to an abelian group L then the composite map $\varphi = \Phi \circ \iota$ is an R-balanced map from $M \times N$ to L.

(2) Conversely, suppose L is an abelian group and $\varphi : M \times N \to L$ is any R-balanced map. Then there is a unique group homomorphism $\Phi : M \otimes_R N \to L$ such that φ factors through ι, i.e., $\varphi = \Phi \circ \iota$ as in (1).

Equivalently, the correspondence $\varphi \leftrightarrow \Phi$ in the commutative diagram



establishes a bijection

$$\left\{ \begin{array}{c} R\text{-balanced maps} \\ \varphi : M \times N \to L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{group homomorphisms} \\ \Phi : M \otimes_R N \to L \end{array} \right\}.$$

Proof: The proof of (1) is immediate from the properties of ι above. For (2), the map φ defines a unique $\mathbb{Z}$-module homomorphism $\tilde{\varphi}$ from the free group on $M \times N$ to L (Theorem 6 in Section 3) such that $\tilde{\varphi}(m, n) = \varphi(m, n) \in L$. Since φ is R-balanced, $\tilde{\varphi}$ maps each of the elements in equation (6) to 0; for example

$$\tilde{\varphi}\left((mr, n) - (m, rn)\right) = \varphi(mr, n) - \varphi(m, rn) = 0.$$

It follows that the kernel of $\tilde{\varphi}$ contains the subgroup generated by these elements, hence $\tilde{\varphi}$ induces a homomorphism Φ on the quotient group $M \otimes_R N$ to L. By definition we then have

$$\Phi(m \otimes n) = \tilde{\varphi}(m, n) = \varphi(m, n),$$

i.e., $\varphi = \Phi \circ \iota$. The homomorphism Φ is uniquely determined by this equation since the elements $m \otimes n$ generate $M \otimes_R N$ as an abelian group. This completes the proof.

Theorem 10 is extremely useful in defining homomorphisms on $M \otimes_R N$ since it replaces the often tedious check that maps defined on simple tensors $m \otimes n$ are well defined with a check that a related map defined on ordered pairs (m, n) is balanced.

The first consequence of the universal property in Theorem 10 is a characterization of the tensor product $M \otimes_R N$ as an abelian group:

Corollary 11. Suppose D is an abelian group and $\iota' : M \times N \to D$ is an R-balanced map such that

(i) the image of ι' generates D as an abelian group, and

(ii) every R-balanced map defined on $M \times N$ factors through ι' as in Theorem 10.

Then there is an isomorphism $f : M \otimes_R N \cong D$ of abelian groups with $\iota' = f \circ \iota$.

Proof: Since $\iota' : M \times N \to D$ is a balanced map, the universal property in (2) of Theorem 10 implies there is a (unique) homomorphism $f : M \otimes_R N \to D$ with $\iota' = f \circ \iota$. In particular $\iota'(m, n) = f(m \otimes n)$ for every $m \in M$, $n \in N$. By the first assumption on ι', these elements generate D as an abelian group, so f is a surjective map. Now, the balanced map $\iota : M \times N \to M \otimes_R N$ together with the second assumption on ι' implies there is a (unique) homomorphism $g : D \to M \otimes_R N$ with $\iota = g \circ \iota'$. Then $m \otimes n = (g \circ f)(m \otimes n)$. Since the simple tensors $m \otimes n$ generate $M \otimes_R N$, it follows that $g \circ f$ is the identity map on $M \otimes_R N$ and so f is injective, hence an isomorphism. This establishes the corollary.

We now return to the question of giving the abelian group $M \otimes_R N$ a *module* structure. As we observed in the special case of extending scalars from R to S for the R-module N, the S-module structure on $S \otimes_R N$ required only a left S-module structure on S together with the compatibility relation $s'(sr) = (s's)r$ for $s, s' \in S$ and $r \in R$. In this special case this relation was simply a consequence of the associative law in the ring S. To obtain an S-module structure on $M \otimes_R N$ more generally we impose a similar structure on M:

Definition. Let R and S be any rings with 1. An abelian group M is called an (S, R)-*bimodule* if M is a left S-module, a right R-module, and $s(mr) = (sm)r$ for all $s \in S$, $r \in R$ and $m \in M$.

Examples

(1) Any ring S is an (S, R)-bimodule for any subring R with $1_R = 1_S$ by the associativity of the multiplication in S. More generally, if $f : R \to S$ is any ring homomorphism with $f(1_R) = 1_S$ then S can be considered as a right R-module with the action $s \cdot r = sf(r)$, and with respect to this action S becomes an (S, R)-bimodule.

(2) Let I be an ideal (two-sided) in the ring R. Then the quotient ring R/I is an $(R/I, R)$-bimodule. This is easy to see directly and is also a special case of the previous example (with respect to the canonical projection homomorphism $R \to R/I$).

(3) Suppose that R is a commutative ring. Then a left (respectively, right) R-module M can always be given the structure of a right (respectively, left) R-module by defining $mr = rm$ (respectively, $rm = mr$), for all $m \in M$ and $r \in R$, and this makes M into

an (R, R)-bimodule. Hence every module (right or left) over a commutative ring R has at least one natural (R, R)-bimodule structure.

(4) Suppose that M is a left S-module and R is a subring contained in the *center* of S (for example, if S is commutative). Then in particular R is commutative so M can be given a right R-module structure as in the previous example. Then for any $s \in S$, $r \in R$ and $m \in M$ by definition of the right action of R we have

$$(sm)r = r(sm) = (rs)m = (sr)m = s(rm) = s(mr)$$

(note that we have used the fact that r commutes with s in the middle equality). Hence M is an (S, R)-bimodule with respect to this definition of the right action of R.

Since the situation in Example 3 occurs so frequently, we give this bimodule structure a name:

Definition. Suppose M is a left (or right) R-module over the commutative ring R. Then the (R, R)-bimodule structure on M defined by letting the left and right R-actions coincide, i.e., $mr = rm$ for all $m \in M$ and $r \in R$, will be called the *standard* R-module structure on M.

Suppose now that N is a left R-module and M is an (S, R)-bimodule. Then just as in the example of extension of scalars the (S, R)-bimodule structure on M implies that

$$s\left(\sum_{\text{finite}} m_i \otimes n_i\right) = \sum_{\text{finite}} (sm_i) \otimes n_i \tag{10.8}$$

gives a well defined action of S under which $M \otimes_R N$ *is a left* S*-module.* Note that Theorem 10 may be used to give an alternate proof that (8) is well defined, replacing the direct calculations on the relations defining the tensor product with the easier check that a map is R-balanced, as follows. It is very easy to see that for each fixed $s \in S$ the map $(m, n) \mapsto sm \otimes n$ is an R-balanced map from $M \times N$ to $M \otimes_R N$. By Theorem 10 there is a well defined group homomorphism λ_s from $M \otimes_R N$ to itself such that $\lambda_s(m \otimes n) = sm \otimes n$. Since the right side of (8) is then $\lambda_s(\sum m_i \otimes n_i)$, the fact that λ_s is well defined shows that this expression is indeed independent of the representation of the tensor $\sum m_i \otimes n_i$ as a sum of simple tensors. Because λ_s is additive, equation (8) holds.

By a completely parallel argument, if M is a right R-module and N is an (R, S)-bimodule then the tensor product $M \otimes_R N$ has the structure of a *right* S-module, where $(\sum m_i \otimes n_i)\, s = \sum m_i \otimes (n_i s)$.

Before giving some more examples of tensor products it is worthwhile to highlight one frequently encountered special case of the previous discussion, namely the case when M and N are two left modules over a *commutative* ring R and $S = R$ (in some works on tensor products this is the only case considered). Then the standard R-module structure on M defined previously gives M the structure of an (R, R)-bimodule, so in this case the tensor product $M \otimes_R N$ always has the structure of a left R-module.

The corresponding map $\iota : M \times N \to M \otimes_R N$ maps $M \times N$ into an R-module and is additive in each factor. Since $r(m \otimes n) = rm \otimes n = mr \otimes n = m \otimes rn$ it also satisfies

$$r\iota(m, n) = \iota(rm, n) = \iota(m, rn).$$

Such maps are given a name:

Definition. Let R be a commutative ring with 1 and let M, N, and L be left R-modules. The map $\varphi : M \times N \to L$ is called *R-bilinear* if it is R-linear in each factor, i.e., if

$$\varphi(r_1m_1 + r_2m_2, n) = r_1\varphi(m_1, n) + r_2\varphi(m_2, n), \quad \text{and}$$
$$\varphi(m, r_1n_1 + r_2n_2) = r_1\varphi(m, n_1) + r_2\varphi(m, n_2)$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r_1, r_2 \in R$.

With this terminology Theorem 10 gives

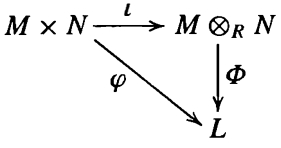
Corollary 12. Suppose R is a commutative ring. Let M and N be two left R-modules and let $M \otimes_R N$ be the tensor product of M and N over R, where M is given the standard R-module structure. Then $M \otimes_R N$ is a left R-module with

$$r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn),$$

and the map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$ is an R-bilinear map. If L is any left R-module then there is a bijection

$$\left\{ \begin{array}{c} R\text{-bilinear maps} \\ \varphi : M \times N \to L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} R\text{-module homomorphisms} \\ \Phi : M \otimes_R N \to L \end{array} \right\}$$

where the correspondence between φ and Φ is given by the commutative diagram



Proof: We have shown $M \otimes_R N$ is an R-module and that ι is bilinear. It remains only to check that in the bijective correspondence in Theorem 10 the bilinear maps correspond with the R-module homomorphisms. If $\varphi : M \times N \to L$ is bilinear then it is an R-balanced map, so the corresponding $\Phi : M \otimes_R N$ is a group homomorphism. Moreover, on simple tensors $\Phi((rm) \otimes n) = \varphi(rm, n) = r\varphi(m, n) = r\Phi(m \otimes n)$, where the middle equality holds because φ is R-linear in the first variable. Since Φ is additive this extends to sums of simple tensors to show Φ is an R-module homomorphism. Conversely, if Φ is an R-module homomorphism it is an exercise to see that the corresponding balanced map φ is bilinear.

Examples

(1) In any tensor product $M \otimes_R N$ we have $m \otimes 0 = m \otimes (0 + 0) = (m \otimes 0) + (m \otimes 0)$, so $m \otimes 0 = 0$. Likewise $0 \otimes n = 0$.

(2) We have $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$, since $3a = a$ for $a \in \mathbb{Z}/2\mathbb{Z}$ so that

$$a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$$

and every simple tensor is reduced to 0. In particular $1 \otimes 1 = 0$. It follows that there are no nonzero balanced (or bilinear) maps from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ to any abelian group.

On the other hand, consider the tensor product $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, which is generated as an abelian group by the elements $0 \otimes 0 = 1 \otimes 0 = 0 \otimes 1 = 0$ and $1 \otimes 1$. In this case $1 \otimes 1 \neq 0$ since, for example, the map $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $(a, b) \mapsto ab$ is clearly nonzero and linear in both a and b. Since $2(1 \otimes 1) = 2 \otimes 1 = 0 \otimes 1 = 0$, the element $1 \otimes 1$ is of order 2. Hence $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.

(3) In general,

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z},$$

where d is the g.c.d. of the integers m and n. To see this, observe first that

$$a \otimes b = a \otimes (b \cdot 1) = (ab) \otimes 1 = ab(1 \otimes 1),$$

from which it follows that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is a cyclic group with $1 \otimes 1$ as generator. Since $m(1 \otimes 1) = m \otimes 1 = 0 \otimes 1 = 0$ and similarly $n(1 \otimes 1) = 1 \otimes n = 0$, we have $d(1 \otimes 1) = 0$, so the cyclic group has order dividing d. The map $\varphi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ defined by $\varphi(a \bmod m, b \bmod n) = ab \bmod d$ is well defined since d divides both m and n. It is clearly $\mathbb{Z}$-bilinear. The induced map $\Phi : \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ from Corollary 12 maps $1 \otimes 1$ to the element $1 \in \mathbb{Z}/d\mathbb{Z}$, which is an element of order d. In particular $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ has order at least d. Hence $1 \otimes 1$ is an element of order d and Φ gives an isomorphism $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$.

(4) In $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ a simple tensor has the form $(a/b \bmod \mathbb{Z}) \otimes (c/d \bmod \mathbb{Z})$ for some rational numbers a/b and c/d. Then

$$\begin{aligned}(\tfrac{a}{b} \bmod \mathbb{Z}) \otimes (\tfrac{c}{d} \bmod \mathbb{Z}) &= d(\tfrac{a}{bd} \bmod \mathbb{Z}) \otimes (\tfrac{c}{d} \bmod \mathbb{Z}) \\ &= (\tfrac{a}{bd} \bmod \mathbb{Z}) \otimes d(\tfrac{c}{d} \bmod \mathbb{Z}) = (\tfrac{a}{bd} \bmod \mathbb{Z}) \otimes 0 = 0\end{aligned}$$

and so

$$\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0.$$

In a similar way, $A \otimes_{\mathbb{Z}} B = 0$ for any *divisible* abelian group A and *torsion* abelian group B (an abelian group in which every element has finite order). For example

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0.$$

(5) The structure of a tensor product can vary considerably depending on the ring over which the tensors are taken. For example $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as left $\mathbb{Q}$-modules (both are one dimensional vector spaces over $\mathbb{Q}$) — cf. the exercises. On the other hand we shall see at the end of this section that $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ are not isomorphic $\mathbb{C}$-modules (the former is a 1-dimensional vector space over $\mathbb{C}$ and the latter is 2-dimensional over $\mathbb{C}$).

(6) *General extension of scalars or change of base:* Let $f : R \to S$ be a ring homomorphism with $f(1_R) = 1_S$. Then $s \cdot r = sf(r)$ gives S the structure of a right R-module with respect to which S is an (S, R)-bimodule. Then for any left R-module N, the resulting tensor product $S \otimes_R N$ is a left S-module obtained by *changing the base* from R to S. This gives a slight generalization of the notion of extension of scalars (where R was a subring of S).

(7) Let $f : R \to S$ be a ring homomorphism as in the preceding example. Then we have $S \otimes_R R \cong S$ as left S-modules, as follows. The map $\varphi : S \times R \to S$ defined by $(s, r) \mapsto sr$ (where $sr = sf(r)$ by definition of the right R-action on S), is an R-balanced map, as is easily checked. For example,

$$\varphi(s_1 + s_2, r) = (s_1 + s_2)r = s_1r + s_2r = \varphi(s_1, r) + \varphi(s_2, r)$$

and

$$\varphi(sr, r') = (sr)r' = s(rr') = \varphi(s, rr').$$

By Theorem 10 we have an associated group homomorphism $\Phi : S \otimes_R R \to S$ with $\Phi(s \otimes r) = sr$. Since $\Phi(s'(s \otimes r)) = \Phi(s's \otimes r) = s'sr = s'\Phi(s \otimes r)$, it follows that Φ is also an S-module homomorphism. The map $\Phi' : S \to S \otimes_R R$ with $s \mapsto s \otimes 1$ is an S-module homomorphism that is inverse to Φ because $\Phi \circ \Phi'(s) = \Phi(s \otimes 1) = s$ gives $\Phi\Phi' = 1$, and

$$\Phi' \circ \Phi(s \otimes r) = \Phi'(sr) = sr \otimes 1 = s \otimes r$$

shows that $\Phi'\Phi$ is the identity on simple tensors, hence $\Phi'\Phi = 1$.

(8) Let R be a ring (not necessarily commutative), let I be a two sided ideal in R, and let N be a left R-module. Then as previously mentioned, R/I is an $(R/I, R)$-bimodule, so the tensor product $R/I \otimes_R N$ is a left R/I-module. This is an example of "extension of scalars" with respect to the natural projection homomorphism $R \to R/I$.

Define

$$IN = \left\{ \sum_{\text{finite}} a_i n_i \mid a_i \in I, n_i \in N \right\},$$

which is easily seen to be a left R-submodule of N (cf. Exercise 5, Section 1). Then

$$(R/I) \otimes_R N \cong N/IN,$$

as left R-modules, as follows. The tensor product is generated as an abelian group by the simple tensors $(r \bmod I) \otimes n = r(1 \otimes n)$ for $r \in R$ and $n \in N$ (viewing the R/I-module tensor product as an R-module on which I acts trivially). Hence the elements $1 \otimes n$ generate $(R/I) \otimes_R N$ as an R/I-module. The map $N \to (R/I) \otimes_R N$ defined by $n \mapsto 1 \otimes n$ is a left R-module homomorphism and, by the previous observation, is surjective. Under this map $a_i n_i$ with $a_i \in I$ and $n_i \in N$ maps to $1 \otimes a_i n_i = a_i \otimes n_i = 0$, and so IN is contained in the kernel. This induces a surjective R-module homomorphism $f : N/IN \to (R/I) \otimes_R N$ with $f(n \bmod I) = 1 \otimes n$. We show f is an isomorphism by exhibiting its inverse. The map $(R/I) \times N \to N/IN$ defined by mapping $(r \bmod I, n)$ to $(rn \bmod IN)$ is well defined and easily checked to be R-balanced. It follows by Theorem 10 that there is an associated group homomorphism $g : (R/I) \otimes N \to N/IN$ with $g((r \bmod I) \otimes n) = rn \bmod IN$. As usual, $fg = 1$ and $gf = 1$, so f is a bijection and $(R/I) \otimes_R N \cong N/IN$, as claimed.

As an example, let $R = \mathbb{Z}$ with ideal $I = m\mathbb{Z}$ and let N be the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$. Then $IN = m(\mathbb{Z}/n\mathbb{Z}) = (m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} = d\mathbb{Z}/n\mathbb{Z}$ where d is the g.c.d. of m and n. Then $N/IN \cong \mathbb{Z}/d\mathbb{Z}$ and we recover the isomorphism $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$ of Example 3 above.

We now establish some of the basic properties of tensor products. Note the frequent application of Theorem 10 to establish the existence of homomorphisms.

Theorem 13. *(The "Tensor Product" of Two Homomorphisms)* Let M, M' be right R-modules, let N, N' be left R-modules, and suppose $\varphi : M \to M'$ and $\psi : N \to N'$ are R-module homomorphisms.

(1) There is a unique group homomorphism, denoted by $\varphi \otimes \psi$, mapping $M \otimes_R N$ into $M' \otimes_R N'$ such that $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$ for all $m \in M$ and $n \in N$.

(2) If M, M' are also (S, R)-bimodules for some ring S and φ is also an S-module homomorphism, then $\varphi \otimes \psi$ is a homomorphism of left S-modules. In particular, if R is commutative then $\varphi \otimes \psi$ is always an R-module homomorphism for the standard R-module structures.

(3) If $\lambda : M' \to M''$ and $\mu : N' \to N''$ are R-module homomorphisms then $(\lambda \otimes \mu) \circ (\varphi \otimes \psi) = (\lambda \circ \varphi) \otimes (\mu \circ \psi)$.

Proof: The map $(m, n) \mapsto \varphi(m) \otimes \psi(n)$ from $M \times N$ to $M' \otimes_R N'$ is clearly R-balanced, so (1) follows immediately from Theorem 10.

In (2) the definition of the (left) action of S on M together with the assumption that φ is an S-module homomorphism imply that on simple tensors

$$(\varphi \otimes \psi)(s(m \otimes n)) = (\varphi \otimes \psi)(sm \otimes n) = \varphi(sm) \otimes \psi(n) = s\varphi(m) \otimes \psi(n).$$

Since $\varphi \otimes \psi$ is additive, this extends to sums of simple tensors to show that $\varphi \otimes \psi$ is an S-module homomorphism. This gives (2).

The uniqueness condition in Theorem 10 implies (3), which completes the proof.

The next result shows that we may write $M \otimes N \otimes L$, or more generally, an n-fold tensor product $M_1 \otimes M_2 \otimes \cdots \otimes M_n$, unambiguously whenever it is defined.

Theorem 14. *(Associativity of the Tensor Product)* Suppose M is a right R-module, N is an (R, T)-bimodule, and L is a left T-module. Then there is a unique isomorphism

$$(M \otimes_R N) \otimes_T L \cong M \otimes_R (N \otimes_T L)$$

of abelian groups such that $(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$. If M is an (S, R)-bimodule, then this is an isomorphism of S-modules.

Proof: Note first that the (R, T)-bimodule structure on N makes $M \otimes_R N$ into a right T-module and $N \otimes_T L$ into a left R-module, so both sides of the isomorphism are well defined. For each fixed $l \in L$, the mapping $(m, n) \mapsto m \otimes (n \otimes l)$ is R-balanced, so by Theorem 10 there is a homomorphism $M \otimes_R N \to M \otimes_R (N \otimes_T L)$ with $m \otimes n \mapsto m \otimes (n \otimes l)$. This shows that the map from $(M \otimes_R N) \times L$ to $M \otimes_R (N \otimes_T L)$ given by $(m \otimes n, l) \mapsto m \otimes (n \otimes l)$ is well defined. Since it is easily seen to be T-balanced, another application of Theorem 10 implies that it induces a homomorphism $(M \otimes_R N) \otimes_T L \to M \otimes_R (N \otimes_T L)$ such that $(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$. In a similar way we can construct a homomorphism in the opposite direction that is inverse to this one. This proves the group isomorphism.

Assume in addition M is an (S, R)-bimodule. Then for $s \in S$ and $t \in T$ we have

$$s((m \otimes n)t) = s(m \otimes nt) = sm \otimes nt = (sm \otimes n)t = (s(m \otimes n))t$$

so that $M \otimes_R N$ is an (S, T)-bimodule. Hence $(M \otimes_R N) \otimes_T L$ is a left S-module. Since $N \otimes_T L$ is a left R-module, also $M \otimes_R (N \otimes_T L)$ is a left S-module. The group isomorphism just established is easily seen to be a homomorphism of left S-modules by the same arguments used in previous proofs: it is additive and is S-linear on simple tensors since $s((m \otimes n) \otimes l) = s(m \otimes n) \otimes l = (sm \otimes n) \otimes l$ maps to the element $sm \otimes (n \otimes l) = s(m \otimes (n \otimes l))$. The proof is complete.

Corollary 15. Suppose R is commutative and M, N, and L are left R-modules. Then

$$(M \otimes N) \otimes L \cong M \otimes (N \otimes L)$$

as R-modules for the standard R-module structures on M, N and L.

There is a natural extension of the notion of a bilinear map:

Definition. Let R be a commutative ring with 1 and let $M_1, M_2, \ldots, M_n$ and L be R-modules with the standard R-module structures. A map $\varphi : M_1 \times \cdots \times M_n \to L$ is called *n-multilinear over R* (or simply *multilinear* if n and R are clear from the context) if it is an R-module homomorphism in each component when the other component entries are kept constant, i.e., for each i

$$\varphi(m_1, \ldots, m_{i-1}, rm_i + r'm_i', m_{i+1}, \ldots, m_n)$$
$$= r\varphi(m_1, \ldots, m_i, \ldots, m_n) + r'\varphi(m_1, \ldots, m_i', \ldots, m_n)$$

for all $m_i, m_i' \in M_i$ and $r, r' \in R$. When $n = 2$ (respectively, 3) one says φ is *bilinear* (respectively *trilinear*) rather than 2-multilinear (or 3-multilinear).

One may construct the n-fold tensor product $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ from first principles and prove its analogous universal property with respect to multilinear maps from $M_1 \times \cdots \times M_n$ to L. By the previous theorem and corollary, however, an n-fold tensor product may be obtained unambiguously by iterating the tensor product of pairs of modules since any bracketing of $M_1 \otimes \cdots \otimes M_n$ into tensor products of pairs gives an isomorphic R-module. The universal property of the tensor product of a pair of modules in Theorem 10 and Corollary 12 then implies that multilinear maps factor uniquely through the R-module $M_1 \otimes \cdots \otimes M_n$, i.e., this tensor product is the universal object with respect to multilinear functions:

Corollary 16. Let R be a commutative ring and let $M_1, \ldots, M_n, L$ be R-modules. Let $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ denote any bracketing of the tensor product of these modules and let

$$\iota : M_1 \times \cdots \times M_n \to M_1 \otimes \cdots \otimes M_n$$

be the map defined by $\iota(m_1, \ldots, m_n) = m_1 \otimes \cdots \otimes m_n$. Then

(1) for every R-module homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$ the map $\varphi = \Phi \circ \iota$ is n-multilinear from $M_1 \times \cdots \times M_n$ to L, and

(2) if $\varphi : M_1 \times \cdots \times M_n \to L$ is an n-multilinear map then there is a unique R-module homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$ such that $\varphi = \Phi \circ \iota$.

Hence there is a bijection

$$\left\{ \begin{array}{c} n\text{-multilinear maps} \\ \varphi : M_1 \times \cdots \times M_n \to L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} R\text{-module homomorphisms} \\ \Phi : M_1 \otimes \cdots \otimes M_n \to L \end{array} \right\}$$

with respect to which the following diagram commutes:

$$\begin{array}{ccc} M \times \cdots \times M_n & \xrightarrow{\iota} & M \otimes \cdots \otimes M_n \\ & \searrow^{\varphi} & \downarrow \Phi \\ & & L \end{array}$$

We have already seen examples where $M_1 \otimes_R N$ is not contained in $M \otimes_R N$ even when M_1 is an R-submodule of M. The next result shows in particular that (an isomorphic copy of) $M_1 \otimes_R N$ *is* contained in $M \otimes_R N$ if M_1 is an R-module *direct summand* of M.

Theorem 17. *(Tensor Products of Direct Sums)* Let M, M' be right R-modules and let N, N' be left R-modules. Then there are unique group isomorphisms

$$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$$
$$M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N')$$

such that $(m, m') \otimes n \mapsto (m \otimes n, m' \otimes n)$ and $m \otimes (n, n') \mapsto (m \otimes n, m \otimes n')$ respectively. If M, M' are also (S, R)-bimodules, then these are isomorphisms of left S-modules. In particular, if R is commutative, these are isomorphisms of R-modules.

Proof: The map $(M \oplus M') \times N \to (M \otimes_R N) \oplus (M' \otimes_R N)$ defined by $((m, m'), n) \mapsto (m \otimes n, m' \otimes n)$ is well defined since m and m' in $M \oplus M'$ are uniquely defined in the direct sum. The map is clearly R-balanced, so induces a homomorphism f from $(M \oplus M') \otimes N$ to $(M \otimes_R N) \oplus (M' \otimes_R N)$ with

$$f((m, m') \otimes n) = (m \otimes n, m' \otimes n).$$

In the other direction, the R-balanced maps $M \times N \to (M \oplus M') \otimes_R N$ and $M' \times N \to (M \oplus M') \otimes_R N$ given by $(m, n) \mapsto (m, 0) \otimes n$ and $(m', n) \mapsto (0, m') \otimes n$, respectively, define homomorphisms from $M \otimes_R N$ and $M' \otimes_R N$ to $(M \oplus M') \otimes_R N$. These in turn give a homomorphism g from the direct sum $(M \otimes_R N) \oplus (M' \otimes_R N)$ to $(M \oplus M') \otimes_R N$ with

$$g((m \otimes n_1, m' \otimes n_2)) = (m, 0) \otimes n_1 + (0, m') \otimes n_2.$$

An easy check shows that f and g are inverse homomorphisms and are S-module isomorphisms when M and M' are (S, R)-bimodules. This completes the proof.

The previous theorem clearly extends by induction to any finite direct sum of R-modules. The corresponding result is also true for arbitrary direct sums. For example

$$M \otimes (\oplus_{i \in I} N_i) \cong \oplus_{i \in I} (M \otimes N_i),$$

where I is any index set (cf. the exercises). This result is referred to by saying that *tensor products commute with direct sums.*

Corollary 18. *(Extension of Scalars for Free Modules)* The module obtained from the free R-module $N \cong R^n$ by extension of scalars from R to S is the free S-module S^n, i.e.,

$$S \otimes_R R^n \cong S^n$$

as left S-modules.

Proof: This follows immediately from Theorem 17 and the isomorphism $S \otimes_R R \cong S$ proved in Example 7 previously.

Corollary 19. Let R be a commutative ring and let $M \cong R^s$ and $N \cong R^t$ be free R-modules with bases $m_1, \ldots, m_s$ and $n_1, \ldots, n_t$, respectively. Then $M \otimes_R N$ is a free R-module of rank st, with basis $m_i \otimes n_j$, $1 \leq i \leq s$ and $1 \leq j \leq t$, i.e.,

$$R^s \otimes_R R^t \cong R^{st}.$$

Remark: More generally, the tensor product of two free modules of arbitrary rank over a commutative ring is free (cf. the exercises).

Proof: This follows easily from Theorem 17 and the first example following Corollary 9.

Proposition 20. Suppose R is a commutative ring and M, N are left R-modules, considered with the standard R-module structures. Then there is a unique R-module isomorphism

$$M \otimes_R N \cong N \otimes_R M$$

mapping $m \otimes n$ to $n \otimes m$.

Proof: The map $M \times N \to N \otimes M$ defined by $(m, n) \mapsto n \otimes m$ is R-balanced. Hence it induces a unique homomorphism f from $M \otimes N$ to $N \otimes M$ with $f(m \otimes n) = n \otimes m$. Similarly, we have a unique homomorphism g from $N \otimes M$ to $M \otimes N$ with $g(n \otimes m) = m \otimes n$ giving the inverse of f, and both maps are easily seen to be R-module isomorphisms.

Remark: When $M = N$ it is not in general true that $a \otimes b = b \otimes a$ for $a, b \in M$. We shall study "symmetric tensors" in Section 11.6.

We end this section by showing that the tensor product of R-algebras is again an R-algebra.

Proposition 21. Let R be a commutative ring and let A and B be R-algebras. Then the multiplication $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ is well defined and makes $A \otimes_R B$ into an R-algebra.

Proof: Note first that the definition of an R-algebra shows that

$$r(a \otimes b) = ra \otimes b = ar \otimes b = a \otimes rb = a \otimes br = (a \otimes b)r$$

for every $r \in R$, $a \in A$ and $b \in B$. To show that $A \otimes B$ is an R-algebra the main task is, as usual, showing that the specified multiplication is well defined. One way to proceed is to use two applications of Corollary 16, as follows. The map $\varphi : A \times B \times A \times B \to A \otimes B$ defined by $f(a, b, a', b') = aa' \otimes bb'$ is multilinear over R. For example,

$$\begin{aligned} f(a, r_1 b_1 + r_2 b_2, a', b') &= aa' \otimes (r_1 b_1 + r_2 b_2) b' \\ &= aa' \otimes r_1 b_1 b' + aa' \otimes r_2 b_2 b' \\ &= r_1 f(a, b_1, a', b') + r_2 f(a, b_2, a', b'). \end{aligned}$$

By Corollary 16, there is a corresponding R-module homomorphism Φ from $A \otimes B \otimes A \otimes B$ to $A \otimes B$ with $\Phi(a \otimes b \otimes a' \otimes b') = aa' \otimes bb'$. Viewing $A \otimes B \otimes A \otimes B$ as $(A \otimes B) \otimes (A \otimes B)$, we can apply Corollary 16 once more to obtain a well defined R-bilinear mapping φ' from $(A \otimes B) \times (A \otimes B)$ to $A \otimes B$ with $\varphi'(a \otimes b, a' \otimes b') = aa' \otimes bb'$. This shows that the multiplication is indeed well defined (and also that it satisfies the distributive laws). It is now a simple matter (left to the exercises) to check that with this multiplication $A \otimes B$ is an R-algebra.

Example

The tensor product $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is free of rank 4 as a module over $\mathbb{R}$ with basis given by $e_1 = 1 \otimes 1$, $e_2 = 1 \otimes i$, $e_3 = i \otimes 1$, and $e_4 = i \otimes i$ (by Corollary 19). By Proposition 21, this tensor product is also a (commutative) ring with $e_1 = 1$, and, for example,

$$e_4^2 = (i \otimes i)(i \otimes i) = i^2 \otimes i^2 = (-1) \otimes (-1) = (-1)(-1) \otimes 1 = 1.$$

Then $(e_4 - 1)(e_4 + 1) = 0$, so $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not an integral domain.

The ring $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is an $\mathbb{R}$-algebra and the left and right $\mathbb{R}$-actions are the same: $xr = rx$ for every $r \in \mathbb{R}$ and $x \in \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. The ring $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ has a structure of a left $\mathbb{C}$-module because the first $\mathbb{C}$ is a $(\mathbb{C}, \mathbb{R})$-bimodule. It also has a right $\mathbb{C}$-module structure because the second $\mathbb{C}$ is an $(\mathbb{R}, \mathbb{C})$-bimodule. For example,

$$i \cdot e_1 = i \cdot (1 \otimes 1) = (i \cdot 1) \otimes 1 = i \otimes 1 = e_3$$

and

$$e_1 \cdot i = (1 \otimes 1) \cdot i = 1 \otimes (1 \cdot i) = 1 \otimes i = e_2.$$

This example also shows that even when the rings involved are commutative there may be natural left and right module structures (over some ring) that are not the same.

EXERCISES

Let R be a ring with 1.

1. Let $f : R \to S$ be a ring homomorphism from the ring R to the ring S with $f(1_R) = 1_S$. Verify the details that $sr = sf(r)$ defines a right R-action on S under which S is an (S, R)-bimodule.
2. Show that the element "$2 \otimes 1$" is 0 in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ but is nonzero in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.
3. Show that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ are both left $\mathbb{R}$-modules but are not isomorphic as $\mathbb{R}$-modules.
4. Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ are isomorphic left $\mathbb{Q}$-modules. [Show they are both 1-dimensional vector spaces over $\mathbb{Q}$.]
5. Let A be a finite abelian group of order n and let p^k be the largest power of the prime p dividing n. Prove that $\mathbb{Z}/p^k\mathbb{Z} \otimes_{\mathbb{Z}} A$ is isomorphic to the Sylow p-subgroup of A.
6. If R is any integral domain with quotient field Q, prove that $(Q/R) \otimes_R (Q/R) = 0$.
7. If R is any integral domain with quotient field Q and N is a left R-module, prove that every element of the tensor product $Q \otimes_R N$ can be written as a simple tensor of the form $(1/d) \otimes n$ for some nonzero $d \in R$ and some $n \in N$.
8. Suppose R is an integral domain with quotient field Q and let N be any R-module. Let $U = R^\times$ be the set of nonzero elements in R and define $U^{-1}N$ to be the set of equivalence classes of ordered pairs of elements (u, n) with $u \in U$ and $n \in N$ under the equivalence relation $(u, n) \sim (u', n)$ if and only if $u'n = un'$ in N.

(a) Prove that $U^{-1}N$ is an abelian group under the addition defined by $\overline{(u_1, n_1)} + \overline{(u_2, n_2)} = \overline{(u_1u_2, u_2n_1 + u_1n_2)}$. Prove that $r\overline{(u, n)} = \overline{(u, rn)}$ defines an action of R on $U^{-1}N$ making it into an R-module. [This is an example of *localization* considered in general in Section 4 of Chapter 15, cf. also Section 5 in Chapter 7.]

(b) Show that the map from $Q \times N$ to $U^{-1}N$ defined by sending $(a/b, n)$ to $\overline{(b, an)}$ for $a \in R$, $b \in U$, $n \in N$, is an R-balanced map, so induces a homomorphism f from $Q \otimes_R N$ to $U^{-1}N$. Show that the map g from $U^{-1}N$ to $Q \otimes_R N$ defined by $g(\overline{(u, n)}) = (1/u) \otimes n$ is well defined and is an inverse homomorphism to f. Conclude that $Q \otimes_R N \cong U^{-1}N$ as R-modules.

(c) Conclude from (b) that $(1/d) \otimes n$ is 0 in $Q \otimes_R N$ if and only if $rn = 0$ for some nonzero $r \in R$.

(d) If A is an abelian group, show that $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$ if and only if A is a torsion abelian group (i.e., every element of A has finite order).

9. Suppose R is an integral domain with quotient field Q and let N be any R-module. Let $Q \otimes_R N$ be the module obtained from N by extension of scalars from R to Q. Prove that the kernel of the R-module homomorphism $\iota : N \to Q \otimes_R N$ is the torsion submodule of N (cf. Exercise 8 in Section 1). [Use the previous exercise.]

10. Suppose R is commutative and $N \cong R^n$ is a free R-module of rank n with R-module basis $e_1, \ldots, e_n$.

(a) For any nonzero R-module M show that every element of $M \otimes N$ can be written uniquely in the form $\sum_{i=1}^{n} m_i \otimes e_i$ where $m_i \in M$. Deduce that if $\sum_{i=1}^{n} m_i \otimes e_i = 0$ in $M \otimes N$ then $m_i = 0$ for $i = 1, \ldots, n$.

(b) Show that if $\sum m_i \otimes n_i = 0$ in $M \otimes N$ where the n_i are merely assumed to be R-linearly independent then it is not necessarily true that all the m_i are 0. [Consider $R = \mathbb{Z}$, $n = 1$, $M = \mathbb{Z}/2\mathbb{Z}$, and the element $1 \otimes 2$.]

11. Let $\{e_1, e_2\}$ be a basis of $V = \mathbb{R}^2$. Show that the element $e_1 \otimes e_2 + e_2 \otimes e_1$ in $V \otimes_{\mathbb{R}} V$ cannot be written as a simple tensor $v \otimes w$ for any $v, w \in \mathbb{R}^2$.

12. Let V be a vector space over the field F and let v, v' be nonzero elements of V. Prove that $v \otimes v' = v' \otimes v$ in $V \otimes_F V$ if and only if $v = av'$ for some $a \in F$.

13. Prove that the usual dot product of vectors defined by letting $(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n)$ be $a_1b_1 + \cdots + a_nb_n$ is a bilinear map from $\mathbb{R}^n \times \mathbb{R}^n$ to $\mathbb{R}$.

14. Let I be an arbitrary nonempty index set and for each $i \in I$ let N_i be a left R-module. Let M be a right R-module. Prove the group isomorphism: $M \otimes (\oplus_{i \in I} N_i) \cong \oplus_{i \in I} (M \otimes N_i)$, where the direct sum of an arbitrary collection of modules is defined in Exercise 20, Section 3. [Use the same argument as for the direct sum of two modules, taking care to note where the direct *sum* hypothesis is needed — cf. the next exercise.]

15. Show that tensor products do not commute with direct products in general. [Consider the extension of scalars from $\mathbb{Z}$ to $\mathbb{Q}$ of the direct product of the modules $M_i = \mathbb{Z}/2^i\mathbb{Z}$, $i = 1, 2, \ldots$]

16. Suppose R is commutative and let I and J be ideals of R, so R/I and R/J are naturally R-modules.

(a) Prove that every element of $R/I \otimes_R R/J$ can be written as a simple tensor of the form $(1 \bmod I) \otimes (r \bmod J)$.

(b) Prove that there is an R-module isomorphism $R/I \otimes_R R/J \cong R/(I + J)$ mapping $(r \bmod I) \otimes (r' \bmod J)$ to $rr' \bmod (I + J)$.

17. Let $I = (2, x)$ be the ideal generated by 2 and x in the ring $R = \mathbb{Z}[x]$. The ring $\mathbb{Z}/2\mathbb{Z} = R/I$ is naturally an R-module annihilated by both 2 and x.

(a) Show that the map $\varphi : I \times I \to \mathbb{Z}/2\mathbb{Z}$ defined by

$$\varphi(a_0 + a_1x + \cdots + a_nx^n, b_0 + b_1x + \cdots + b_mx^m) = \frac{a_0}{2}b_1 \bmod 2$$

is R-bilinear.

(b) Show that there is an R-module homomorphism from $I \otimes_R I \to \mathbb{Z}/2\mathbb{Z}$ mapping $p(x) \otimes q(x)$ to $\frac{p(0)}{2}q'(0)$ where q' denotes the usual polynomial derivative of q.

(c) Show that $2 \otimes x \neq x \otimes 2$ in $I \otimes_R I$.

18. Suppose I is a principal ideal in the integral domain R. Prove that the R-module $I \otimes_R I$ has no nonzero torsion elements (i.e., $rm = 0$ with $0 \neq r \in R$ and $m \in I \otimes_R I$ implies that $m = 0$).

19. Let $I = (2, x)$ be the ideal generated by 2 and x in the ring $R = \mathbb{Z}[x]$ as in Exercise 17. Show that the nonzero element $2 \otimes x - x \otimes 2$ in $I \otimes_R I$ is a torsion element. Show in fact that $2 \otimes x - x \otimes 2$ is annihilated by both 2 and x and that the submodule of $I \otimes_R I$ generated by $2 \otimes x - x \otimes 2$ is isomorphic to R/I.

20. Let $I = (2, x)$ be the ideal generated by 2 and x in the ring $R = \mathbb{Z}[x]$. Show that the element $2 \otimes 2 + x \otimes x$ in $I \otimes_R I$ is not a simple tensor, i.e., cannot be written as $a \otimes b$ for some $a, b \in I$.

21. Suppose R is commutative and let I and J be ideals of R.

(a) Show there is a surjective R-module homomorphism from $I \otimes_R J$ to the product ideal IJ mapping $i \otimes j$ to the element ij.

(b) Give an example to show that the map in (a) need not be injective (cf. Exercise 17).

22. Suppose that M is a left and a right R-module such that $rm = mr$ for all $r \in R$ and $m \in M$. Show that the elements r_1r_2 and r_2r_1 act the same on M for every $r_1, r_2 \in R$. (This explains why the assumption that R is commutative in the definition of an R-algebra is a fairly natural one.)

23. Verify the details that the multiplication in Proposition 19 makes $A \otimes_R B$ into an R-algebra.

24. Prove that the extension of scalars from $\mathbb{Z}$ to the Gaussian integers $\mathbb{Z}[i]$ of the ring $\mathbb{R}$ is isomorphic to $\mathbb{C}$ as a ring: $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{C}$ as rings.

25. Let R be a subring of the commutative ring S and let x be an indeterminate over S. Prove that $S[x]$ and $S \otimes_R R[x]$ are isomorphic as S-algebras.

26. Let S be a commutative ring containing R (with $1_S = 1_R$) and let $x_1, \ldots, x_n$ be independent indeterminates over the ring S. Show that for every ideal I in the polynomial ring $R[x_1, \ldots, x_n]$ that $S \otimes_R (R[x_1, \ldots, x_n]/I) \cong S[x_1, \ldots, x_n]/IS[x_1, \ldots, x_n]$ as S-algebras.

The next exercise shows the ring $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ introduced at the end of this section is isomorphic to $\mathbb{C} \times \mathbb{C}$. One may also prove this via Exercise 26 and Proposition 16 in Section 9.5, since $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$. The ring $\mathbb{C} \times \mathbb{C}$ is also discussed in Exercise 23 of Section 1.

27. **(a)** Write down a formula for the multiplication of two elements $a \cdot 1 + b \cdot e_2 + c \cdot e_3 + d \cdot e_4$ and $a' \cdot 1 + b' \cdot e_2 + c' \cdot e_3 + d' \cdot e_4$ in the example $A = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ following Proposition 21 (where $1 = 1 \otimes 1$ is the identity of A).

(b) Let $\epsilon_1 = \frac{1}{2}(1 \otimes 1 + i \otimes i)$ and $\epsilon_2 = \frac{1}{2}(1 \otimes 1 - i \otimes i)$. Show that $\epsilon_1\epsilon_2 = 0, \epsilon_1 + \epsilon_2 = 1$, and $\epsilon_j^2 = \epsilon_j$ for $j = 1, 2$ (ϵ_1 and ϵ_2 are called *orthogonal idempotents* in A). Deduce that A is isomorphic as a ring to the direct product of two principal ideals: $A \cong A\epsilon_1 \times A\epsilon_2$ (cf. Exercise 1, Section 7.6).

(c) Prove that the map $\varphi : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ by $\varphi(z_1, z_2) = (z_1z_2, z_1\overline{z_2})$, where $\overline{z_2}$ denotes the complex conjugate of z_2, is an $\mathbb{R}$-bilinear map.

(d) Let Φ be the $\mathbb{R}$-module homomorphism from A to $\mathbb{C} \times \mathbb{C}$ obtained from φ in (c). Show that $\Phi(\epsilon_1) = (0, 1)$ and $\Phi(\epsilon_2) = (1, 0)$. Show also that Φ is $\mathbb{C}$-linear, where the action of $\mathbb{C}$ is on the left tensor factor in A and on both factors in $\mathbb{C} \times \mathbb{C}$. Deduce that Φ is surjective. Show that Φ is a $\mathbb{C}$-algebra isomorphism.

10.5 EXACT SEQUENCES—PROJECTIVE, INJECTIVE, AND FLAT MODULES

One of the fundamental results for studying the structure of an algebraic object B (e.g., a group, a ring, or a module) is the First Isomorphism Theorem, which relates the subobjects of B (the normal subgroups, the ideals, or the submodules, respectively) with the possible homomorphic images of B. We have already seen many examples applying this theorem to understand the structure of B from an understanding of its "smaller" constituents—for example in analyzing the structure of the dihedral group D_8 by determining its center and the resulting quotient by the center.

In most of these examples we began *first* with a given B and then determined some of its basic properties by constructing a homomorphism φ (often given implicitly by the specification of $\ker \varphi \subseteq B$) and examining both $\ker \varphi$ and the resulting quotient $B/\ker \varphi$. We now consider in some greater detail the reverse situation, namely whether we may *first* specify the "smaller constituents." More precisely, we consider whether, given two modules A and C, there exists a module B containing (an isomorphic copy of) A such that the resulting quotient module B/A is isomorphic to C—in which case B is said to be an *extension of C by A*. It is then natural to ask how many such B exist for a given A and C, and the extent to which properties of B are determined by the corresponding properties of A and C. There are, of course, analogous problems in the contexts of groups and rings. This is the *extension problem* first discussed (for groups) in Section 3.4; in this section we shall be primarily concerned with left modules over a ring R, making note where necessary of the modifications required for some other structures, notably noncommutative groups. As in the previous section, throughout this section all rings contain a 1.

We first introduce a very convenient notation. To say that A is isomorphic to a submodule of B, is to say that there is an injective homomorphism $\psi : A \to B$ (so then $A \cong \psi(A) \subseteq B$). To say that C is isomorphic to the resulting quotient is to say that there is a surjective homomorphism $\varphi : B \to C$ with $\ker \varphi = \psi(A)$. In particular this gives us a pair of homomorphisms:

$$A \xrightarrow{\psi} B \xrightarrow{\varphi} C$$

with image $\psi = \ker \varphi$. A pair of homomorphisms with this property is given a name:

Definition.

(1) The pair of homomorphisms $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is said to be *exact* (at Y) if image $\alpha = \ker \beta$.

(2) A sequence $\cdots \to X_{n-1} \to X_n \to X_{n+1} \to \cdots$ of homomorphisms is said to be an *exact sequence* if it is exact at every X_n between a pair of homomorphisms.

With this terminology, the pair of homomorphisms $A \xrightarrow{\psi} B \xrightarrow{\varphi} C$ above is exact at B. We can also use this terminology to express the fact that for these maps ψ is injective and φ is surjective:

Proposition 22. Let A, B and C be R-modules over some ring R. Then

(1) The sequence $0 \to A \xrightarrow{\psi} B$ is exact (at A) if and only if ψ is injective.

(2) The sequence $B \xrightarrow{\varphi} C \to 0$ is exact (at C) if and only if φ is surjective.

Proof: The (uniquely defined) homomorphism $0 \to A$ has image 0 in A. This will be the kernel of ψ if and only if ψ is injective. Similarly, the kernel of the (uniquely defined) zero homomorphism $C \to 0$ is all of C, which is the image of φ if and only if φ is surjective.

Corollary 23. The sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is exact if and only if ψ is injective, φ is surjective, and image $\psi = \ker \varphi$, i.e., B is an extension of C by A.

Definition. The exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is called a *short exact sequence*.

In terms of this notation, the extension problem can be stated succinctly as follows: given modules A and C, determine all the short exact sequences

$$0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} C \longrightarrow 0. \tag{10.9}$$

We shall see below that the exact sequence notation is also extremely convenient for analyzing the extent to which properties of A and C determine the corresponding properties of B. If A, B and C are groups written multiplicatively, the sequence (9) will be written

$$1 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} C \longrightarrow 1 \tag{10.9'}$$

where 1 denotes the trivial group. Both Proposition 22 and Corollary 23 are valid with the obvious notational changes.

Note that any exact sequence can be written as a succession of short exact sequences since to say $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is exact at Y is the same as saying that the sequence $0 \to \alpha(X) \to Y \to Y/\ker \beta \to 0$ is a short exact sequence.

Examples

(1) Given modules A and C we can always form their direct sum $B = A \oplus C$ and the sequence

$$0 \to A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \to 0$$

where $\iota(a) = (a, 0)$ and $\pi(a, c) = c$ is a short exact sequence. In particular, it follows that there always exists at least one extension of C by A.

(2) As a special case of the previous example, consider the two $\mathbb{Z}$-modules $A = \mathbb{Z}$ and $C = \mathbb{Z}/n\mathbb{Z}$:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \oplus (\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

giving one extension of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$.

Another extension of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$ is given by the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$$

where n denotes the map $x \mapsto nx$ given by multiplication by n, and π denotes the natural projection. Note that the modules in the middle of the previous two exact sequences are not isomorphic even though the respective "A" and "C" terms are isomorphic. Thus there are (at least) two "essentially different" or "inequivalent" ways of extending $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$.

(3) If $\varphi : B \to C$ is any homomorphism we may form an exact sequence:

$$0 \longrightarrow \ker\varphi \xrightarrow{\iota} B \xrightarrow{\varphi} \text{image}\,\varphi \longrightarrow 0$$

where ι is the inclusion map. In particular, if φ is surjective, the sequence $\varphi : B \to C$ may be extended to a short exact sequence with $A = \ker\varphi$.

(4) One particularly important instance of the preceding example is when M is an R-module and S is a set of generators for M. Let $F(S)$ be the free R-module on S. Then

$$0 \longrightarrow K \xrightarrow{\iota} F(S) \xrightarrow{\varphi} M \longrightarrow 0$$

is the short exact sequence where φ is the unique R-module homomorphism which is the identity on S (cf. Theorem 6) and $K = \ker\varphi$.

More generally, when M is any group (possibly non-abelian) the above short exact sequence (with 1's at the ends, if M is written multiplicatively) describes a *presentation* of M, where K is the normal subgroup of $F(S)$ generated by the *relations* defining M (cf. Section 6.3).

(5) Two "inequivalent" extensions G of the Klein 4-group by the cyclic group Z_2 of order two are

$$1 \longrightarrow Z_2 \xrightarrow{\iota} D_8 \xrightarrow{\varphi} Z_2 \times Z_2 \longrightarrow 1, \text{ and}$$
$$1 \longrightarrow Z_2 \xrightarrow{\iota} Q_8 \xrightarrow{\varphi} Z_2 \times Z_2 \longrightarrow 1,$$

where in each case ι maps Z_2 injectively into the center of G (recall that both D_8 and Q_8 have centers of order two), and φ is the natural projection of G onto $G/Z(G)$.

Two other inequivalent extensions G of the Klein 4-group by Z_2 occur when G is either of the abelian groups $Z_2 \times Z_2 \times Z_2$ or $Z_2 \times Z_4$ for appropriate maps ι and φ.

Examples 2 and 5 above show that, for a fixed A and C, in general there may be several extensions of C by A. To distinguish different extensions we define the notion of a homomorphism (and isomorphism) between two exact sequences. Recall first that a diagram involving various homomorphisms is said to *commute* if any compositions of homomorphisms with the same starting and ending points are equal, i.e., the composite map defined by following a path of homomorphisms in the diagram depends only on the starting and ending points and not on the choice of the path taken.

Definition. Let $0 \to A \to B \to C \to 0$ and $0 \to A' \to B' \to C' \to 0$ be two short exact sequences of modules.

(1) A *homomorphism of short exact sequences* is a triple α, β, γ of module homomorphisms such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

The homomorphism is an *isomorphism of short exact sequences* if α, β, γ are all isomorphisms, in which case the extensions B and B' are said to be *isomorphic extensions.*

(2) The two exact sequences are called *equivalent* if $A = A'$, $C = C'$, and there is an isomorphism between them as in (1) that is the identity maps on A and C (i.e., α and γ are the identity). In this case the corresponding extensions B and B' are said to be *equivalent* extensions.

If B and B' are isomorphic extensions then in particular B and B' are isomorphic as R-modules, but more is true: there is an R-module isomorphism between B and B' that restricts to an isomorphism from A to A' and induces an isomorphism on the quotients C and C'. For a given A and C the condition that two extensions B and B' of C by A are equivalent is stronger still: there must exist an R-module isomorphism between B and B' that restricts to the *identity* map on A and induces the *identity* map on C. The notion of isomorphic extensions measures how many different extensions of C by A there are, allowing for C and A to be changed by an isomorphism. The notion of equivalent extensions measures how many different extensions of C by A there are when A and C are rigidly fixed.

Homomorphisms and isomorphisms between short exact sequences of multiplicative groups (9′) are defined similarly.

It is an easy exercise to see that the composition of homomorphisms of short exact sequences is also a homomorphism. Likewise, if the triple α, β, γ is an isomorphism (or equivalence) then $\alpha^{-1}, \beta^{-1}, \gamma^{-1}$ is an isomorphism (equivalence, respectively) in the reverse direction. It follows that "isomorphism" (or equivalence) is an equivalence relation on any set of short exact sequences.

Examples

(1) Let m and n be integers greater than 1. Assume n divides m and let $k = m/n$. Define a map from the exact sequence of $\mathbb{Z}$-modules in Example 2 of the preceding set of examples:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & \mathbb{Z}/k\mathbb{Z} & \xrightarrow{\iota} & \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\pi'} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where α and β are the natural projections, γ is the identity map, ι maps $a \bmod k$ to $na \bmod m$, and π' is the natural projection of $\mathbb{Z}/m\mathbb{Z}$ onto its quotient $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z})$

(which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$). One easily checks that this is a homomorphism of short exact sequences.

(2) If again $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$ is the short exact sequence of $\mathbb{Z}$-modules defined previously, map each module to itself by $x \mapsto -x$. This triple of homomorphisms gives an isomorphism of the exact sequence with itself. This isomorphism is not an equivalence of sequences since it is not the identity on the first $\mathbb{Z}$.

(3) The short exact sequences in Examples 1 and 2 following Corollary 23 are not isomorphic—the extension modules are not isomorphic $\mathbb{Z}$-modules (abelian groups). Likewise the two extensions, D_8 and Q_8, in Example 5 of the same set are not isomorphic (hence not equivalent), even though the two end terms "A" and "C" are the same for both sequences.

(4) Consider the maps

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\psi} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \mathrm{id} & & \downarrow \beta & & \downarrow \mathrm{id} & & \\ 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\psi'} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\varphi'} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where ψ maps $\mathbb{Z}/2\mathbb{Z}$ injectively into the first component of the direct sum and φ projects the direct sum onto its second component. Also ψ' embeds $\mathbb{Z}/2\mathbb{Z}$ into the *second* component of the direct sum and φ' projects the direct sum onto its *first* component. If β maps the direct sum $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ to itself by interchanging the two factors, then this diagram is seen to commute, hence giving an equivalence of the two exact sequences that is not the identity isomorphism.

(5) We exhibit two isomorphic but inequivalent $\mathbb{Z}$-module extensions. For $i = 1, 2$ define

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi_i} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

where $\psi : 1 \mapsto (2, 0)$ in both sequences, φ_1 is defined by $\varphi_1(a \bmod 4, b \bmod 2) = (a \bmod 2, b \bmod 2)$, and $\varphi_2(a \bmod 4, b \bmod 2) = (b \bmod 2, a \bmod 2)$. It is easy to see that the resulting two sequences are both short exact sequences.

An evident isomorphism between these two exact sequences is provided by the triple of maps id, id, γ, where $\gamma : \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is the map $\gamma((c, d)) = (d, c)$ that interchanges the two direct factors.

We now check that these two isomorphic sequences are *not equivalent*, as follows. Since $\varphi_1(0, 1) = (0, 1)$, any equivalence, id, β, id, from the first sequence to the second must map $(0, 1) \in \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ to either $(1, 0)$ or $(3, 0)$ in $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, since these are the two possible elements mapping to $(0, 1)$ by φ_2. This is impossible, however, since the isomorphism β cannot send an element of order 2 to an element of order 4.

Put another way, equivalences involving the same extension module B are automorphisms of B that restrict to the identity on both $\psi(A)$ and $B/\psi(A)$. Any such automorphism of $B = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ must fix the coset $(0, 1) + \psi(A)$ since this is the unique nonidentity coset containing elements of order 2. Thus maps which send this coset to different elements in C give inequivalent extensions. In particular, there is yet a third inequivalent extension involving the same modules $A = \mathbb{Z}/2\mathbb{Z}$, $B = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $C = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, that maps the coset $(0, 1) + \psi(A)$ to the element $(1, 1) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

By similar reasoning there are three inequivalent but isomorphic group extensions of $Z_2 \times Z_2$ by Z_2 with $B \cong D_8$ (cf. the exercises).

The homomorphisms α, β, γ in a homomorphism of short exact sequences are not independent. The next result gives some relations among these three homomorphisms.

Proposition 24. *(The Short Five Lemma)* Let α, β, γ be a homomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

(1) If α and γ are injective then so is β.
(2) If α and γ are surjective then so is β.
(3) If α and γ are isomorphisms then so is β (and then the two sequences are isomorphic).

Remark: These results hold also for short exact sequences of (possibly non-abelian) groups (as the proof demonstrates).

Proof: We shall prove (1), leaving the proof of (2) as an exercise (and (3) follows immediately from (1) and (2)). Suppose then that α and γ are injective and suppose $b \in B$ with $\beta(b) = 0$. Let $\psi : A \to B$ and $\varphi : B \to C$ denote the homomorphisms in the first short exact sequence. Since $\beta(b) = 0$, it follows in particular that the image of $\beta(b)$ in the quotient C' is also 0. By the commutativity of the diagram this implies that $\gamma(\varphi(b)) = 0$, and since γ is assumed injective, we obtain $\varphi(b) = 0$, i.e., b is in the kernel of φ. By the exactness of the first sequence, this means that b is in the image of ψ, i.e., $b = \psi(a)$ for some $a \in A$. Then, again by the commutativity of the diagram, the image of $\alpha(a)$ in B' is the same as $\beta(\psi(a)) = \beta(b) = 0$. But α and the map from A' to B' are injective by assumption, and it follows that $a = 0$. Finally, $b = \psi(a) = \psi(0) = 0$ and we see that β is indeed injective.

We have already seen that there is always at least one extension of a module C by A, namely the direct sum $B = A \oplus C$. In this case the module B contains a submodule C' isomorphic to C (namely $C' = 0 \oplus C$) as well as the submodule A, and this submodule complement to A "splits" B into a direct sum. In the case of groups the existence of a subgroup complement C' to a normal subgroup in B implies that B is a semidirect product (cf. Section 5 in Chapter 5). The fact that B is a direct sum in the context of modules is a reflection of the fact that the underlying group structure in this case is *abelian*; for abelian groups semidirect products are direct products. In either case the corresponding short exact sequence is said to "split":

Definition.

(1) Let R be a ring and let $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ be a short exact sequence of R-modules. The sequence is said to be *split* if there is an R-module complement to $\psi(A)$ in B. In this case, up to isomorphism, $B = A \oplus C$ (more precisely, $B = \psi(A) \oplus C'$ for some submodule C', and C' is mapped isomorphically onto C by φ: $\varphi(C') \cong C$).

(2) If $1 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 1$ is a short exact sequence of groups, then the sequence is said to be *split* if there is a subgroup complement to $\psi(A)$ in B. In this case, up to isomorphism, $B = A \rtimes C$ (more precisely, $B = \psi(A) \rtimes C'$ for some subgroup C', and C' is mapped isomorphically onto C by φ: $\varphi(C') \cong C$).

In either case the extension B is said to be a *split extension* of C by A.

The question of whether an extension splits is the question of the existence of a complement to $\psi(A)$ in B isomorphic (by φ) to C, so the notion of a split extension may equivalently be phrased in the language of homomorphisms:

Proposition 25. The short exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ of R-modules is split if and only if there is an R-module homomorphism $\mu : C \to B$ such that $\varphi \circ \mu$ is the identity map on C. Similarly, the short exact sequence $1 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 1$ of groups is split if and only if there is a group homomorphism $\mu : C \to B$ such that $\varphi \circ \mu$ is the identity map on C.

Proof: This follows directly from the definitions: if μ is given define $C' = \mu(C) \subseteq B$ and if C' is given define $\mu = \varphi^{-1} : C \cong C' \subseteq B$.

Definition. With notation as in Proposition 25, any set map $\mu : C \to B$ such that $\varphi \circ \mu = \mathrm{id}$ is called a *section* of φ. If μ is a *homomorphism* as in Proposition 25 then μ is called a *splitting homomorphism* for the sequence.

Note that a section of φ is nothing more than a choice of coset representatives in B for the quotient $B/\ker\varphi \cong C$. A section is a (splitting) homomorphism if this set of coset representatives forms a *submodule* (respectively, *subgroup*) in B, in which case this submodule (respectively, subgroup) gives a complement to $\psi(A)$ in B.

Examples

(1) The split short exact sequence $0 \to A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \to 0$ has the evident splitting homomorphism $\mu(c) = (0, c)$.

(2) The extension $0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \oplus (\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z} \to 0$, of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$ is split (with splitting homomorphism μ mapping $\mathbb{Z}/n\mathbb{Z}$ isomorphically onto the second factor of the direct sum). On the other hand, the exact sequence of $\mathbb{Z}$-modules $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$ is not split since there is no nonzero homomorphism of $\mathbb{Z}/n\mathbb{Z}$ into $\mathbb{Z}$.

(3) Neither D_8 nor Q_8 is a split extension of $Z_2 \times Z_2$ by Z_2 because in neither group is there a subgroup complement to the center (Section 2.5 gives the subgroup structures of these groups).

(4) The group D_8 *is* a split extension of Z_2 by Z_4, i.e., there is a split short exact sequence

$$1 \longrightarrow Z_4 \xrightarrow{\iota} D_8 \xrightarrow{\pi} Z_2 \longrightarrow 1,$$

namely,

$$1 \longrightarrow \langle r \rangle \xrightarrow{\iota} D_8 \xrightarrow{\pi} \langle \bar{s} \rangle \longrightarrow 1,$$

using our usual set of generators for D_8. Here ι is the inclusion map and $\pi : r^a s^b \mapsto \bar{s}^b$ is the projection onto the quotient $D_8/\langle r \rangle \cong Z_2$. The splitting homomorphism μ

maps $\langle \bar{s} \rangle$ isomorphically onto the complement $\langle s \rangle$ for $\langle r \rangle$ in D_8. Equivalently, D_8 is the semidirect product of the normal subgroup $\langle r \rangle$ (isomorphic to Z_4) with $\langle s \rangle$ (isomorphic to Z_2).

On the other hand, while Q_8 is also an extension of Z_2 by Z_4 (for example, $\langle i \rangle \cong Z_4$ has quotient isomorphic to Z_2), Q_8 is *not* a split extension of Z_2 by Z_4: no cyclic subgroup of Q_8 of order 4 has a complement in Q_8.

Section 5.5 contains many more examples of split extensions of groups.

Proposition 25 shows that an extension B of C by A is a split extension if and only if there is a splitting homomorphism μ of the projection map $\varphi : B \to C$ from B to the quotient C. The next proposition shows in particular that for modules this is equivalent to the existence of a splitting homomorphism for ψ at the other end of the sequence.

Proposition 26. Let $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ be a short exact sequence of modules (respectively, $1 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 1$ a short exact sequence of groups). Then $B = \psi(A) \oplus C'$ for some submodule C' of B with $\varphi(C') \cong C$ (respectively, $B = \psi(A) \times C'$ for some subgroup C' of B with $\varphi(C') \cong C$) if and only if there is a homomorphism $\lambda : B \to A$ such that $\lambda \circ \psi$ is the identity map on A.

Proof: This is similar to the proof of Proposition 25. If λ is given, define $C' = \ker \lambda \subseteq B$ and if C' is given define $\lambda : B = \psi(A) \oplus C' \to A$ by $\lambda((\psi(a), c') = a$. Note that in this case $C' = \ker \lambda$ is *normal* in B, so that C' is a *normal* complement to $\psi(A)$ in B, which in turn implies that B is the *direct sum* of $\psi(A)$ and C' (cf. Theorem 9 of Section 5.4).

Proposition 26 shows that for general group extensions, the existence of a splitting homomorphism λ on the *left* end of the sequence is stronger than the condition that the extension splits: in this case the extension group is a *direct* product, and not just a *semidirect* product. The fact that these two notions are equivalent in the context of modules is again a reflection of the abelian nature of the underlying groups, where semidirect products are always direct products.

Modules and $Hom_R(D, \_\_)$

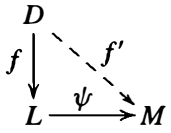
Let R be a ring with 1 and suppose the R-module M is an extension of N by L, with

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

the corresponding short exact sequence of R-modules. It is natural to ask whether properties for L and N imply related properties for the extension M. The first situation we shall consider is whether an R-module homomorphism from some fixed R-module D to either L or N implies there is also an R-module homomorphism from D to M.

The question of obtaining a homomorphism from D to M given a homomorphism from D to L is easily disposed of: if $f \in \mathrm{Hom}_R(D, L)$ is an R-module homomorphism from D to L then the composite $f' = \psi \circ f$ is an R-module homomorphism from D to

M. The relation between these maps can be indicated pictorially by the commutative diagram



Put another way, composition with ψ induces a map

$$\psi' : \mathrm{Hom}_R(D, L) \longrightarrow \mathrm{Hom}_R(D, M)$$
$$f \longmapsto f' = \psi \circ f.$$

Recall that, by Proposition 2, $\mathrm{Hom}_R(D, L)$ and $\mathrm{Hom}_R(D, M)$ are abelian groups.

Proposition 27. Let D, L and M be R-modules and let $\psi : L \to M$ be an R-module homomorphism. Then the map

$$\psi' : \mathrm{Hom}_R(D, L) \longrightarrow \mathrm{Hom}_R(D, M)$$
$$f \longmapsto f' = \psi \circ f$$

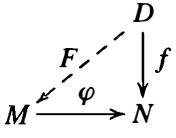
is a homomorphism of abelian groups. If ψ is injective, then ψ' is also injective, i.e.,

$$\text{if} \quad 0 \longrightarrow L \xrightarrow{\psi} M \quad \text{is exact,}$$

$$\text{then} \quad 0 \longrightarrow \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \quad \text{is also exact.}$$

Proof: The fact that ψ' is a homomorphism is immediate. If ψ is injective, then distinct homomorphisms f and g from D into L give distinct homomorphisms $\psi \circ f$ and $\psi \circ g$ from D into M, which is to say that ψ' is also injective.

While obtaining homomorphisms into M from homomorphisms into the submodule L is straightforward, the situation for homomorphisms into the quotient N is much less evident. More precisely, given an R-module homomorphism $f : D \to N$ the question is whether there exists an R-module homomorphism $F : D \to M$ that *extends* or *lifts* f to M, i.e., that makes the following diagram commute:



As before, composition with the homomorphism φ induces a homomorphism of abelian groups

$$\varphi' : \mathrm{Hom}_R(D, M) \longrightarrow \mathrm{Hom}_R(D, N)$$
$$F \longmapsto F' = \varphi \circ F.$$

In terms of φ', the homomorphism f to N lifts to a homomorphism to M if and only if f is in the image of φ' (namely, f is the image of the lift F).

In general it may not be possible to lift a homomorphism f from D to N to a homomorphism from D to M. For example, consider the nonsplit exact sequence $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$ from the previous set of examples. Let $D = \mathbb{Z}/2\mathbb{Z}$ and let f be the identity map from D into N. Any homomorphism F of D into $M = \mathbb{Z}$ must map D to 0 (since $\mathbb{Z}$ has no elements of order 2), hence $\pi \circ F$ maps D to 0 in N, and in particular, $\pi \circ F \neq f$. Phrased in terms of the map φ', this shows that

$$\text{if} \quad M \xrightarrow{\varphi} N \longrightarrow 0 \quad \text{is exact,}$$

$$\text{then} \quad \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \longrightarrow 0 \quad \text{is } \textit{not necessarily} \text{ exact.}$$

These results relating the homomorphisms into L and N to the homomorphisms into M can be neatly summarized as part of the following theorem.

Theorem 28. Let D, L, M, and N be R-modules. If

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0 \quad \text{is exact,}$$

then the associated sequence

$$0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \quad \text{is exact.} \tag{10.10}$$

A homomorphism $f : D \to N$ lifts to a homomorphism $F : D \to M$ if and only if $f \in \mathrm{Hom}_R(D, N)$ is in the image of φ'. In general $\varphi' : \mathrm{Hom}_R(D, M) \to \mathrm{Hom}_R(D, N)$ need not be surjective; the map φ' is surjective if and only if every homomorphism from D to N lifts to a homomorphism from D to M, in which case the sequence (10) can be extended to a short exact sequence.

The sequence (10) is exact for *all* R-modules D if and only if the sequence

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \quad \text{is exact.}$$

Proof: The only item in the first statement that has not already been proved is the exactness of (10) at $\mathrm{Hom}_R(D, M)$, i.e., $\ker \varphi' = \text{image } \psi'$. Suppose $F : D \to M$ is an element of $\mathrm{Hom}_R(D, M)$ lying in the kernel of φ', i.e., with $\varphi \circ F = 0$ as homomorphisms from D to N. If $d \in D$ is any element of D, this implies that $\varphi(F(d)) = 0$ and $F(d) \in \ker \varphi$. By the exactness of the sequence defining the extension M we have $\ker \varphi = \text{image } \psi$, so there is some element $l \in L$ with $F(d) = \psi(l)$. Since ψ is injective, the element l is unique, so this gives a well defined map $F' : D \to L$ given by $F'(d) = l$. It is an easy check to verify that F' is a homomorphism, i.e., $F' \in \mathrm{Hom}_R(D, L)$. Since $\psi \circ F'(d) = \psi(l) = F(d)$, we have $F = \psi'(F')$ which shows that F is in the image of ψ', proving that $\ker \varphi' \subseteq \text{image } \psi'$. Conversely, if F is in the image of ψ' then $F = \psi'(F')$ for some $F' \in \mathrm{Hom}_R(D, L)$ and so $\varphi(F(d)) = \varphi(\psi(F'(d)))$ for any $d \in D$. Since $\ker \varphi = \text{image } \psi$ we have $\varphi \circ \psi = 0$, and it follows that $\varphi(F(d)) = 0$ for any $d \in D$, i.e., $\varphi'(F) = 0$. Hence F is in the kernel of φ', proving the reverse containment: $\text{image } \psi' \subseteq \ker \varphi'$.

For the last statement in the theorem, note first that the surjectivity of φ was not required for the proof that (10) is exact, so the "if" portion of the statement has already

been proved. For the converse, suppose that the sequence (10) is exact for all R-modules D. In general, $\mathrm{Hom}_R(R, X) \cong X$ for any left R-module X, the isomorphism being given by mapping a homomorphism to its value on the element $1 \in R$ (cf. Exercise 10(b)). Taking $D = R$ in (10), the exactness of the sequence $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N$ follows easily.

By Theorem 28, the sequence

$$0 \longrightarrow \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \longrightarrow 0 \qquad (10.11)$$

is in general *not* a short exact sequence since the homomorphism φ' need not be surjective. The question of whether this sequence is exact precisely measures the extent to which the homomorphisms from D into M are uniquely determined by pairs of homomorphisms from D into L and D into N. More precisely, this sequence is exact if and only if there is a bijection $F \leftrightarrow (g, f)$ between homomorphisms $F : D \to M$ and pairs of homomorphisms $g : D \to L$ and $f : D \to N$ given by $F|_{\psi(L)} = \psi'(g)$ and $f = \varphi'(F)$.

One situation in which the sequence (11) is exact occurs when the original sequence $0 \to L \to M \to N \to 0$ is a *split* exact sequence, i.e., when $M = L \oplus N$. In this case the sequence (11) is also a split exact sequence, as the first part of the following proposition shows.

Proposition 29. Let D, L and N be R-modules. Then
(1) $\mathrm{Hom}_R(D, L \oplus N) \cong \mathrm{Hom}_R(D, L) \oplus \mathrm{Hom}_R(D, N)$, and
(2) $\mathrm{Hom}_R(L \oplus N, D) \cong \mathrm{Hom}_R(L, D) \oplus \mathrm{Hom}_R(N, D)$.

Proof: Let $\pi_1 : L \oplus N \to L$ be the natural projection from $L \oplus N$ to L and similarly let π_2 be the natural projection to N. If $f \in \mathrm{Hom}_R(D, L \oplus N)$ then the compositions $\pi_1 \circ f$ and $\pi_2 \circ f$ give elements in $\mathrm{Hom}_R(D, L)$ and $\mathrm{Hom}_R(D, N)$, respectively. This defines a map from $\mathrm{Hom}_R(D, L \oplus N)$ to $\mathrm{Hom}_R(D, L) \oplus \mathrm{Hom}_R(D, N)$ which is easily seen to be a homomorphism. Conversely, given $f_1 \in \mathrm{Hom}_R(D, L)$ and $f_2 \in \mathrm{Hom}_R(D, N)$, define the map $f \in \mathrm{Hom}_R(D, L \oplus N)$ by $f(d) = (f_1(d), f_2(d))$. This defines a map from $\mathrm{Hom}_R(D, L) \oplus \mathrm{Hom}_R(D, N)$ to $\mathrm{Hom}_R(D, L \oplus N)$ that is easily checked to be a homomorphism inverse to the map above, proving the isomorphism in (1). The proof of (2) is similar and is left as an exercise.

The results in Proposition 29 extend immediately by induction to any finite direct sum of R-modules. These results are referred to by saying that Hom *commutes with finite direct sums in either variable* (compare to Theorem 17 for a corresponding result for tensor products). For infinite direct sums the situation is more complicated. Part (1) remains true if $L \oplus N$ is replaced by an arbitrary direct sum and the direct sum on the right hand side is replaced by a direct product (Exercise 13 shows that the direct product is necessary). Part (2) remains true if the direct sums on both sides are replaced by direct products.

This proposition shows that if the sequence

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

is a split short exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \longrightarrow 0$$

is also a split short exact sequence of abelian groups for every R-module D. Exercise 14 shows that a converse holds: if $0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \to 0$ is exact for every R-module D then $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is a split short exact sequence (which then implies that if the original Hom sequence is exact for every D, then in fact it is split exact for every D).

Proposition 29 identifies a situation in which the sequence (11) is exact in terms of the modules L, M, and N. The next result adopts a slightly different perspective, characterizing instead the modules D having the property that the sequence (10) in Theorem 28 can *always* be extended to a short exact sequence:

Proposition 30. Let P be an R-module. Then the following are equivalent:

(1) For any R-modules L, M, and N, if

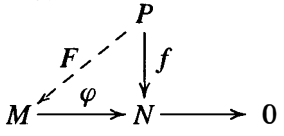
$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

is a short exact sequence, then

$$0 \longrightarrow \mathrm{Hom}_R(P, L) \xrightarrow{\psi'} \mathrm{Hom}_R(P, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(P, N) \longrightarrow 0$$

is also a short exact sequence.

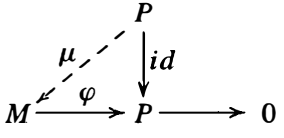
(2) For any R-modules M and N, if $M \xrightarrow{\varphi} N \to 0$ is exact, then every R-module homomorphism from P into N lifts to an R-module homomorphism into M, i.e., given $f \in \mathrm{Hom}_R(P, N)$ there is a lift $F \in \mathrm{Hom}_R(P, M)$ making the following diagram commute:



(3) If P is a quotient of the R-module M then P is isomorphic to a direct summand of M, i.e., every short exact sequence $0 \to L \to M \to P \to 0$ splits.

(4) P is a direct summand of a free R-module.

Proof: The equivalence of (1) and (2) is a restatement of a result in Theorem 28. Suppose now that (2) is satisfied, and let $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} P \to 0$ be exact. By (2), the identity map from P to P lifts to a homomorphism μ making the following diagram commute:

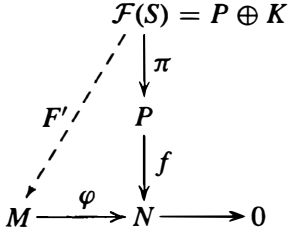


Then $\varphi \circ \mu = 1$, so μ is a splitting homomorphism for the sequence, which proves (3).

Every module P is the quotient of a free module (for example, the free module on the

set of elements in P), so there is always an exact sequence $0 \to \ker \varphi \to \mathcal{F} \xrightarrow{\varphi} P \to 0$ where $\mathcal{F}$ is a free R-module (cf. Example 4 following Corollary 23). If (3) is satisfied, then this sequence splits, so $\mathcal{F}$ is isomorphic to the direct sum of $\ker \varphi$ and P, which proves (4).

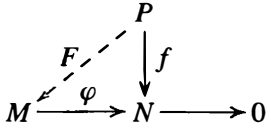
Finally, to prove (4) implies (2), suppose that P is a direct summand of a free R-module on some set S, say $\mathcal{F}(S) = P \oplus K$, and that we are given a homomorphism f from P to N as in (2). Let π denote the natural projection from $\mathcal{F}(S)$ to P, so that $f \circ \pi$ is a homomorphism from $\mathcal{F}(S)$ to N. For any $s \in S$ define $n_s = f \circ \pi(s) \in N$ and let $m_s \in M$ be any element of M with $\varphi(m_s) = n_s$ (which exists because φ is surjective). By the universal property for free modules (Theorem 6 of Section 3), there is a unique R-module homomorphism F' from $\mathcal{F}(S)$ to M with $F'(s) = m_s$. The diagram is the following:



By definition of the homomorphism F' we have $\varphi \circ F'(s) = \varphi(m_s) = n_s = f \circ \pi(s)$, from which it follows that $\varphi \circ F' = f \circ \pi$ on $\mathcal{F}(S)$, i.e., the diagram above is commutative. Now define a map $F : P \to M$ by $F(d) = F'((d, 0))$. Since F is the composite of the injection $P \to \mathcal{F}(S)$ with the homomorphism F', it follows that F is an R-module homomorphism. Then

$$\varphi \circ F(d) = \varphi \circ F'((d, 0)) = f \circ \pi((d, 0)) = f(d)$$

i.e., $\varphi \circ F = f$, so the diagram



commutes, which proves that (4) implies (2) and completes the proof.

Definition. An R-module P is called *projective* if it satisfies any of the equivalent conditions of Proposition 30.

The third statement in Proposition 30 can be rephrased as saying that any module M that projects onto P has (an isomorphic copy of) P as a direct summand, which explains the terminology.

The following result is immediate from Proposition 30 (and its proof):

Corollary 31. Free modules are projective. A finitely generated module is projective if and only if it is a direct summand of a finitely generated free module. Every module is a quotient of a projective module.

If D is fixed, then given any R-module X we have an associated abelian group $\mathrm{Hom}_R(D, X)$. Further, an R-module homomorphism $\alpha : X \to Y$ induces an abelian group homomorphism $\alpha' : \mathrm{Hom}_R(D, X) \to \mathrm{Hom}_R(D, Y)$, defined by $\alpha'(f) = \alpha \circ f$. Put another way, the map $\mathrm{Hom}_R(D, \_\_)$ is a *covariant functor* from the category of R-modules to the category of abelian groups (cf. Appendix II). Theorem 28 shows that applying this functor to the terms in the exact sequence

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

produces an exact sequence

$$0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N).$$

This is referred to by saying that $\mathrm{Hom}_R(D, \_\_)$ is a *left exact* functor. By Proposition 30, the functor $\mathrm{Hom}_R(D, \_\_)$ is *exact*, i.e., always takes short exact sequences to short exact sequences, if and only if D is projective. We summarize this as

Corollary 32. If D is an R-module, then the functor $\mathrm{Hom}_R(D, \_\_)$ from the category of R-modules to the category of abelian groups is left exact. It is exact if and only if D is a projective R-module.

Note that if $\mathrm{Hom}_R(D, \_\_)$ takes short exact sequences to short exact sequences, then it takes exact sequences of any length to exact sequences since any exact sequence can be broken up into a succession of short exact sequences.

As we have seen, the functor $\mathrm{Hom}_R(D, \_\_)$ is in general not exact on the right. Measuring the extent to which functors such as $\mathrm{Hom}_R(D, \_\_)$ fail to be exact leads to the notions of "homological algebra," considered in Chapter 17.

Examples

(1) We shall see in Section 11.1 that if $R = F$ is a field then every F-module is projective (although we only prove this for finitely generated modules).

(2) By Corollary 31, $\mathbb{Z}$ is a projective $\mathbb{Z}$-module. This can be seen directly as follows: suppose f is a map from $\mathbb{Z}$ to N and $M \xrightarrow{\varphi} N \to 0$ is exact. The homomorphism f is uniquely determined by the value $n = f(1)$. Then f can be lifted to a homomorphism $F : \mathbb{Z} \to M$ by first defining $F(1) = m$, where m is any element in M mapped to n by φ, and then extending F to all of $\mathbb{Z}$ by additivity.

By the first statement in Proposition 30, since $\mathbb{Z}$ is projective, if

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

is an exact sequence of $\mathbb{Z}$-modules, then

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, L) \xrightarrow{\psi'} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M) \xrightarrow{\varphi'} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \longrightarrow 0$$

is also an exact sequence. This can also be seen directly using the isomorphism $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M) \cong M$ of abelian groups, which shows that the two exact sequences above are essentially the same.

(3) Free $\mathbb{Z}$-modules have no nonzero elements of finite order so no nonzero finite abelian group can be isomorphic to a submodule of a free module. By Corollary 31 it follows that no nonzero finite abelian group is a projective $\mathbb{Z}$-module.

(4) As a particular case of the preceding example, we see that for $n \geq 2$ the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is not projective. By Theorem 28 it must be possible to find a short exact sequence which after applying the functor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \_\_)$ is no longer exact on the right. One such sequence is the exact sequence of Example 2 following Corollary 23:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

for $n \geq 2$. Note first that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$ since there are no nonzero $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$. It is also easy to see that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$, as follows. Every homomorphism f is uniquely determined by $f(1) = a \in \mathbb{Z}/n\mathbb{Z}$, and given any $a \in \mathbb{Z}/n\mathbb{Z}$ there is a unique homomorphism f_a with $f_a(1) = a$; the map $f_a \mapsto a$ is easily checked to be an isomorphism from $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ to $\mathbb{Z}/n\mathbb{Z}$.

Applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \_\_)$ to the short exact sequence above thus gives the sequence

$$0 \longrightarrow 0 \xrightarrow{n'} 0 \xrightarrow{\pi'} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

which is not exact at its only nonzero term.

(5) Since $\mathbb{Q}/\mathbb{Z}$ is a torsion $\mathbb{Z}$-module it is not a submodule of a free $\mathbb{Z}$-module, hence is not projective. Note also that the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \xrightarrow{\pi} \mathbb{Q}/\mathbb{Z} \to 0$ does not split since $\mathbb{Q}$ contains no submodule isomorphic to $\mathbb{Q}/\mathbb{Z}$.

(6) The $\mathbb{Z}$-module $\mathbb{Q}$ is not projective (cf. the exercises).

(7) We shall see in Chapter 12 that a finitely generated $\mathbb{Z}$-module is projective if and only if it is free.

(8) Let R be the commutative ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ under componentwise addition and multiplication. If P_1 and P_2 are the principal ideals generated by $(1, 0)$ and $(0, 1)$ respectively then $R = P_1 \oplus P_2$, hence both P_1 and P_2 are projective R-modules by Proposition 30. Neither P_1 nor P_2 is free, since any free module has order a multiple of four.

(9) The direct sum of two projective modules is again projective (cf. Exercise 3).

(10) We shall see in Part VI that if F is any field and $n \in \mathbb{Z}^+$ then the ring $R = M_n(F)$ of all $n \times n$ matrices with entries from F has the property that every R-module is projective. We shall also see that if G is a finite group of order n and $n \neq 0$ in the field F then the group ring FG also has the property that every module is projective.

Injective Modules and $Hom_R(\_\_, D)$

If $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$ is a short exact sequence of R-modules then, instead of considering maps *from* an R-module D into L or N and the extent to which these determine maps from D into M, we can consider the "dual" question of maps from L or N *to* D. In this case, it is easy to dispose of the situation of a map from N to D: an R-module map from N to D immediately gives a map from M to D simply by composing with φ. It is easy to check that this defines an injective homomorphism of abelian groups

$$\varphi' : \mathrm{Hom}_R(N, D) \longrightarrow \mathrm{Hom}_R(M, D)$$
$$f \longmapsto f' = f \circ \varphi,$$

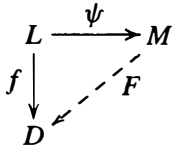
or, put another way,

$$\text{if} \quad M \xrightarrow{\varphi} N \to 0 \quad \text{is exact,}$$

$$\text{then} \quad 0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \quad \text{is exact.}$$

(Note that the associated maps on the homomorphism groups are in the reverse direction from the original maps.)

On the other hand, given an R-module homomorphism f from L to D it may not be possible to extend f to a map F from M to D, i.e., given f it may not be possible to find a map F making the following diagram commute:



For example, consider the exact sequence $0 \longrightarrow \mathbb{Z} \xrightarrow{\psi} \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ of $\mathbb{Z}$-modules, where ψ is multiplication by 2 and φ is the natural projection. Take $D = \mathbb{Z}/2\mathbb{Z}$ and let $f : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be reduction modulo 2 on the first $\mathbb{Z}$ in the sequence. There is only one nonzero homomorphism F from the second $\mathbb{Z}$ in the sequence to $\mathbb{Z}/2\mathbb{Z}$ (namely, reduction modulo 2), but this F does not lift the map f since $F \circ \psi(\mathbb{Z}) = F(2\mathbb{Z}) = 0$, so $F \circ \psi \neq f$.

Composition with ψ induces an abelian group homomorphism ψ' from $\mathrm{Hom}_R(M, D)$ to $\mathrm{Hom}_R(L, D)$, and in terms of the map ψ', the homomorphism $f \in \mathrm{Hom}_R(L, D)$ can be lifted to a homomorphism from M to D if and only if f is in the image of ψ'. The example above shows that

$$\text{if} \quad 0 \longrightarrow L \xrightarrow{\psi} M \quad \text{is exact,}$$

$$\text{then} \quad \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \longrightarrow 0 \quad \text{is } \textit{not necessarily} \text{ exact.}$$

We can summarize these results in the following dual version of Theorem 28:

Theorem 33. Let D, L, M, and N be R-modules. If

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0 \quad \text{is exact,}$$

then the associated sequence

$$0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \quad \text{is exact.} \qquad (10.12)$$

A homomorphism $f : L \to D$ lifts to a homomorphism $F : M \to D$ if and only if $f \in \mathrm{Hom}_R(L, D)$ is in the image of ψ'. In general $\psi' : \mathrm{Hom}_R(M, D) \to \mathrm{Hom}_R(L, D)$ need not be surjective; the map ψ' is surjective if and only if every homomorphism from L to D lifts to a homomorphism from M to D, in which case the sequence (12) can be extended to a short exact sequence.

The sequence (12) is exact for *all* R-modules D if and only if the sequence

$$L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0 \quad \text{is exact.}$$

Proof: The only item remaining to be proved in the first statement is the exactness of (12) at $\mathrm{Hom}_R(M, D)$. The proof of this statement is very similar to the proof of the corresponding result in Theorem 28 and is left as an exercise. Note also that the injectivity of ψ is not required, which proves the "if" portion of the final statement of the theorem.

Suppose now that the sequence (12) is exact for all R-modules D. We first show that $\varphi : M \to N$ is a surjection. Take $D = N/\varphi(M)$. If $\pi_1 : N \to N/\varphi(M)$ is the natural projection homomorphism, then $\pi_1 \circ \varphi(M) = 0$ by definition of π_1. Since $\pi_1 \circ \varphi = \varphi'(\pi_1)$, this means that the element $\pi_1 \in \mathrm{Hom}_R(N, N/\varphi(M))$ is mapped to 0 by φ'. Since φ' is assumed to be injective for all modules D, this means π_1 is the zero map, i.e., $N = \varphi(M)$ and so φ is a surjection. We next show that $\varphi \circ \psi = 0$, which will imply that image $\psi \subseteq \ker \varphi$. For this we take $D = N$ and observe that the identity map id_N on N is contained in $\mathrm{Hom}_R(N, N)$, hence $\varphi'(id_N) \in \mathrm{Hom}_R(M, N)$. Then the exactness of (12) for $D = N$ implies that $\varphi'(id_N) \in \ker \psi'$, so $\psi'(\varphi'(id_N)) = 0$. Then $id_N \circ \psi \circ \varphi = 0$, i.e., $\psi \circ \varphi = 0$, as claimed. Finally, we show that $\ker \varphi \subseteq$ image ψ. Let $D = M/\psi(L)$ and let $\pi_2 : M \to M/\psi(L)$ be the natural projection. Then $\psi'(\pi_2) = 0$ since $\pi_2(\psi(L)) = 0$ by definition of π_2. The exactness of (12) for this D then implies that π_2 is in the image of φ', say $\pi_2 = \varphi'(f)$ for some homomorphism $f \in \mathrm{Hom}_R(N, M/\psi(L))$, i.e., $\pi_2 = f \circ \varphi$. If $m \in \ker \varphi$ then $\pi_2(m) = f(\varphi(m)) = 0$, which means that $m \in \psi(L)$ since π_2 is just the projection from M into the quotient $M/\psi(L)$. Hence $\ker \varphi \subseteq$ image ψ, completing the proof.

By Theorem 33, the sequence

$$0 \longrightarrow \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \longrightarrow 0$$

is in general *not* a short exact sequence since ψ' need not be surjective, and the question of whether this sequence is exact precisely measures the extent to which homomorphisms from M to D are uniquely determined by pairs of homomorphisms from L and N to D.

The second statement in Proposition 29 shows that this sequence is exact when the original exact sequence $0 \to L \to M \to N \to 0$ is a *split* exact sequence. In fact in this case the sequence $0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \to 0$ is also a split exact sequence of abelian groups for every R-module D. Exercise 14 shows that a converse holds: if $0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \to 0$ is exact for every R-module D then $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is a split short exact sequence (which then implies that if the Hom sequence is exact for every D, then in fact it is split exact for every D).

There is also a dual version of the first three parts of Proposition 30, which describes the R-modules D having the property that the sequence (12) in Theorem 33 can *always* be extended to a short exact sequence:

Proposition 34. Let Q be an R-module. Then the following are equivalent:

(1) For any R-modules L, M, and N, if

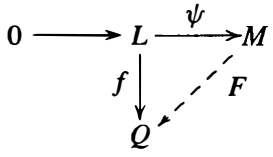
$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

is a short exact sequence, then

$$0 \longrightarrow \mathrm{Hom}_R(N, Q) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, Q) \xrightarrow{\psi'} \mathrm{Hom}_R(L, Q) \longrightarrow 0$$

is also a short exact sequence.

(2) For any R-modules L and M, if $0 \to L \xrightarrow{\psi} M$ is exact, then every R-module homomorphism from L into Q lifts to an R-module homomorphism of M into Q, i.e., given $f \in \mathrm{Hom}_R(L, Q)$ there is a lift $F \in \mathrm{Hom}_R(M, Q)$ making the following diagram commute:



(3) If Q is a submodule of the R-module M then Q is a direct summand of M, i.e., every short exact sequence $0 \to Q \to M \to N \to 0$ splits.

Proof: The equivalence of (1) and (2) is part of Theorem 33. Suppose now that (2) is satisfied and let $0 \to Q \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ be exact. Taking $L = Q$ and f the identity map from Q to itself, it follows by (2) that there is a homomorphism $F : M \to Q$ with $F \circ \psi = 1$, so F is a splitting homomorphism for the sequence, which proves (3). The proof that (3) implies (2) is outlined in the exercises.

Definition. An R-module Q is called *injective* if it satisfies any of the equivalent conditions of Proposition 34.

The third statement in Proposition 34 can be rephrased as saying that any module M into which Q injects has (an isomorphic copy of) Q as a direct summand, which explains the terminology.

If D is fixed, then given any R-module X we have an associated abelian group $\mathrm{Hom}_R(X, D)$. Further, an R-module homomorphism $\alpha : X \to Y$ induces an abelian group homomorphism $\alpha' : \mathrm{Hom}_R(Y, D) \to \mathrm{Hom}_R(X, D)$, defined by $\alpha'(f) = f \circ \alpha$, that "reverses" the direction of the arrow. Put another way, the map $\mathrm{Hom}_R(D, \_\_)$ is a *contravariant functor* from the category of R-modules to the category of abelian groups (cf. Appendix II). Theorem 33 shows that applying this functor to the terms in the exact sequence

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

produces an exact sequence

$$0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D).$$

This is referred to by saying that $\mathrm{Hom}_R(\_\_, D)$ is a *left exact* (contravariant) functor. Note that the functor $\mathrm{Hom}_R(\_\_, D)$ and the functor $\mathrm{Hom}_R(D, \_\_)$ considered earlier

are both left exact; the former reverses the directions of the maps in the original short exact sequence, the latter maintains the directions of the maps.

By Proposition 34, the functor $\mathrm{Hom}_R(\_, D)$ is *exact*, i.e., always takes short exact sequences to short exact sequences (and hence exact sequences of any length to exact sequences), if and only if D is injective. We summarize this in the following proposition, which is dual to the covariant result of Corollary 32.

Corollary 35. If D is an R-module, then the functor $\mathrm{Hom}_R(\_, D)$ from the category of R-modules to the category of abelian groups is left exact. It is exact if and only if D is an injective R-module.

We have seen that an R-module is projective if and only if it is a direct summand of a free R-module. Providing such a simple characterization of injective R-modules is not so easy. The next result gives a criterion for Q to be an injective R-module (a result due to Baer, who introduced the notion of injective modules around 1940), and using it we can give a characterization of injective modules when $R = \mathbb{Z}$ (or, more generally, when R is a P.I.D.). Recall that a $\mathbb{Z}$-module A (i.e., an abelian group, written additively) is said to be *divisible* if $A = nA$ for all nonzero integers n. For example, both $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible (cf. Exercises 18 and 19 in Section 2.4 and Exercise 15 in Section 3.1).

Proposition 36. Let Q be an R-module.

(1) *(Baer's Criterion)* The module Q is injective if and only if for every left ideal I of R any R-module homomorphism $g : I \to Q$ can be extended to an R-module homomorphism $G : R \to Q$.

(2) If R is a P.I.D. then Q is injective if and only if $rQ = Q$ for every nonzero $r \in R$. In particular, a $\mathbb{Z}$-module is injective if and only if it is divisible. When R is a P.I.D., quotient modules of injective R-modules are again injective.

Proof: If Q is injective and $g : I \to Q$ is an R-module homomorphism from the nonzero ideal I of R into Q, then g can be extended to an R-module homomorphism from R into Q by Proposition 34(2) applied to the exact sequence $0 \to I \to R$, which proves the "only if" portion of (1). Suppose conversely that every homomorphism $g : I \to Q$ can be lifted to a homomorphism $G : R \to Q$. To show that Q is injective we must show that if $0 \to L \to M$ is exact and $f : L \to Q$ is an R-module homomorphism then there is a lift $F : M \to Q$ extending f. If $\mathcal{S}$ is the collection (f', L') of lifts $f' : L' \to Q$ of f to a submodule L' of M containing L, then the ordering $(f', L') \leq (f'', L'')$ if $L' \subseteq L''$ and $f'' = f'$ on L' partially orders $\mathcal{S}$. Since $\mathcal{S} \neq \emptyset$, by Zorn's Lemma there is a maximal element (F, M') in $\mathcal{S}$. The map $F : M' \to Q$ is a lift of f and it suffices to show that $M' = M$. Suppose that there is some element $m \in M$ not contained in M' and let $I = \{r \in R \mid rm \in M'\}$. It is easy to check that I is a left ideal in R, and the map $g : I \to Q$ defined by $g(x) = F(xm)$ is an R-module homomorphism from I to Q. By hypothesis, there is a lift $G : R \to Q$ of g. Consider the submodule $M' + Rm$ of M, and define the map $F' : M' + Rm \to Q$ by $F'(m' + rm) = F(m') + G(r)$. If $m_1 + r_1 m = m_2 + r_2 m$ then $(r_1 - r_2)m = m_2 - m_1$

shows that $r_1 - r_2 \in I$, so that

$$G(r_1 - r_2) = g(r_1 - r_2) = F((r_1 - r_2)m) = F(m_2 - m_1),$$

and so $F(m_1) + G(r_1) = F(m_2) + G(r_2)$. Hence F' is well defined and it is then immediate that F' is an R-module homomorphism extending f to $M' + Rm$. This contradicts the maximality of M', so that $M' = M$, which completes the proof of (1).

To prove (2), suppose R is a P.I.D. Any nonzero ideal I of R is of the form $I = (r)$ for some nonzero element r of R. An R-module homomorphism $f : I \to Q$ is completely determined by the image $f(r) = q$ in Q. This homomorphism can be extended to a homomorphism $F : R \to Q$ if and only if there is an element q' in Q with $F(1) = q'$ satisfying $q = f(r) = F(r) = rq'$. It follows that Baer's criterion for Q is satisfied if and only if $rQ = Q$, which proves the first two statements in (2). The final statement follows since a quotient of a module Q with $rQ = Q$ for all $r \neq 0$ in R has the same property.

Examples

(1) Since $\mathbb{Z}$ is not divisible, $\mathbb{Z}$ is not an injective $\mathbb{Z}$-module. This also follows from the fact that the exact sequence $0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ corresponding to multiplication by 2 does not split.

(2) The rational numbers $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

(3) The quotient $\mathbb{Q}/\mathbb{Z}$ of the injective $\mathbb{Z}$-module $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

(4) It is immediate that a direct sum of divisible $\mathbb{Z}$-modules is again divisible, hence a direct sum of injective $\mathbb{Z}$-modules is again injective. For example, $\mathbb{Q} \oplus \mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module. (See also Exercise 4).

(5) We shall see in Chapter 12 that no nonzero finitely generated $\mathbb{Z}$-module is injective.

(6) Suppose that the ring R is an integral domain. An R-module A is said to be a *divisible* R-module if $rA = A$ for every nonzero $r \in R$. The proof of Proposition 36 shows that in this case an injective R-module is divisible.

(7) We shall see in Section 11.1 that if $R = F$ is a field then every F-module is injective.

(8) We shall see in Part VI that if F is any field and $n \in \mathbb{Z}^+$ then the ring $R = M_n(F)$ of all $n \times n$ matrices with entries from F has the property that every R-module is injective (and also projective). We shall also see that if G is a finite group of order n and $n \neq 0$ in the field F then the group ring FG also has the property that every module is injective (and also projective).

Corollary 37. Every $\mathbb{Z}$-module is a submodule of an injective $\mathbb{Z}$-module.

Proof: Let M be a $\mathbb{Z}$-module and let A be any set of $\mathbb{Z}$-module generators of M. Let $\mathcal{F} = F(A)$ be the free $\mathbb{Z}$-module on the set A. Then by Theorem 6 there is a surjective $\mathbb{Z}$-module homomorphism from $\mathcal{F}$ to M and if $\mathcal{K}$ denotes the kernel of this homomorphism then $\mathcal{K}$ is a $\mathbb{Z}$-submodule of $\mathcal{F}$ and we can identify $M = \mathcal{F}/\mathcal{K}$. Let $\mathcal{Q}$ be the free $\mathbb{Q}$-module on the set A. Then $\mathcal{Q}$ is a direct sum of a number of copies of $\mathbb{Q}$, so is a divisible, hence (by Proposition 36) injective, $\mathbb{Z}$-module containing $\mathcal{F}$. Then $\mathcal{K}$ is also a $\mathbb{Z}$-submodule of $\mathcal{Q}$, so the quotient $\mathcal{Q}/\mathcal{K}$ is injective, again by Proposition 36. Since $M = \mathcal{F}/\mathcal{K} \subseteq \mathcal{Q}/\mathcal{K}$, it follows that M is contained in an injective $\mathbb{Z}$-module.

Corollary 37 can be used to prove the following more general version valid for arbitrary R-modules. This theorem is the injective analogue of the results in Theorem 6 and Corollary 31 showing that every R-module is a quotient of a projective R-module.