Workbook in Higher Algebra

David Surowski
Department of Mathematics
Kansas State University
Manhattan, KS 66506-2602, USA
dbski@math.ksu.edu

Contents

Acknowledgement **iii**

1 Group Theory **1**
1.1 Review of Important Basics 1
1.2 The Concept of a Group Action 5
1.3 Sylow's Theorem 13
1.4 Examples: The Linear Groups 15
1.5 Automorphism Groups 17
1.6 The Symmetric and Alternating Groups 23
1.7 The Commutator Subgroup 29
1.8 Free Groups; Generators and Relations 37

2 Field and Galois Theory **43**
2.1 Basics 43
2.2 Splitting Fields and Algebraic Closure 48
2.3 Galois Extensions and Galois Groups 51
2.4 Separability and the Galois Criterion 56
2.5 Brief Interlude: the Krull Topology 62
2.6 The Fundamental Theorem of Algebra 63
2.7 The Galois Group of a Polynomial 63
2.8 The Cyclotomic Polynomials 67
2.9 Solvability by Radicals 70
2.10 The Primitive Element Theorem 71

3 Elementary Factorization Theory **73**
3.1 Basics 73
3.2 Unique Factorization Domains 77
3.3 Noetherian Rings and Principal Ideal Domains 83

3.4 Principal Ideal Domains and Euclidean Domains 86

4 Dedekind Domains **89**
4.1 A Few Remarks About Module Theory 89
4.2 Algebraic Integer Domains 93
4.3 $\mathcal{O}_{\mathbb{E}}$ is a Dedekind Domain 98
4.4 Factorization Theory in Dedekind Domains 99
4.5 The Ideal Class Group of a Dedekind Domain 102
4.6 A Characterization of Dedekind Domains 103

5 Module Theory **107**
5.1 The Basic Homomorphism Theorems 107
5.2 Direct Products and Sums of Modules 109
5.3 Modules over a Principal Ideal Domain 117
5.4 Calculation of Invariant Factors 121
5.5 Application to a Single Linear Transformation 125
5.6 Chain Conditions and Series of Modules 131
5.7 The Krull-Schmidt Theorem 134
5.8 Injective and Projective Modules 137
5.9 Semisimple Modules 144
5.10 Example: Group Algebras 148

6 Ring Structure Theory **151**
6.1 The Jacobson Radical 151

7 Tensor Products **156**
7.1 Tensor Product as an Abelian Group 156
7.2 Tensor Product as a Left S-Module 160
7.3 Tensor Product as an Algebra 165
7.4 Tensor, Symmetric and Exterior Algebra 167
7.5 The Adjointness Relationship 175

A Zorn's Lemma and some Applications **178**

Acknowledgement

The present set of notes was developed as a result of Higher Algebra courses that I taught during the academic years 1987-88, 1989-90 and 1991-92. The distinctive feature of these notes is that proofs are not supplied. There are two reasons for this. First, I would hope that the serious student who really intends to master the material will actually try to supply many of the missing proofs. Indeed, I have tried to break down the exposition in such a way that by the time a proof is called for, there is little doubt as to the basic idea of the proof. The real reason, however, for not supplying proofs is that if I have the proofs already in hard copy, then my basic laziness often encourages me not to spend any time in preparing to present the proofs in class. In other words, if I can simply read the proofs to the students, why not? Of course, the main reason for this is obvious; I end up looking like a fool.

Anyway, I am thankful to the many graduate students who checked and critiqued these notes. I am particularly indebted to Francis Fung for his scores of incisive remarks, observations and corrections. Nontheless, these notes are probably far from their final form; they will surely undergo many future changes, if only motivited by the suggestions of colleagues and future graduate students.

Finally, I wish to single out Shan Zhu, who helped with some of the more labor-intensive aspects of the preparation of some of the early drafts of these notes. Without his help, the inertial drag inherent in my nature would surely have prevented the production of this set of notes.

David B. Surowski,

Chapter 1

Group Theory

1.1 Review of Important Basics

In this short section we gather together some of the basics of elementary group theory, and at the same time establish a bit of the notation which will be used in these notes. The following terms should be well-understood by the reader (if in doubt, consult any elementary treatment of group theory): [1] *group, abelian group, subgroup, coset, normal subgroup, quotient group, order of a group, homomorphism, kernel of a homomorphism, isomorphism, normalizer of a subgroup, centralizer of a subgroup, conjugacy, index of a subgroup, subgroup generated by a set of elements* Denote the identity element of the group G by e, and set $G^{\#} = G - \{e\}$. If G is a group and if H is a subgroup of G, we shall usually simply write $H \leq G$. Homomorphisms are usually written as *left* operators: thus if $\phi : G \to G'$ is a homomorphism of groups, and if $g \in G$, write the image of g in G' as $\phi(g)$.

The following is basic in the theory of finite groups.

THEOREM 1.1.1 (LAGRANGE'S THEOREM) *Let G be a finite group, and let H be a subgroup of G. Then $|H|$ divides $|G|$.*

The reader should be quite familiar with both the statement, as well as the proof, of the following.

THEOREM 1.1.2 (THE FUNDAMENTAL HOMOMORPHISM THEOREM) *Let G, G' be groups, and assume that $\phi : G \to G'$ is a surjective homomorphism.*

[1] Many, if not most of these terms will be defined below.

Then

$$G/ker\phi \cong G'$$

via $gker\phi \mapsto \phi(g)$. *Furthermore, the mapping*

$$\phi^{-1} : \{subgroups\ of\ G'\} \to \{subgroups\ of\ \ G\ which\ contain\ ker\,\phi\}$$

is a bijection, as is the mapping

$$\phi^{-1} : \{normal\ subgroups\ of G'\} \to \{\ normal\ subgroups\ of\ G\ which\ contain\ ker\,\phi\}$$

Let G be a group, and let $x \in G$. Define the *order* of x, denoted by $o(x)$, as the least positive integer n with $x^n = e$. If no such integer exists, say that x has *infinite* order, and write $o(x) = \infty$. The following simple fact comes directly from the division algorithm in the ring of integers.

LEMMA 1.1.3 *Let G be a group, and let $x \in G$, with $o(x) = n < \infty$. If k is any integer with $x^k = e$, then $n|k$.*

The following fundamental result, known as Cauchy's theorem , is very useful.

THEOREM 1.1.4 (CAUCHY'S THEOREM) *Let G be a finite group, and let p be a prime number with p dividing the order of G. Then G has an element of order p.*

The most commonly quoted proof involves distinguishing two cases: *G is abelian*, and *G is not*; this proof is very instructive and is worth knowing.

Let G be a group and let $X \subseteq G$ be a subset of G. Denote by $\langle X \rangle$ the smallest subgroup of G containing X; thus $\langle X \rangle$ can be realized as the intersection of all subgroups $H \leq G$ with $X \subseteq H$. Alternatively, $\langle X \rangle$ can be represented as the set of all elements of the form $x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r}$ where $x_1, x_2, \ldots x_r \in X$, and where $e_1, e_2, \ldots, e_r \in \mathbb{Z}$. If $X = \{x\}$, it is customary to write $\langle x \rangle$ in place of $\langle \{x\} \rangle$. If G is a group such that for some $x \in G$, $G = \langle x \rangle$, then G is said to be a *cyclic group* with *generator* x. Note that, in general, a cyclic group can have many generators.

The following classifies cyclic groups, up to isomorphism:

LEMMA 1.1.5 *Let G be a group and let $x \in G$. Then*

$$\langle x \rangle \cong \begin{cases} (\mathbb{Z}/(n), +) & \text{if } o(x) = n, \\ (\mathbb{Z}, +) & \text{if } o(x) = \infty. \end{cases}$$

Let X be a set, and recall that the *symmetric group* S_X is the group of bijections $X \to X$. When $X = \{1, 2, \ldots, n\}$, it is customary to write S_X simply as S_n. If X_1 and X_2 are sets and if $\alpha : X_1 \to X_2$ is a bijection, there is a naturally defined group isomorphism $\phi_\alpha : S_{X_1} \to S_{X_2}$. (A "naturally" defined homomorphism is, roughly speaking, one that practically defines itself. Given this, the reader should determine the appropriate definition of ϕ_α.)

If G is a group and if H is a subgroup, denote by G/H the set of left cosets of H in G. Thus,

$$G/H \ = \ \{gH |\ g \in G\}.$$

In this situation, there is always a natural homomorphism $G \to S_{G/H}$, defined by

$$g \mapsto (xH \mapsto gxH),$$

where $g, x \in G$. The above might look complicated, but it really just means that there is a homomorphism $\phi : G \to S_{G/H}$, defined by setting $\phi(g)(xH) = (gx)H$. That ϕ really is a homomorphism is routine, but should be checked! The point of the above is that for every subgroup of a group, there is automatically a homomorphism into a corresponding symmetric group. Note further that if G is a group with $H \leq G$, $[G : H] = n$, then there exists a homomorphism $G \to S_n$. Of course this is established via the sequence of homomorphisms $G \to S_{G/H} \to S_n$, where the last map is the isomorphism $S_{G/H} \cong S_n$ of the above paragraph.

EXERCISES 1.1

1. Let G be a group and let $x \in G$ be an element of finite order n. If $k \in \mathbb{Z}$, show that $o(x^k) = n/(n, k)$, where (n, k) is the greatest common divisor of n and k. Conclude that x^k is a generator of $\langle x \rangle$ if and only if $(n, k) = 1$.

2. Let H, K be subgroups of G, both of finite index in G. Prove that $H \cap K$ also has finite index. In fact, $[G : H \cap K] = [G : H][H : H \cap K]$.

3. Let G be a group and let $H \leq G$. Define the *normalizer* of H in G by setting $N_G(H) = \{x \in G |\ xHx^{-1} = H\}$.

   (a) Prove that $N_G(H)$ is a subgroup of G.

   (b) If $T \leq G$ with $T \leq N_G(H)$, prove that $HT \leq G$.

4. Let $H \leq G$, and let $\phi : G \to S_{G/H}$ be as above. Prove that $\ker\phi = \bigcap xHx^{-1}$, where the intersection is taken over the elements $x \in G$.

5. Let $\phi : G \to S_{G/H}$ exactly as above. If $[G : H] = n$, prove that $n||\phi(G)|$, where $\phi(G)$ is the image of G in $S_{G/H}$.

6. Let G be a group of order 15, and let $x \in G$ be an element of order 5, which exists by Cauchy's theorem. If $H = \langle x \rangle$, show that $H \triangleleft G$. (Hint: We have $G \to S_3$, and $|S_3| = 6$. So what?)

7. Let G be a group, and let K and N be subgroups of G, with N normal in G. If $G = NK$, prove that there is a $1-1$ correspondence between the subgroups X of G satisfying $K \leq X \leq G$, and the subgroups T normalized by K and satisfying $N \cap K \leq T \leq N$.

8. The group G is said to be a *dihedral group* if G is generated by two elements of order two. Show that any dihedral group contains a subgroup of index 2 (necessarily normal).

9. Let G be a finite group and let $\mathbb{C}^\times$ be the multiplicative group of complex numbers. If $\sigma : G \to \mathbb{C}^\times$ is a non-trivial homomorphism, prove that $\sum_{x \in G} \sigma(x) = 0$.

10. Let G be a group of even order. Prove that G has an odd number of involutions. (An *involution* is an element of order 2.)

1.2 The Concept of a Group Action

Let X be a set, and let G be a group. Say that G *acts on* X if there is a homomorphism $\phi : G \to S_X$. (The homomorphism $\phi : G \to S_X$ is sometimes referred to as a *group action* .) It is customary to write gx or $g \cdot x$ in place of $\phi(g)(x)$, when $g \in G,\ x \in X$. In the last section we already met the prototypical example of a group action. Indeed, if G is a group and $H \leq G$ then there is a homomorphsm $G \to S_{G/H}$, i.e., G acts on the quotient set G/H by left multiplication. If $K = \ker\phi$ we say that K is the *kernel* of the action. If this kernel is trivial, we say that the group acts *faithfully* on X, or that the group action is *faithful* .

Let G act on the set X, and let $x \in X$. The *stabilizer* , $\mathrm{Stab}_G(x)$, of x in G, is the subgroup

$$\mathrm{Stab}_G(x) \ = \ \{g \in G |\ g \cdot x = x\}.$$

Note that $\mathrm{Stab}_G(x)$ is a subgroup of G and that if $g \in G,\ x \in X$, then $\mathrm{Stab}_G(gx) = g\mathrm{Stab}_G(x)g^{-1}$. If $x \in X$, the *G-orbit* in X of x is the set

$$\mathcal{O}_G(x) \ = \ \{g \cdot x |\ g \in G\} \ \subseteq X.$$

If $g \in G$ set

$$\mathrm{Fix}(g) \ = \ \{x \in X |\ g \cdot x = x\} \subseteq X,$$

the *fixed point set* of g in X. More generally, if $H \leq G$, there is the set of *H-fixed points* :

$$\mathrm{Fix}(H) \ = \ \{x \in X |\ h \cdot x = x \text{ for all } h \in H\}.$$

The following is fundamental.

Theorem 1.2.1 (Orbit-Stabilizer Reciprocity Theorem) *Let G be a finite group acting on the set X, and fix $x \in X$. Then*

$$|\mathcal{O}_G(x)| \ = \ [G : Stab_G(x)].$$

The above theorem is often applied in the following context. That is, let G be a finite group acting on itself by conjugation ($g \cdot x = gxg^{-1}$, $g, x \in G$). In this case the orbits are called *conjugacy classes* and denoted

$$\mathcal{C}_G(x) \ = \ \{gxg^{-1} |\ g \in G\}, \ \ x \in G.$$

In this context, the stabilizer of the element $x \in G$, is called the *centralizer of x in G*, and denoted

$$C_G(x) \;=\; \{g \in G|\; gxg^{-1} = x\}.$$

As an immediate corollary to *Theorem* 1.2.1 we get

COROLLARY 1.2.1.1 *Let G be a finite group and let $x \in G$. Then $|\mathcal{C}_G(x)| = [G : C_G(x)]$.*

Note that if G is a group (not necessarily finite) acting on itself by conjugation, then the kernel of this action is the *center* of the group G:

$$Z(G) \;=\; \{z \in G|\; zxz^{-1} = x \text{ for all } x \in G\}.$$

Let p be a prime and assume that P is a group (not necessarily finite) all of whose elements have finite p-power order. Then P is called a p-group. Note that if the p-group P is finite then $|P|$ is also a power of p by Cauchy's Theorem.

LEMMA 1.2.2 ("p ON p' " LEMMA) *Let p be a prime and let P be a finite p-group. Assume that P acts on the finite set X of order p', where $p \not| p'$. Then there exists $x \in X$, with $gx = x$ for all $g \in P$.*

The following is immediate.

COROLLARY 1.2.2.1 *Let p be a prime, and let P be a finite p-group. Then $Z(P) \neq \{e\}$.*

The following is not only frequently useful, but very interesting in its own right.

THEOREM 1.2.3 (BURNSIDE'S THEOREM) *Let G be a finite group acting on the finite set X. Then*

$$\frac{1}{|G|}\sum_{g\in G}|Fix(g)| \;=\; \#\ of\ G\text{-}orbits\ in\ X.$$

Burnside's Theorem often begets amusing number theoretic results. Here is one such (for another, see *Exercise* 4, below):

PROPOSITION 1.2.4 *Let x, n be integers with $x \geq 0,\ n > 0$. Then*

$$\sum_{a=0}^{n-1} x^{(a,n)} \ \equiv \ 0 \ (mod\ n),$$

where (a, n) is the greatest common divisor of a and n.

Let G act on the set X; if $\mathcal{O}_G(x) = X$, for some $x \in X$ then G is said to act *transitively* on X, or that the action is *transitive* . Note that if G acts transitively on X, then $\mathcal{O}_G(x) = X$ *for all* $x \in X$. In light of Burnside's Theorem, it follows that if G acts transitively on the set X, then the elements of G fix, on the average, one element of X.

There is the important notion of *equivalent* permutation actions. Let G be a group acting on sets $X_1,\ X_2$. A mapping $\alpha : X_1 \to X_2$ is called G-*equivariant* if for each $g \in G$ the diagram below commutes:

$$\begin{array}{ccc} X_1 & \xrightarrow{\alpha} & X_2 \\ \Big\downarrow g & & \Big\downarrow g \\ X_1 & \xrightarrow{\alpha} & X_2 \end{array}$$

If the G-equivariant mapping above is a bijection, then we say that the actions of G on X_1 and X_2 are *permutation isomorphic*, , and write $X_1 \cong_G X_2$.

An important problem of group theory, especially finite group theory, is to classify, up to equivalence, the transitive permutation representations of a given group G. That this is really an "internal" problem, can be seen from the following important result.

THEOREM 1.2.5 *Let G act transitively on the set X, fix $x \in X$, and set $H = Stab_G(x)$. Then the actions of G on X and on G/H are equivalent.*

Thus, classifying the transitive permutation actions of the group G is tantamount to having a good knowledge of the subgroup structure of G. (See *Exercises* 5, 6, 8, below.)

EXERCISES 1.2

1. Let G be a group and let $x, y \in G$. Prove that x and y are conjugate if and only if there exist elements $u, v \in G$ such that $x = uv$ and $y = vu$.

2. Let G be a finite group acting transitively on the set X. If $|X| \neq 1$ show that there exist elements of G which fix no elements of X.

3. Use *Exercise* 2 to prove the following. Let G be a finite group and let $H < G$ be a proper subgroup. Then $G \neq \cup_{g \in G} gHg^{-1}$.

4. Let n be a positive integer, and let $d(n) =$# of divisors of n. Show that
$$\sum_{\substack{a=0 \\ (a,n)=1}}^{n-1} (a-1, n) \;=\; \phi(n)d(n),$$
where ϕ is the Euler ϕ-function. (Hint: Let $Z_n = \langle x \rangle$ be the cyclic group of order n, and let $G = \mathrm{Aut}(Z_n)$.[2] What is $|G|$? [See *Section* 4, below.] How many orbits does G produce in Z_n? If $g \in G$ has the effect $x \mapsto x^a$, what is $|\mathrm{Fix}(g)|$?)

5. Assume that G acts transitively on the sets X_1, X_2. Let $x_1 \in X_1,\ x_2 \in X_2$, and let G_{x_1}, G_{x_2} be the respective stabilizers in G. Prove that these actions are equivalent if and only if the subgroups G_{x_1} and G_{x_2} are conjugate in G. (Hint: Assume that for some $\tau \in G$ we have $G_{x_1} = \tau G_{x_2} \tau^{-1}$. Show that the mapping $\alpha : X_1 \to X_2$ given by $\alpha(gx_1) = g\tau(x_2),\ g \in G$, is a well-defined bijection that realizes an equivalence of the actions of G. Conversely, assume that $\alpha : X_1 \to X_2$ realizes an equivalence of actions. If $y_1 \in X_1$ and if $y_2 = \alpha(x_1) \in X_2$, prove that $G_{y_1} = G_{y_2}$. By transitivity, the result follows.)

6. Using *Exercise* 5, classify the transitive permutation representations of the symmetric group S_3.

7. Let G be a group and let H be a subgroup of G. Assume that $H = \mathrm{N}_G(H)$. Show that the following actions of G are equivalent:

   (a) The action of G on the left cosets of H in G by left multiplication;

[2] For any group G, $\mathrm{Aut}(G)$ is the group of all automorphisms of G, *i.e.* isomorphisms $G \to G$. We discuss this concept more fully in *Section* 1.5.

(b) The action of G on the conjugates of H in G by conjugation.

8. Let $G = \langle a, b\rangle \cong Z_2 \times Z_2$. Let $X = \{\pm 1\}$, and let G act on X in the following two ways:

   (a) $a^i b^j \cdot x \;=\; (-1)^i \cdot x$.

   (b) $a^i b^j \cdot x \;=\; (-1)^j \cdot x$.

   Prove that these two actions are *not* equivalent.

9. Let G be a group acting on the set X, and let $N \triangleleft G$. Show that G acts on $\mathrm{Fix}(N)$.

10. Let G be a group acting on a set X. We say that G acts *doubly transitively* on X if given $x_1 \neq x_2 \in X,\ y_1 \neq y_2 \in X$ there exists $g \in G$ such that $gx_1 = y_1,\ gx_2 = y_2$.

    (i) Show that the above condition is equivalent to G acting transitively on $X \times X - \Delta(X \times X)$, where G acts in the obvious way on $X \times X$ and where $\Delta(X \times X)$ is the diagonal in $X \times X$.

    (ii) Assume that G is a finite group acting doubly transitively on the set X. Prove that $\dfrac{1}{|G|}\displaystyle\sum_{g\in G} |\mathrm{Fix}(g)|^2 = 2$.

11. Let X be a set and let $G_1, G_2 \leq S_X$. Assume that $g_1 g_2 = g_2 g_1$ for all $g_1 \in G_1,\ g_2 \in G_2$. Show that G_1 acts on the G_2-orbits in X and that G_2 acts on the G_1-orbits in X. If X is a finite set, show that in the above actions the number of G_1-orbits is the same as the number of G_2-orbits.

12. Let G act transitively on the set X via the homomorphism $\phi : G \to S_X$, and define $\mathrm{Aut}(G, X) = C_{S_X}(G) = \{s \in S_X |\ s\phi(g)(x) = \phi(g)s(x) \text{ for all } g \in G\}$. Fix $x \in X$, and let $G_x = \mathrm{Stab}_G(x)$. We define a new action of $N = N_G(G_x)$ on X by the rule $n \circ (g \cdot x) = (gn^{-1}) \cdot x$.

    (i) Show that the above is a well defined action of N on X.

    (ii) Show that, under the map $n \mapsto n\circ,\ n \in N$, one has $N \to \mathrm{Aut}(G, X)$.

    (iii) Show that $\mathrm{Aut}(G, X) \cong N/G_x$. (Hint: If $c \in \mathrm{Aut}(G, X)$, then by transitivity, there exists $g \in G$ such that $cx = g^{-1}x$. Argue that, in fact, $g \in N$, i.e., the homomorphism of part (ii) is onto.)

13. Let G act doubly transitively on the set X and let N be a normal subgroup of G not contained in the kernel of the action. Prove that N acts transitively on X. (The double transitivity hypothesis can be weakened somewhat; see *Exercise* 15 of *Section* 1.6.)

14. Let A be a finite abelian group and define the *character group* A^* of A by setting $A^* = \mathrm{Hom}(A, \mathbb{C}^\times)$, the set of homomorphisms $A \to \mathbb{C}^\times$, with pointwise multiplication. If H is a group of automorphisms of A, then H acts on A^* by $h(\alpha)(a) = \alpha(h(a^{-1})),\ \alpha \in A^*,\ a \in A,\ h \in H$.

    (a) Show that for each $h \in H$, the number of fixed points of h on A is the same as the number of fixed points of h on A^*.

    (b) Show that the number of H-orbits in A equals the number of H-orbits in A^*.

    (c) Show by example that the actions of H on A and on A^* need not be equivalent.

    (Hint: Let $A = \{a_1, a_2, \ldots, a_n\},\ A^* = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and form the matrix $X = [x_{ij}]$ where $x_{ij} = \alpha_i(a_j)$. If $h \in H$, set $P(h) = [p_{ij}],\ Q(h) = [q_{ij}]$, where

    $$p_{ij} = \begin{cases} 1 & \text{if } h(\alpha_i) = \alpha_j \\ 0 & \text{if } h(\alpha_i) \neq \alpha_j \end{cases}, \quad q_{ij} = \begin{cases} 1 & \text{if } h(a_i) = a_j \\ 0 & \text{if } h(a_i) \neq a_j \end{cases}.$$

    Argue that $P(h)X = XQ(h)$; by *Exercise* 9 of *page* 4 one has that $X \cdot X^* = |A| \cdot I$, where X^* is the conjugate transpose of the matrix X. In particular, X is nonsingular and so trace $P(h) =$ trace $Q(h)$.)

15. Let G be a group acting transitively on the set X, and let $\beta : G \to G$ be an automorphism.

    (a) Prove that there exists a bijection $\phi : X \to X$ such that $\phi(g \cdot x) = \beta(g) \cdot \phi(x),\ g \in G,\ x \in X$ if and only if β permutes the stabilizers of points $x \in X$.

    (b) If $\phi : X \to X$ exists as above, show that the number of such bijections is $[N_G(H) : H]$, where $H = \mathrm{Stab}_G(x)$, for some $x \in X$. (If the above number is not finite, interpret it as a cardinality.)

16. Let G be a finite group of order n acting on the set X. Assume the following about this action:

(a) For each $x \in X$, $\mathrm{Stab}_G(x) \neq \{e\}$.

(b) Each $e \neq g \in G$ fixes exactly two elements of X.

Prove that X is finite; if G acts in k orbits on X, prove that one of the following must happen:

(a) $|X| = 2$ and that G acts trivially on X (so $k = 2$).

(b) $k = 3$.

In case (b) above, write $k = k_1 + k_2 + k_3$, where $k_1 \geq k_2 \geq k_3$ are the sizes of the G-orbits on X. Prove that $k_1 = n/2$ and that $k_2 < n/2$ implies that $n = 12, 24$ or 60. (This is exactly the kind of analysis needed to analyize the proper orthogonal groups in Euclidean 3-space; see *e.g.*, L.C. Grove and C.T. Benson, *Finite Reflection Groups*", Second ed., Springer-Verlag, New York, 1985, *pp.* 17-18.)

17. Let G be a group and let H be a subgroup of G. If X is acted on by G, then it is certainly acted on by H, giving rise to the assignment $X \mapsto \mathrm{Res}^G_H X$, called the *restriction* of X *to* H. Conversely, assume that Y is a set acted on by H. On the set $G \times Y$, impose the equivalence relation $(g, y) \sim (g', y')$ if an only if there exists $h \in H$ with $g' = gh^{-1}$, $y' = hy$, $g, g' \in G$, $y, y' \in Y$. Set $G \otimes_H Y = G \times Y/\sim$, and define an action of G on $G \otimes_H Y$ by $g'(g \otimes y) = g'g \otimes y$, where $g \otimes y$ is the equivalence class in $G \otimes_H Y$ containing (g, y). Show that this gives a well-defined action of G on $G \otimes_H Y$, we write $\mathrm{Ind}^G_H Y = G \otimes_H Y$, and call the assignment $Y \mapsto \mathrm{Ind}^G_H Y$ *induction* of Y to G. Show also that if G and Y are finite, then $|G \otimes_H Y| = [G : H] \cdot |Y|$. Finally, if $|Y| = 1$, show that $G \otimes_H Y \cong_G G/H$.

18. If X_1, X_2 are sets acted on by the group G, we denote by $\mathrm{Hom}_G(X_1, X_2)$ the set of G-equivariant mappings $X_1 \to X_2$ (see page 7). Now let H be a subgroup of G, let H act on the set Y, and let G act on the set X. Define the mappings

$$\eta : \mathrm{Hom}_G(\mathrm{Ind}^G_H Y, X) \to \mathrm{Hom}_H(Y, \mathrm{Res}^G_H X),$$

$$\tau : \mathrm{Hom}_H(Y, \mathrm{Res}^G_H X) \to \mathrm{Hom}_G(\mathrm{Ind}^G_H Y, X)$$

by setting

$$\eta(\phi)(y) = \phi(1 \otimes y),\ \tau(\theta)(g \otimes y) = g\theta(y),$$

where $\phi \in \mathrm{Hom}_G(\mathrm{Ind}_H^G Y, X),\ \theta \in \mathrm{Hom}_H(Y, \mathrm{Res}_H^G X)$. Show that η and τ are inverse to each other.

1.3 Sylow's Theorem

In this section all groups are finite. Let G be one such. If p is a prime number, and if n is a nonnegative integer with $p^n||G|$, $p^{n+1} \not| |G|$, write $p^n = |G|_p$, and call p^n the *p-part* of $|G|$. If $|G|_p = p^n$, and if $P \leq G$ with $|P| = p^n$, call P a *p-Sylow subgroup* of G. The set of all p-Sylow subgroups of G is denoted $\mathrm{Syl}_p(G)$. Sylow's Theorem (see *Theorem* 1.3.2, below) provides us with valuable information about $\mathrm{Syl}_p(G)$; in particular, that $\mathrm{Syl}_p(G) \neq \emptyset$, thereby providing a "partial converse" to Lagrange's Theorem (*Theorem* 1.1.1, above). First a technical lemma[3]

LEMMA 1.3.1 *Let X be a finite set acted on by the finite group G, and let p be a prime divisor of $|G|$. Assume that for each $x \in X$ there exists a p-subgroup $P(x) \leq G$ with $\{x\} = Fix(P(x))$. Then*

(1) G is transitive on X, and

(2) $|X| \equiv 1 (mod\ p)$.

Here it is:

THEOREM 1.3.2 (SYLOW'S THEOREM) *Let G be a finite group and let p be a prime.*

(Existence) $Syl_p(G) \neq \emptyset$.

(Conjugacy) G acts transitively on $Syl_p(G)$ via conjugation.

(Enumeration) $|Syl_p(G)| \equiv 1 (mod\ p)$.

(Covering) Every p-subgroup of G is contained in some p-Sylow subgroup of G.

EXERCISES 1.3

1. Show that a finite group of order 20 has a normal 5-Sylow subgroup.
2. Let G be a group of order 56. Prove that either G has a normal 2-Sylow subgroup or a normal 7-Sylow subgroup.

[3]See, M. Aschbacher, *Finite Group Theory*, Cambridge studies in advanced mathematics 10, Cambridge University Press 1986.

3. Let $|G| = p^e m,\ p > m$, where p is prime. Show that G has a normal p-Sylow subgroup.

4. Let $|G| = pq$, where p and q are primes. Prove that G has a normal p-Sylow subgroup or a normal q-Sylow subgroup.

5. Let $|G| = pq^2$, where p and q are distinct primes. Prove that one of the following holds:

   (1) $q > p$ and G has a normal q-Sylow subgroup.

   (2) $p > q$ and G has a normal p-Sylow subgroup.

   (3) $|G| = 12$ and G has a normal 2-Sylow subgroup.

6. Let G be a finite group and let $N \triangleleft G$. Assume that for all $e \neq n \in N$, $\mathrm{C}_G(n) \leq N$. Prove that $(|N|, [G : N]) = 1$.

7. Let G be a finite group acting transitively on the set X. Let $x \in X$, $G_x = \mathrm{Stab}_G(x)$, and let $P \in \mathrm{Syl}_p(G_x)$. Prove that $N_G(P)$ acts transitively on $\mathrm{Fix}(P)$.

8. (The Frattini argument) Let $H \triangleleft G$ and let $P \in \mathrm{Syl}_p(G)$, with $P \leq H$. Prove that $G = HN_G(P)$.

9. The group G is called a CA-group if for every $e \neq x \in G$, $C_G(x)$ is abelian. Prove that if G is a CA-group, then

   (i) The relation $x \sim y$ if and only if $xy = yx$ is an equivalence relation on $G^{\#}$;

   (ii) If $\mathcal{C}$ is an equivalence class in $G^{\#}$, then $H = \{e\} \cup \mathcal{C}$ is a subgroup of G;

   (iii) If G is a finite group, and if H is a subgroup constructed as in (ii) above, then $(|H|, [G : H]) = 1$. (Hint: If the prime p divides the order of H, show that H contains a full p-Sylow subgroup of G.)

1.4 Examples: The Linear Groups

Let $\mathbb{F}$ be a field and let V be a finite-dimensional vector space over the field $\mathbb{F}$. Denote by $\mathrm{GL}(V)$ the set of non-singular linear transformations $T : V \to V$. Clearly $\mathrm{GL}(V)$ is a group with respect to composition; call this group the *general linear group* of the vector space V. If $\dim V = n$, and if we denote by $\mathrm{GL}_n(\mathbb{F})$ the multiplicative group of invertible n by n matrices over $\mathbb{F}$, then choice of an ordered basis $\mathcal{A} = (v_1, v_2, \ldots, v_n)$ yields an isomorphism

$$\mathrm{GL}(V) \xrightarrow{\cong} \mathrm{GL}_n(\mathbb{F}), \quad T \mapsto [T]_{\mathcal{A}},$$

where $[T]_{\mathcal{A}}$ is the matrix representation of T relative to the ordered basis $\mathcal{A}$.

An easy calculation reveals that the center of the general linear group $\mathrm{GL}(V)$ consists of the *scalar transformations*:

$$Z(\mathrm{GL}(V)) \;=\; \{\alpha \cdot I |\; \alpha \in \mathbb{F}\} \cong \mathbb{F}^\times,$$

where $\mathbb{F}^\times$ is the multiplicative group of nonzero elements of the field $\mathbb{F}$.

Another normal subgroup of $\mathrm{GL}(V)$ is the *special linear group* :

$$\mathrm{SL}(V) \;=\; \{T \in \mathrm{GL}(V) |\; \det T = 1\}.$$

Finally, the *projective linear group* and *projective special linear group* are defined respectively by setting

$$\mathrm{PGL}(V) \;=\; \mathrm{GL}(V)/Z(\mathrm{GL}(V)), \quad \mathrm{PSL}(V) \;=\; \mathrm{SL}(V)/Z(\mathrm{SL}(V)).$$

If $\mathbb{F} = \mathbb{F}_q$ is the finite field[4] of q elements, it is customary to use the notations $\mathrm{GL}_n(q) = \mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{SL}_n(q) = \mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{PGL}_n(q) = \mathrm{PGL}_n(\mathbb{F}_q)$, $\mathrm{PSL}_n(q) = \mathrm{PSL}_n(\mathbb{F}_q)$. These are finite groups, whose orders are given by the following:

PROPOSITION 1.4.1 *The orders of the finite linear groups are given by*

$|GL_n(q)| = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1)\cdots(q - 1).$

$|SL_n(q)| = \frac{1}{q-1}|GL_n(q)|.$

$|PGL_n(q)| = |SL_n(q)| = \frac{1}{q-1}|GL_n(q)|.$

$|PSL_n(q)| = \frac{1}{(n,q-1)}|SL_n(q)|.$

[4]We discuss finite fields in much more detail in *Section* 2.4.

Notice that the general and special linear groups $\mathrm{GL}(V)$ and $\mathrm{SL}(V)$ obviously act on the set of vectors in the vector space V. If we denote $V^\sharp = V - \{0\}$, then $\mathrm{GL}(V)$ and $\mathrm{SL}(V)$ both act transitively on $V^\sharp$, except when $\dim V = 1$ (see *Exercise* 1, below).

Next, set $P(V) = \{\text{one-dimensional subspaces of } V\}$, the *projective space of* V; note that $\mathrm{GL}(V)$, $\mathrm{SL}(V)$, $\mathrm{PGL}(V)$, and $\mathrm{PSL}(V)$ all act on $P(V)$. These actions turn out to be doubly transitive (*Exercise* 2).

A *flag* in the n-dimensional vector space V is a sequence of subspaces

$$V_{i_1} \subseteq V_{i_2} \subseteq \cdots \subseteq V_{i_r} \subseteq V,$$

where $\dim V_{i_j} = i_j,\ j = 1, 2, \cdots, r$. We call the flag $[V_{i_1} \subseteq V_{i_2} \subseteq \cdots \subseteq V_{i_r}]$ a flag of *type* $(i_1 < i_2 < \cdots < i_r)$. Denote by $\Omega(i_1 < i_2 < \cdots < i_r)$ the set of flags of type $(i_1 < i_2 < \cdots < i_r)$.

THEOREM 1.4.2 *The groups $GL(V)$, $SL(V)$, $PGL(V)$ and $PSL(V)$ all act transitively on $\Omega(i_1 < i_2 < \cdots < i_r)$.*

EXERCISES 1.4

1. Prove if $\dim V > 1$, $\mathrm{GL}(V)$ and $\mathrm{SL}(V)$ act transitively on $V^\sharp = V - \{0\}$. What happens if $\dim V = 1$?

2. Show that all of the groups $\mathrm{GL}(V)$, $\mathrm{SL}(V)$, $\mathrm{PGL}(V)$, and $\mathrm{PSL}(V)$ act doubly transitively on the projective space $P(V)$.

3. Let V have dimension n over the field $\mathbb{F}$, and consider the set $\Omega(1 < 2 < \cdots < n-1)$ of *complete flags* . Fix a complete flag

$$\mathcal{F} \ = \ [V_1 \subseteq V_2 \subseteq \cdots \subseteq V_{n-1}] \in \Omega(1 < 2 < \cdots < n-1).$$

   If $G = \mathrm{GL}(V)$ and if $B = \mathrm{Stab}_G(\mathcal{F})$, show that B is isomorphic with the group of upper triangular $n \times n$ invertible matrices over $\mathbb{F}$. If $\mathbb{F} = \mathbb{F}_q$ is finite of order $q = p^k$, where p is prime, show that $B = N_G(P)$ for some p-Sylow subgroup $P \leq G$.

4. The group $\mathrm{SL}_2(\mathbb{Z})$ consisting of 2×2 matrices having integer entries and determinant 1 is obviously a group (why?). Likewise, for any positive integer n, $\mathrm{SL}_2(\mathbb{Z}/(n))$ makes perfectly good sense and is a group. Indeed, if we reduce matrices in $\mathrm{SL}_2(\mathbb{Z})$ modulo n, then we

get a homomorphism $\rho_n : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/(n))$. Prove that this homomorphism is surjective. In particular, conclude that the group $\mathrm{SL}_2(\mathbb{Z})$ is infinite.

5. We set $\mathrm{PSL}_2(\mathbb{Z}/(n)) = \mathrm{SL}_n(\mathbb{Z}/(n))/Z(\mathrm{SL}_n(\mathbb{Z}/(n))$; show that

$$|\mathrm{PSL}_2(\mathbb{Z}/(n))| \;=\; \begin{cases} 6 & \text{if } n = 2, \\ \frac{n^3}{2}\prod_{p|n}(1-\frac{1}{p^2}) & \text{if } n > 2, \end{cases}$$

where p ranges over the distinct prime factors of n.

1.5 Automorphism Groups and the Semi-Direct Product

Let G be a group, and define $\mathrm{Aut}(G)$ to be the group of automorphisms of G, with function composition as the operation. Knowledge of the structure of $\mathrm{Aut}(G)$ is frequently helpful, especially in the following situation. Suppose that G is a group, and $H \triangleleft G$. Then G acts on H by conjugation as a group of automorphisms; thus there is a homomorphism $G \to \mathrm{Aut}(G)$. Note that the kernel of this automorphism consists of all elements of G that centralize every element of H. In particular, the homomorphism is trivial, i.e. G is the kernel, precisely when G centralizes H.

In certain situations, it is useful to know the automorphism group of a cyclic group $Z = \langle x \rangle$, of order n. Clearly, any such automorphism is of the form $x \mapsto x^a$, where $o(x^a) = n$. In turn, by *Exercise* 1 of *Section* 1.1, $o(x^a) = n$ precisely when $\gcd(a, n) = 1$. This implies the following.

PROPOSITION 1.5.1 *Let $Z_n = \langle x \rangle$ be a cyclic group of order n. Then $Aut(Z_n) \cong \mathcal{U}(\mathbb{Z}/(n))$, where $\mathcal{U}(\mathbb{Z}/(n))$ is the multiplicative group of residue classes mod(n), relatively prime to n. The isomorphism is given by $[a] \mapsto (x \mapsto x^a)$.*

It is clear that if $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ is the prime factorization of n, then

$$\mathrm{Aut}(Z_n) \cong \mathrm{Aut}(Z_{p_1}) \times \mathrm{Aut}(Z_{p_2}) \times \cdots \times \mathrm{Aut}(Z_{p_r});$$

therefore to compute the structure of $\mathrm{Aut}(Z_n)$, it suffices to determine the automorphism groups of cyclic p-groups. For the answer, see *Exercises* 1 and 2, below.

Here's a typical sort of example. Let G be a group of order $45 = 3^2 \cdot 5$. Let $P \in \mathrm{Syl}_3(G)$, $Q \in \mathrm{Syl}_5(G)$; by Sylow's theorem $Q \triangleleft G$ and so P acts on Q, forcing $P \to \mathrm{Aut}(Q)$. Since $|\mathrm{Aut}(Q)| = 4 = \phi(5)$, it follows that the kernel of the action is all of P. Thus P centralizes Q; consequently $G \cong P \times Q$. (See *Exercise* 6, below.) The reader is now encouraged to make up further examples; see *Exercises* 13, 15, and 16.

Here's another simple example. Let G be a group of order 15, and let P, Q be 3 and 5-Sylow subgroups, respectively. It's trivial to see that $Q \triangleleft G$, and so P acts on Q by conjugation. By *Proposition* 1.5.1, it follows that the action is trivial so P, Q centralize each other. Therefore $G \cong P \times Q$; since P, Q are both cyclic of relatively prime orders, it follows that $P \times Q$ is itself cyclic, i.e., $G \cong Z_{15}$. An obvious generalization is *Exercise* 13, below.

As another application of automorphism groups, we consider the *semi-direct product* construction as follows. First of all, assume that G is a group and H, K are subgroups of G with $H \leq N_G(K)$. Then an easy calculation reveals that in fact, $KH \leq G$ (see *Exercise* 3 of *Section* 1.1.). Now suppose that in addition,

(i) $G = KH$, and

(ii) $K \cap H = \{e\}$.

Then we call G the *internal semi-direct product* of K by H. Note that if G is the internal semi-direct product of K by H, and if $H \leq C_G(K)$, then G is the (internal) direct product of K and H.

The above can be "externalized" as follows. Let H, K be groups and let $\theta : H \to \mathrm{Aut}(K)$ be a homomorphism. Construct the group $K \times_\theta H$, where

(i) $K \times_\theta H \ = \ K \times H$ (*as a set*).

(ii) $(k_1, h_1) \cdot (k_2, h_2) = (k_1\theta(h_1)(k_2), h_1h_2)$.

It is routine to show that $K \times_\theta H$ is a group, relative to the above binary operation; we call $K \times_\theta H$ the *external semi-direct product* of K by H.

Finally, we can see that $G = K \times_\theta H$ is actually an internal semidirect product. To this end, set $K' = \{(k, e)|\ k \in K\}$, $H' = \{(e, h)|\ h \in H\}$, and observe that H' and K' are both subgroups of G. Furthermore,

(i) $K' \cong K$, $H' \cong H$,

(ii) $K' \triangleleft G$,

(iii) $K' \cap H' = \{e\}$,

(iv) $G = K'H'$ (so G is the internal semidirect product of K' by H'),

(v) If $k' = (k, e) \in K'$, $h' = (e, h) \in H'$, then $h'k'h'^{-1} = (\theta(h)(k), e) \in K'$. (Therefore θ determines the conjugation action of H' on K'.)

(vi) $G = K \times_\theta H \cong K \times H$ if and only if $H = \ker \phi$.

As an application, consider the following:

(1) Construct a group of order 56 with a non-normal 2-Sylow subgroup (so the 7-Sylow subgroup is normal).

(2) Construct a group of order 56 with a non-normal 7-Sylow subgroup (so the 2-Sylow subgroup is normal).

The constructions are straight-forward, but interesting. Watch this:

(1) Let $P = \langle x \rangle$, a cyclic group of order 7. By *Proposition* 1.5.1 above, $\mathrm{Aut}(P) \cong Z_6$, a cyclic group of order 6. Let $H \in \mathrm{Syl}_2(\mathrm{Aut}(P))$, so H is cyclic of order 2. Let $Q = \langle y \rangle$ be a cyclic group of order 8, and let $\theta : Q \to H$ be the unique nontrivial homorphism. Form $P \times_\theta Q$.

(2) Let $P = Z_2 \times Z_2 \times Z_2$; by *Exercise* 17, below, $\mathrm{Aut}(P) \cong \mathrm{GL}_3(2)$. That $\mathrm{GL}_3(2)$ is a group of order 168 is a fairly routine exercise. Thus, let $Q \in \mathrm{Syl}_7(\mathrm{Aut}(P))$, and let $\theta : Q \to \mathrm{Aut}(P)$ be the inclusion map. Construct $P \times_\theta Q$.

Let G be a group, and let $g \in G$. Then the automorphism $\sigma_g : G \to G$ induced by conjugation by g ($x \mapsto gxg^{-1}$) is called an *inner automorphism* of G. We set $\mathrm{Inn}(G) = \{\sigma_g |\ g \in G\} \leq \mathrm{Aut}(G)$. Clearly one has $\mathrm{Inn}(G) \cong G/Z(G)$. Next if $\tau \in \mathrm{Aut}(G)$, $\sigma_g \in \mathrm{Inn}(G)$, then $\tau\sigma_g\tau^{-1} = \sigma_{\tau g}$. This implies that $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$; we set $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$, the group of *outer automorphisms* of G. (See *Exercise* 26, below.)

Exercises 1.5

1. Let p be an odd prime; show that $\mathrm{Aut}(Z_{p^r}) \cong Z_{p^{r-1}(p-1)}$, as follows. First of all, the natural surjection $\mathbb{Z}/(p^r) \to \mathbb{Z}/(p)$ induces a surjection $\mathcal{U}(\mathbb{Z}/(p^r)) \to \mathcal{U}(\mathbb{Z}/(p))$. Since the latter is isomorphic with Z_{p-1},

conclude that $\mathrm{Aut}(Z_{p_r})$ contains an element of order $p-1$. Next, use the Binomial Theorem to prove that $(1+p)^{p^{r-1}} \equiv 1(\bmod p^r)$ but $(1+p)^{p^{r-2}} \not\equiv 1(\bmod p^r)$. Thus the residue class of $1+p$ has order p^{r-1} in $\mathcal{U}(\mathbb{Z}/(p^r))$. Thus, $\mathcal{U}(\mathbb{Z}/(p^r))$ has an element of order $p^{r-1}(p-1)$ so is cyclic.

2. Show that if $r \geq 3$, then $(1+2^2)^{2^{r-2}} \equiv 1(\bmod 2^r)$ but $(1+2^2)^{2^{r-3}} \not\equiv 1(\bmod 2^r)$. Deduce from this that the class of 5 in $\mathcal{U}(\mathbb{Z}/(2^r))$ has order 2^{r-2}. Now set $C = \langle [5] \rangle$ and note that if $[a] \in C$, then $a \equiv 1(\bmod 4)$. Therefore, $[-1] \notin C$, and so $\mathcal{U}(\mathbb{Z}/(2^r)) \cong \langle [-1] \rangle \times C$.

3. Compute Aut (Z), where Z is infinite cyclic.

4. If Z is infinite cyclic, compute the automorphism group of $Z \times Z$.

5. Let $G = KH$ be a semidirect product where $K \triangleleft G$. If also $H \triangleleft G$ show that G is the direct product of K and H.

6. Let G be a finite group of order $p^a q^b$, where p, q are distinct primes. Let $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$, and assume that P, $Q \triangleleft G$. Prove that P and Q centralize each other. Conclude that $G \cong P \times Q$.

7. Let G be a finite group of order $2k$, where k is odd. If G has more than one involution, prove that $\mathrm{Aut}(G)$ is non-abelian.

8. Prove that the following are equivalent for the group G:

   (a) G is dihedral;

   (b) G factors as a semidirect product $G = NH$, where $N \triangleleft G$, N is cyclic and H is a cyclic subgroup of order 2 of G which acts on N by inver ting the elements of N.

9. Let G be a finite dihedral group of order $2k$. Prove that G is generated by elements $n, h \in G$ such that $n^k = h^2 = e$, $hnh = n^{-1}$.

10. Let $N = \langle n \rangle$ be a cyclic group of order 2^n, and let $H = \langle h \rangle$ be a cyclic group of order 2. Define mappings $\theta_1, \theta_2 : H \to \mathrm{Aut}\ (N)$ by $\theta_1(h)(n) = n^{-1+2^{n-1}}$, $\theta_2(h)(n) = n^{1+2^{n-1}}$. Define the groups $G_1 = N \times_{\theta_1} H$, $G_2 = N \times_{\theta_2} H$. G_1 is called a *semidihedral group*, and G_2 is called a *quasi-dihedral group* . Thus, if $G = G_1$ or G_2, then G is a 2-group of order 2^{n+1} having a normal cyclic subgroup N of order 2^n.

(a) What are the possible orders of elements in $G_1 - N$?

(b) What are the possible orders of elements in $G_2 - N$?

11. Let $N = \langle n \rangle$ be a cyclic group of order 2^n, and let $H = \langle h \rangle$ be a cyclic group of order 4. Let H act on N by inverting the elements of N and form the semidirect product $G = NH$ (there's no harm in writing this as an internal semidirect product). Let $Z = \langle n^{2^{n-1}} h^2 \rangle$.

    (a) Prove that Z is a normal cyclic subgroup of G or order 2;

    (b) Prove that the group $Q = Q_{2^{n+1}} = G/Z$ is generated by elements $x, y \in Q$ such that $x^{2^n} = y^4 = e,\ yxy^{-1} = x^{-1},\ x^{2^{n-1}} = y^2$.

    The group $Q_{2^{n+1}}$, constructed above, is called the *generalized quaternion group* of order 2^{n+1}. The group Q_8 is usually just called the *quaternion group*.

12. Let G be an abelian group and let N be a subgoup of G. If G/N is an infinite cyclic group, prove that $G \cong N \times (G/N)$.

13. Let G be a group of order pq, where $p,\ q$ are primes with $p < q$. If $p \not| (q-1)$, prove that G is cyclic.

14. Assume that G is a group of order p^2q, where p and q are odd primes and where $q > p$. Prove that G has a normal q-Sylow subgroup. Give a counter-example to this assertion if $p = 2$.

15. Let G be a group of order 231, and prove that the 11-Sylow subgroup is in the center of G.

16. Let G be a group of order 385. Prove that its 11-Sylow is normal, and that its 7-Sylow is in the center of G.

17. Let $P = Z_p \times Z_p \times \cdots \times Z_p$, ($n$ factors) where p is a prime and Z_p is a cyclic group of order p. Prove that $\mathrm{Aut}(P) \cong \mathrm{GL}_n(p)$, where $\mathrm{GL}_n(p)$ is the group of $n \times n$ invertible matrices with coefficients in the field $\mathbf{Z}/(p)$.

18. Let H be a finite group, and let $G = \mathrm{Aut}(H)$. What can you say about H if

    (a) G acts transitively on $H^{\#}$?

    (b) G acts 2-transitively on $H^{\#}$?

(c) G acts 3-transitively on $H^{\#}$?

19. Assume that $G = NK$, a semi-direct product with $1 \neq N$ an abelian minimal normal subgroup of G. Prove that K is a maximal proper subgroup of G.

20. Assume that G is a group of order 60. Prove that G is either simple or has a normal 5-Sylow subgroup.

21. Let G be a dihedral group of order $2p$, where p is prime, and assume that G acts faithfully on $V = Z_2 \times Z_2 \times \cdots \times Z_2$ as a group of automorphisms. If $x \in G$ has order p, and if $C_V(x) = \{e\}$, show that for any element $\tau \in G$ of order 2, $|C_V(\tau)|^2 = |V|$.

22. Assume that $G = K_1H_1 = K_2H_2$ where $K_1, K_2 \triangleleft G$, $K_1 \cap H_1 = K_2 \cap H_2 = \{e\}$, and $K_1 \cong K_2$. Show by giving a counter-example that it need not happen that $H_1 \cong H_2$.

23. Same hypotheses as in *Exercise* 22 above, except that G is a finite group and that K_1, K_2 are p-Sylow subgroups of G for some prime p. Show in this case that $H_1 \cong H_2$.

24. Let G be a group. Show that $\mathrm{Aut}(G)$ permutes the conjugacy classes of G.

25. Let G be a group and let $H \leq G$. We say that H is *characteristic* in G if for every $\tau \in \mathrm{Aut}(G)$, we have $\tau(H) = H$. If this is the case, we write H char G. Prove the following:

    (a) If H char G, then $H \triangleleft G$.

    (b) If H char G then there is a homomorphism $\mathrm{Aut}(G) \to \mathrm{Aut}(H)$.

26. Let $G = S_6$ be the symmetric group on the set of letters $X = \{1, 2, 3, 4, 5, 6\}$, and let H be the stabilizer of the letter 1. Thus $H \cong S_5$. A simple application of Sylow's theorem shows that H acts transitively on the set Y of 5-Sylow subgroups in G, and that there are six 5-Sylow subgroups in G. If we fix a bijection $\phi : Y \to X$, then ϕ induces an automorphism of G via $\sigma \mapsto \phi^{-1}\sigma\phi$. Show that this automorphism of G must be outer.[5] (Hint: this automorphism must carry H to the normalizer of a 5-Sylow subgroup.)

[5]This is the only finite symmetric group for which there are outer automorphisms. See D.S. Passman, *Permutation Groups*, W.A. Benjamin, Inc., 1968, *pp.* 29-35.

1.6 The Symmetric and Alternating Groups

In this section we present some of the simpler properties of the symmetric and alternating groups.

Recall that, by definition, S_n is the group of permutations of the set $\{1, 2, \ldots, n\}$. Let $i_1, i_2, \ldots, i_k$ be distinct elements of $\{1, 2, \ldots, n\}$ and define $\sigma := (i_1\ i_2\ \cdots\ i_k) \in S_n$ to be the permutation satisfying $\sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \ldots,\ \sigma(i_k) = i_1,\ \sigma(i) = i$ for all $i \notin \{i_1, i_2, \cdots, i_k\}$. We call σ a *cycle* in S_n. Two cycles in S_n are said to be *disjoint* if the sets of elements that they permute nontrivially are disjoint. Thus the cycles

$$(2\ 4\ 7) \text{ and } (1\ 3\ 6\ 5)\ \in\ S_n$$

are disjoint. One has the following:

PROPOSITION 1.6.1 *If $\sigma \in S_n$, then σ can be expressed as the product of disjoint cycles. This product is unique up to the order of the factors in the product.*

A *transposition* in S_n is simply a cycle of the form $(a\ b),\ a \neq b$. That any permutation in S_n is a product of transpositions is easy; just note the factorization for cycles:

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2).$$

Let V be a vector space over the field of (say) rational numbers, and let $(v_1, v_2, \ldots, v_n) \subseteq V$ be an ordered basis. Let G act on the set $\{1, 2, \ldots, n\}$ and define $\phi : G \to \mathrm{GL}(V)$ by

$$\sigma \mapsto (v_i \mapsto v_{\sigma(i)}),\ i = 1, 2, \ldots, n.$$

One easily checks that the kernel of this homomorphism is precisely the same as the kernel of the induced map $G \to S_n$. In particular, if $G = S_n$ the homomorphism $\phi : S_n \to \mathrm{GL}(V)$ is injective. Note that the image $\phi(i\ j)$ of the transposition (i, j) is simply the identity matrix with rows i and j switched. As a result, it follows that $\det(\phi(i\ j)) = -1$. Since $\det : \mathrm{GL}(V) \to \mathbb{Q}^\times$ is a group homomorphism, it follows that $\ker(\det \circ \phi)$ is a normal subgroup of S_n, called the *alternating group of degree n* and denoted A_n. It is customary to write "sgn" in place of $\det \circ \phi$, called the "sign" homomorphism of S_n. Thus, $A_n = \ker(\mathrm{sgn})$.[6] Note that $\sigma \in A_n$ if and only

[6]The astute reader will notice that the above passage is actually tautological, as the cited property of determinants above depends on the well-definedness of "sgn."

if it is possible to write σ as a product of an even number of transpostions. (A more elementary, and indeed more honest treatment, due to E. Spitznagel, can be found in Larry Grove's book, *Algebra*, Academic Press, New York, 1983, page 17.)

Let $(i_1\ i_2\ \cdots\ i_k)$ be a k-cycle in S_n, and let $\sigma \in S_n$. One has

LEMMA 1.6.2 $\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\cdots\ \sigma(i_k))$.

From the above lemma it is immediate that the conjugacy class of an element of S_n is uniquely determined by its *cycle type*. In other words, the elements (2 5)(3 10)(1 8 7 9) and (3 7)(5 1)(2 10 4 8) are conjugate in S_{10}, but (1 3 4)(2 5 7) and (2 6 4 10)(3 9 8) are not. It is often convenient to use the notation $[1^{e_1}2^{e_2}\cdots n^{e_n}]$ to represent the conjugacy class in S_n with a typical element being the product of e_1 1-cycles, e_2 2-cycles, $\ldots, e_n$ n-cycles. Note that $\sum e_i \cdot i = n$. Thus, in particular, the conjugacy class containing the element (4 2)(1 7)(3 6 10 5) $\in S_{10}$ would be parametrized by the symbol $[1^2 2^2 4]$. Note that if σ is in the class parametrized by the symbol $[1^{e_1}\cdots]$ then $|\mathrm{Fix}(\sigma)| = e_1$.

Example. From the above discussion, it follows that

- The conjugacy classes of S_5 are parametrized by the symbols $[1^5]$, $[1^3 2]$, $[1^2 3]$, $[14]$, $[12^2]$, $[23]$, $[5]$.
- The conjugacy classes of S_6 are parametrized by the symbols $[1^6]$, $[1^4 2]$, $[1^3 3]$, $[1^2 4]$, $[1^2 2^2]$, $[123]$, $[15]$, $[2^3]$, $[24]$, $[3^2]$, $[6]$.

Before leaving this section, we shall investigate the alternating groups in somewhat greater detail. Just as the symmetric group S_n is generated by transpositions, the alternating group A_n is generated by 3-cycles. (This is easy to prove; simply show how to write a product $(ab)(cd)$ as either a 3-cycle or as a product of two 3-cycles.) The following is important.

THEOREM 1.6.3 *If $n \geq 5$, then A_n is simple.*

For $n = 5$, the above is quite easy to prove. For $n \geq 6$, see *Exercise* 19 below.

Recall that if G is a group having a subgroup $H \leq G$ of index n, then there is a homomorphism $G \to S_n$. However, if G is simple, the image of the above map is actually contained in A_n, i.e., $G \to A_n$. Indeed, there is the composition $G \to S_n \to \{\pm 1\}$; if the image of $G \to S_n$ is not contained in A_n, then G will have a normal subgroup of index 2, viz., $\ker(G \to S_n \to \{\pm 1\})$.

The above can be put to use in the following examples.

Example 1. Let G be a group of order $112 = 2^4 \cdot 7$. Then G cannot be simple. Indeed, if G were simple, then G must have 7 2-Sylow subgroups creating a homomorphism $G \to A_7$. But $|A_7|_2 = 8$, so G can't "fit," i.e., G can't be simple.

Example 2. Suppose that G is a group of order $180 = 2^2 \cdot 3^2 \cdot 5$. Again, we show that G can't be simple. If G were simple, it's not too hard to show that G must have 6 5-Sylow subgroups. But then there is a homomorphism $G \to A_6$. Since G is assumed to be simple, the homomorphism is injective, so the image of G in A_6 has index $\frac{360}{180} = 2$. But A_6 is a simple group, so it can't have a subgroup of index 2.

As mentioned above, the conjugacy classes of S_n are uniquely determined by cycle type. However, the same can't be said about the conjugacy classes in A_n. Indeed, look already at $A_3 = \{e, (123), (132)\}$, an abelian group. Thus the two 3-cycles are clearly not conjugate in A_3, even though they are conjugate in S_3. In other words the two classes in A_3 "fuse" in S_3. The abstract setting is the following. Let G be a group and let $N \triangleleft G$. Let $n \in N$, and let $\mathcal{C}$ be the G-conjugacy class of n in N:

$$\mathcal{C} \;=\; \{gng^{-1} |\; g \in G\}.$$

Clearly $\mathcal{C}$ is a union of N-conjugacy classes; it is interesting to determine how many N-conjugacy classes $\mathcal{C}$ splits into. Here's the answer:

PROPOSITION 1.6.4 *With the above notation in force, assume that $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \cdots \cup \mathcal{C}_k$ is the decomposition of $\mathcal{C}$ into disjoint N-conjugacy classes. If $n \in \mathcal{C}$, then $k = [G : C_G(n)N]$.*

The above explains why the set of 5-cycles in A_5 splits into two A_5-conjugacy classes (doesn't it? See *Exercise* 7, below.) This can all be cast in a more general framework, as follows. Let G act on a set X. Assume that X admits a decomposition as a disjoint union $X = \cup X_\alpha$ ($\alpha \in \mathcal{A}$) where for each $g \in G$ and each $\alpha \in \mathcal{A}$, $gX_\alpha = X_\beta$ for some $\beta \in \mathcal{A}$. The collection of subsets $X_\alpha \subseteq X$ is called a *system of imprimitivity* for the action. Notice that there are always the *trivial* systems of imprimitivity, viz., $X = X$, and $X = \cup_{x \in X}\{x\}$. Any other system of imprimitivity is called *non-trivial*. If the action of G on X admits a non-trivial system of imprimitivity, we say that G acts *imprimitively* on X. Otherwise we say that G acts *primitively* on X.

Consider the case investigated above, namely that of a group G and a normal subgroup N. If $n \in N$, then the classes $\mathcal{C}_G(n) = \mathcal{C}_N(n)$ precisely when the conjugation action of G on the set $\mathcal{C}_G(n)$ is a primitive one. Essentially the same proof as that of *Proposition* 1.6.4 will yield the result of *Exercise* 15, below.

EXERCISES 1.6

1. Give the parametrization of the conjugacy classes of S_7.
2. Let G be a group of order 120. Show that G can't be simple.
3. Find the conjugacy classes in A_5, A_6.
4. Prove that A_4 is the semidirect product of $Z_2 \times Z_2$ by Z_3.
5. Show that $S_n = \langle (12), (23), \ldots, (n-1\ n) \rangle$.
6. Let p be prime and let $G \leq S_p$. Assume that G contains a transposition and a p-cycle. Prove that $G = S_p$.
7. Let $x \in S_n$ be either an n-cycle or an $n-1$-cycle. Prove that $C_{S_n}(x) = \langle x \rangle$.
8. Show that S_n contains a dihedral group of order $2n$ for each positive integer n.
9. Let n be a power of 2. Show that S_n cannot contain a generalized quaternion group Q_{2n}.
10. Let G act on the set X, and let k be a non-negative integer. We say that G acts *k-transitively* on X if given any pair of sequences $(x_1, x_2, \ldots, x_k)$ and $(x'_1, x'_2, \ldots, x'_k)$ with $x_i \neq x_j$, $x'_i \neq x'_j$ for all $i \neq j$ then there exists $g \in G$ such that $g(x_i) = x'_i$, $i = 1, 2, \ldots, k$. Note that transitivity is just 1-transitivity, and double transitivity is 2-transitivity. Show that S_n acts n-transitively on $\{1, 2, \ldots, n\}$, and that A_n acts $(n-2)-$*transitively* (but not $(n-1)$-transitively) on $\{1, 2, \ldots, n\}$.
11. Let G act primitively on X. Show that G acts transitively on X.
12. Let G act doubly transitively on X. Show that G acts primitively on X.

13. Let G act transitively on the set X and assume that $Y \subseteq X$ has the property that for all $g \in G$, either $gY = Y$ or $gY \cap Y = \emptyset$. Show that the distinct subsets of the form gY form a system of imprimitivity in X.

14. Let G be a group acting transitively on the set X, let $x \in X$, and let G_x be the stabilizer in G of x. Show that G acts primitively on X if and only if G_x is a maximal subgroup of G (i.e., is not properly contained in any proper subgroup of G). (Hint: If $\{X_\alpha\}$ is a system of imprimitivity of G, and if $x \in X_\alpha$, show that the subgroup $M = \mathrm{Stab}_G(X_\alpha) = \{g \in G |\ gX_\alpha = X_\alpha\}$ is a proper subgroup of G properly containing G_x. Conversely, assume that M is a proper subgroup of G properly containing G_x. Let Y be the orbit containing $\{x\}$ in X of the subgroup M, and show that for all $g \in G$, either $gY = Y$ or $gY \cap Y = \emptyset$. Now use *Exercise* 13, above.)

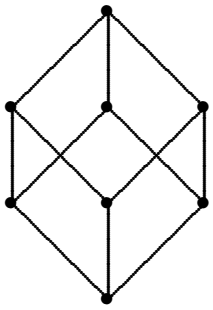
15. Let G act on the set X, and assume that $N \triangleleft G$. Show that the N-orbits of N on X form a system of imprimitivity. In particular, if the action is primitive, and if N is not in the kernel of this action, conclude that N acts transitively on X.

16. Prove the following simplicity criterion. Let G act primitively on the finite set X and assume that for $x \in X$, the stabilizer G_x is simple. Then either

    (a) G is simple, or

    (b) G has a normal transitive subgroup N with $|N| = |X|$. (Such a subgroup is called a *regular normal subgroup* .)

17. Let G be the group of automorphisms of the "cubical graph," depicted below:



Show that there are two distinct decompositions of the vertices of the above graph into systems of imprimitivity: one is as four sets of two vertices each and the other is as two sets of four vertices each. In the second decomposition, if V denotes the vertices and if $V = V_1 \cup V_2$ is the decomposition of V into two sets of imprimitivity of four vertices each, show that the setwise stabilizer of V_1 is isomorphic with S_4.

18. Let G act on X, and assume that N is a regular normal subgroup of G. Thus, if $x \in X$, then G_x acts on $X - \{x\}$ and, by conjugation, on $N^{\#} := N - \{1\}$. Prove that these actions are equivalent.

19. Using *Exercises* 16 and 18, prove that the alternating groups of degree ≥ 6 are simple.

20. Let G act on the set $\{1, 2, \ldots, n\}$, let $\mathbb{F}$ be a field and let V be the $\mathbb{F}$-vector space with ordered basis $(v_1, v_2, \ldots, v_n)$. As we have already seen, G acts on V via the homomorphism $\phi : G \to \mathrm{GL}(V)$. Set $V^G = \{v \in V |\ \phi(g)v = v\}$.

    (a) Show that $\dim V^G =$ the number of orbits of G on $\{1, 2, \ldots, n\}$.

    (b) Let $V_1 \subseteq V$ be a G-invariant subspace of V; thus G acts as a group of linear transformations on the quotient space V/V_1. Show that if the field $\mathbb{F}$ has characteristic 0 or is prime to the order of $|\phi(G)|$, then
    $$(V/V_1)^G \cong V^G/V_1^G.$$

    (c) Assume that $G_1, G_2 \leq S_n$, acting on V as usual. If $g_1 g_2 = g_2 g_1$ for all $g_1 \in G_1,\ g_2 \in G_2$ show that G_2 acts on V^{G_1} and that $(V^{G_1})^{G_2} = V^{G_1} \cap V^{G_2}$. Use this result to obtain another solution of *Exercise* 11 of *Section* 1.2.

1.7 The Commutator Subgroup and Iterated Constructions

For any group G there is the so-called *commutator subgroup* , G' (or sometimes denoted $[G, G]$) which is defined by setting

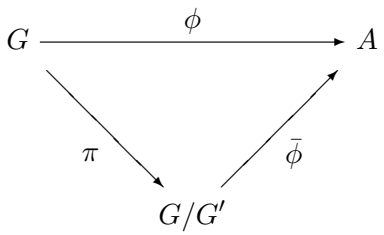
$$G' \;=\; \langle xyx^{-1}y^{-1} |\; x, y \in G \rangle.$$

Note that G is a normal subgroup of G, since the conjugate of any *commutator* $[x, y] := xyx^{-1}y^{-1}$ is again a commutator. If you think about the following long enough, it becomes very obvious.

PROPOSITION 1.7.1 *Let G be a group, with commutator subgroup G'.*

(a) G/G' is an abelian group.

(b) If $\phi : G \to A$ is a homomorphism into the abelian group A, then there is a unique factorization of ϕ, according to the commutativity of the diagram below:



The following concept is quite useful, especially in the present context. Let G be a group, and let $H \leq G$. H is called a *characteristic subgroup* of G (and written H char G) if for any automorphism $\alpha : G \to G$, $\alpha(H) = H$. Note that since conjugation by an element $g \in G$ is an automorphism of G, it follows that any characteristic subgroup of G is normal. The following property is clear, but useful:

$$H \text{ char } N \text{ char } G \Longrightarrow H \text{ char } G.$$

In particular, since the commutator subgroup G' of G is easily seen to be a characteristic subgroup of G, it follows that the iterated commutators

$G^{(1)} = G', G^{(2)} = (G^{(1)})', \ldots$ are all characteristic, hence normal, subgroups of G.

By definition, a group G is *solvable* if for some k, $G^{(k)} = \{e\}$. The historical importance of solvable groups will be seen later on, in the discussions of *Galois Theory* in *Chapter* 2.

The following is fundamental, and reveals the inductive nature of solvability:

THEOREM 1.7.2 *If $N \triangleleft G$, then G is solvable if and only if both G/N and N are solvable.*

There is an alternative, and frequently more useful way of defining solvability. First, a *normal series* in G is a sequence

$$G = G_0 \geq G_1 \geq \cdots,$$

with each G_i normal in G. Thus, the commutator series

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \cdots$$

is a normal series. Note that G acts on each quotient G_i/G_{i+1} in a normal series by conjugation (how is this?). A *subnormal series* is just like a normal series, except that one requires only that each G_i be normal in G_{i-1} (and not necessarily normal in G). The following is often a useful characterization of solvability.

THEOREM 1.7.3 *A group G is solvable if and only if it has a subnormal series of the form*

$$G = G_0 \geq G_1 \geq \cdots \geq G_m = \{e\}$$

with each G_i/G_{i+1} abelian.

A subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_m = \{e\}$ is called a *composition series* if each quotient G_i/G_{i+1} is a non-trivial simple group. Obviously, any finite group has a composition series. As a simple example, if $n \geq 5$, then $S_n \geq A_n \geq \{e\}$ is a composition series. For $n = 4$ one has a composition series for S_4 of the form $S_4 \geq A_4 \geq K \geq Z \geq \{e\}$, where $K \cong Z_2 \times Z_2$ and $Z \cong Z_2$.

While it seems possible for a group to be resolvable into a composition series in many different ways, the situation is not too bad for finite groups.

THEOREM 1.7.4 (JORDAN-HÖLDER THEOREM.) *Let G be a finite group, and let*

$$G = G_0 \geq G_1 \geq \cdots \geq G_h = \{e\},$$
$$G = H_0 \geq H_1 \geq \cdots \geq H_k = \{e\}$$

be composition series for G. Then $h = k$ and there is a bijective correspondence between the sets of composition quotients so that these corresponding quotients are isomorphic.

Let G be a group, and let $H, K \leq G$ with $K \triangleleft G$. We set $[H, K] = \langle [h, k] |\ h \in H,\ k \in K \rangle$, the *commutator* of H and K. Note that $[H, K] \leq K$. In particular, set $L^0(G) = G, L^1(G) = [G, L^0(G)], \ldots L^i(G) = [G, L^{i-1}(G)], \ldots$. Now consider the series

$$L^0(G) \geq L^1(G) \geq L^2(G) \cdots.$$

Note that this series is actually a normal series. This series is called the *lower central series* for G. If $L^i(G) = \{e\}$ for some i, call G *nilpotent* . Note that G acts trivially by conjugation on each factor in the lower central series. In fact,

THEOREM 1.7.5 *The group G is nilpotent if and only if it has a finite normal series, with each quotient acted on trivially by G.*

The descending central series is computed from "top to bottom" in a group G. There is an analogous series, constructed from "bottom to top:"

$$Z_0(G) = \{e\} \leq Z_1(G) = Z(G) \leq Z_2(G) \leq Z_3(G) \leq \cdots,$$

where $Z_{i+1} = Z(G/Z_i(G))$ for each i. Again this is a normal series, and it is clear that G acts trivially on each $Z_i(G)/Z_{i+1}(G)$. Thus, the following is immediate:

THEOREM 1.7.6 *G is nilpotent if and only if $Z_m(G) = G$ for some $m \geq 0$.*

The following should be absolutely clear.

THEOREM 1.7.7 **Abelian $\Longrightarrow$ Nilpotent $\Longrightarrow$ Solvable**

The reader should be quickly convinced that the above implications cannot be reversed.

We conclude this section with a characterization of finite nilpotent groups; see *Theorem* 1.7.10, below.

PROPOSITION 1.7.8 *If P is a finite p-group, then P is nilpotent.*

LEMMA 1.7.9 *If G is nilpotent, and if H is a proper subgroup of G, then $H \neq N_G(H)$. Thus, normalizers "grow" in nilpotent groups.*

The above ahows that the Sylow subgroups in a nilpotent group are all normal, In fact,

THEOREM 1.7.10 *Let G be a finite group. Then G is nilpotent if and only if G is the direct product of its Sylow subgroups.*

EXERCISES 1.7

1. Show that H char $N \triangleleft G \Rightarrow H \triangleleft G$.
2. Let H be a subgroup of the group G with $G' \leq H$. Prove that $H \triangleleft G$.
3. Let G be a finite group and let P be a 2-Sylow subgroup of G. If $M \leq P$ is a subgroup of index 2 in P and if $\tau \in G$ is an involution *not* conjugate to any element of M, conclude that $\tau \notin G'$ (commutator subgroup). [Hint: Look at the action of τ on the set of left cosets of M in G. If τ an even permutation or an odd permutation?]
4. Show that any subgroup of a cyclic group is characteristic.
5. Give an example of a group G and a normal subgroup K such that K isn't characteristic in G.
6. Let G be a group. Prove that G' is the intersection of all normal subgroups $N \triangleleft G$, such that G/N is abelian.
7. Give an example of a subnormal series in A_4 that isn't a normal series.
8. Let G be a group and let $x, y \in G$. If $[x, y]$ commutes with x and y, prove that for all positive integers k, $(xy)^k = x^k y^k [y, x]^{\binom{k}{2}}$.
9. A sequence of homomorphisms $K \xrightarrow{\alpha} G \xrightarrow{\beta} H$ is called *exact* (at G) if im α = ker β . Prove the following mild generalization of *Theorem* 1.7.2. If $K \xrightarrow{\alpha} G \xrightarrow{\beta} H$ is an exact sequence with K, H both solvable groups, so is G.

10. Let $K \to G_1 \to G_2 \to H$ be an exact sequence of homomorphisms of groups (meaning exactness at both G_1 and G_2.) If K and H are both solvable, must G_1 and/or G_2 be solvable? Prove, or give a counter-example.

11. Let $\mathbb{F}$ be a field and let

$$G = \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix} \mid \alpha, \beta, \gamma \in \mathbb{F}, \alpha\gamma \neq 0 \right\}.$$

Prove that G is a solvable group.

12. Let G be a finite solvable group, and let $K \triangleleft G$ be a *minimal* normal subgroup. Prove that K is an elementary abelian p-group for some prime p (i.e., $K \cong Z_p \times Z_p \times \cdots \times Z_p$).

13. Show that the finite group G is solvable if and only if it has a subnormal series

$$G = G_0 \geq G_1 \geq \cdots \geq G_m = \{e\},$$

with each G_i/G_{i+1} a group of prime order.

14. By now you may have realized that if G is a finite nonabelian simple group of order less than or equal to 200, then $|G| = 60$ or 168. Using this, if G is a nonsolvable group of order less than or equal to 200, what are the possible group orders?

15. Let q be a prime power; we shall investigate the special linear group $G = \mathrm{SL}_2(q)$.

    (a) Show that G is generated by its elements of order p, where $q = p^a$. This is perhaps best done by investigating the equations

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & (\alpha-1)\gamma^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix} \begin{bmatrix} 1 & (\delta-1)\gamma^{-1} \\ 0 & 1 \end{bmatrix}, \text{ if } \gamma \neq 0,$$

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (\delta-1)\beta^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ (\alpha-1)\beta^{-1} & 1 \end{bmatrix}, \text{ if } \beta \neq 0,$$

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \alpha^{-1}-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \alpha-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -\alpha^{-1} \\ 0 & 1 \end{bmatrix}.$$

(b) Show that if $q \geq 4$, then $G' = G$. Indeed, look at

$$\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{bmatrix} \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \mu^{-1} & 0 \\ 0 & \mu \end{bmatrix} = \begin{bmatrix} 1 & \alpha(1-\mu^2) \\ 0 & 1 \end{bmatrix}.$$

(c) Conclude that if $q \geq 4$, then the groups $\mathrm{GL}_2(q)$, $\mathrm{SL}_2(q)$, $\mathrm{PSL}_2(q)$ are all nonsolvable groups.

16. If p and q are primes, show that any group of order p^2q is solvable.

17. More generally, let G be a group of order p^nq, where p and q are primes. Show that G is solvable. (Hint: Let P_1 and P_2 be distinct p-Sylow subgroups such that $H := P_1 \cap P_2$ is maximal among all such pairs of intersections. Look at $N_G(H)$ and note that if Q is a q-Sylow subgroup of G, then $Q \leq N_G(H)$. Now write $G = Q \cdot P_1$ and conclude that the group $H^* = \langle gHg^{-1} |\ g \in G \rangle$ is, in fact, a normal subgroup of G *and is contained in* P_1. Now use induction together with *Theorem* 1.7.2.)

18. Let P be a p-group of order p^n. Prove that for all $k = 1, 2, \ldots n$, P has a normal subgroup of order p^k.

19. Let G be a finite group and let N_1, N_2 be normal nilpotent subgroups. Prove that N_1N_2 is again a normal nilpotent subgroup of G. (Hint: use *Theorem* 1.7.10.)

20. (*The Heisenberg Group.*) Let V be an m-dimensional vector space over the field $\mathbb{F}$, and assume that $\mathbb{F}$ either has characteristic 0 or has odd characteristic. Assume that $\langle\ ,\ \rangle : V \times V \to \mathbb{F}$ is a *non-degenerate, alternating* bilinear form. This means that

    (i) $\langle v, w \rangle = -\langle w, v \rangle$ for all $v, w \in V$, and

    (ii) $\langle v, w \rangle = 0$ for all $w \in V$ implies that $v = 0$.

    Now define a group, $\mathcal{H}(V)$, the *Heisenberg group*, as follows. We set $\mathcal{H}(V) = V \times \mathbb{F}$, and define multiplication by setting

    $$(v_1, \alpha_1) \cdot (v_2, \alpha_2) \ = \ (v_1 + v_2, \alpha_1 + \alpha_2 + \frac{1}{2}\langle v_1, v_2 \rangle),$$

    where $v_1, v_2 \in V$, and $\alpha_1, \alpha_2 \in \mathbb{F}$. Show that

    (i) $\mathcal{H}(V)$, with the above operation, is a group.

(ii) If $\mathcal{H} = \mathcal{H}(V)$, then $Z(\mathcal{H}) = \{(0, \alpha) |\ \alpha \in \mathbb{F}\}$.

(iii) $\mathcal{H}' = Z(\mathcal{H})$, and so $\mathcal{H}$ is a nilpotent group.

21. *The Frattini subgroup of a finite p-group.* Let P be a finite p-group, and let $\Phi(P)$ be the intersection of all maximal subgroups of P. Prove that

(i) $P/\Phi(P)$ is elementary abelian.

(ii) $\Phi(P)$ is trivial if and only if P is elementary abelian.

(iii) If $P = \langle a, \Phi(P)\rangle$, then $P = \langle a\rangle$.

(Hint: for (i) prove first that if $M \leq P$ is a maximal subgroup of P, then $[M : P] = p$ and so $M \lhd P$. This shows that if $x \in P$, the $x^p \in M$. By the same token, as P/M is abelian, $P' \leq M$. Since M was an arbitrary maximal subgroup this gives (i). Part (ii) should be routine.)

22. Let P be a finite p-group, and assume that $|P| = p^k$. Prove that the number of maximal subgroups (i.e., subgroups of index p) is less than or equal to $(p^k - 1)/(p - 1)$ with equality if and only if P is elementary abelian. (Hint: If P is elementary abelian, then we regard P as a vector space over the field $\mathbb{Z}/(p)$. Thus subgroups of index p become vector subspaces of dimension $k - 1$; and easy count shows that there are $(p^k - 1)/(p - 1)$ such. If P is not elementary abelian, then $\Phi(P)$ is not trivial, and every maximal subgroup of P contains $\Phi(P)$. Thus the subgroups of P of index P correspond bijectively with maximal subgroups of $P/\Phi(P)$; apply the above remark.)

23. Let P be a group and let p be a prime. Say that P is a C_p-group if whenever $x, y \in P$ satisfy $x^p = y^p$, then $xy = yx$. (Note that dihedral and generalized quaternion groups of order at least 8 are definitely not C_2-groups.) Prove that if P is a p-group where p is an odd prime, and if every element of order p is in $Z(P)$, then P is a C_p-group, by proving the following:

(a) Let P be a minimal counterexample to the assertion, and let $x, y \in P$ with $x^p = y^p$. Argue that $P = \langle x, y\rangle$.

(b) Show that $(yxy^{-1})^p = x^p$.

(c) Show that $yxy^{-1} \in \langle x, \Phi(P)\rangle$; conclude that $\langle x, yxy^{-1}\rangle$ is a proper subgroup of P. Thus, by (b), x and yxy^{-1} commute.

(d) Conclude from (c) that if $z = [x, y] = xyx^{-1}y^{-1}$, then $z^p = [x^p, y] = [y^p, y] = e$. Thus, by hypothesis, z commutes with x and y.

(e) Show that $[y^{-1}, x] = [x, y]$. (Conjugate z by y^{-1}.)

(f) Show that $(xy^{-1})^p = e$. (Use *Exercise* 8.)

(g) Conclude that x and y commute, a contradition.[7]

24. Here's an interesting simplicity criterion. Let G be a group acting primitively on the set X, and let H be the stabilizer of some element of X. Assume

(i) $G = G'$,

(i) H contains a normal solvable subgroup A such that G is generated by the conjugates of A.

Prove that G is simple.

25. Using the above exercise, prove that the groups $\mathrm{PSL}_2(q)$ $q \geq 4$ are all simple groups.

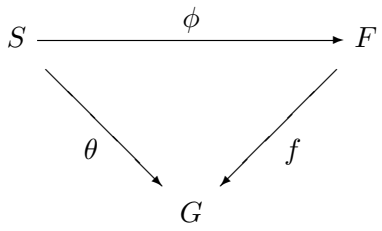
26. Let G be a group and let $Z = Z(G)$. Prove that if G/Z is nilpotent, so is G.

27. Let G be a finite group such that for any subgroup H of G we have $[G : N_G(H)] \leq 2$. Prove that G is nilpotent.

[7]The above have been extracted from Bianchi, Gillio Berta Mauri and Verardi, Groups in which elements with the same p-power permute, *LE MATHEMATICHE*, Vol. LI (1996) - Supplemento, *pp.* 53-61. The authors actually show that a necessary and sufficient condition for a p-group to be a C_p-group is that all elements of order p are central. In the general case when G is not a p-group, then the authors show that G is a p-group if and only if G has a normal p-Sylow sugroup which is also a p-group.

1.8 Free Groups; Generators and Relations

Let S be a nonempty set and let F be a group. Say that F is *free* on S if there exists a function $\phi : S \to F$ such that if G is any group and $\theta : S \to G$ is any function then there is a unique homomorphism $f : F \to G$ such that the diagram



commutes.

The following is routine, but important (see *Exercises* 1, 2 and 3):

PROPOSITION 1.8.1 *Let F be free on the set S, with mapping $\phi : S \to F$.*

(i) $\phi : S \to F$ is injective.

(ii) $F = \langle \phi(S) \rangle$.

(iii) Via the map $\phi : \{s\} \to \mathbb{Z}$, $\phi(s) = 1$, the additive group $\mathbb{Z}$ is free on one generator.

(iv) If F is free on a set with more than one generator, then F is non-abelian.

The following is absolutely fundamental.

PROPOSITION 1.8.2 *If S is nonempty, then a free group exists on S, and is unique up to isomorphism.*

Now let G be an arbitrary group. It is clear that G is the homomorphic image of some free group F. Indeed, let F be the free group on the set G; the map $F \to G$ is then that induced by $1_G : G \to G$. More generally (and economically), if $G = \langle S \rangle$, and if F is free on S, then the homomorphism $F \to G$ induced by the inclusion $S \to G$ is surjective.

The following notation, though not standard, will prove useful. Let H be a group, and let R be a subset of H. Denote by $\langle\langle R\rangle\rangle$ the smallest normal subgroup of H which contains R. This normal subgroup $\langle\langle R\rangle\rangle$ is called the *normal closure* of R. The reader should note carefully the difference between $\langle R\rangle$ and $\langle\langle R\rangle\rangle$. Now assume that $G = \langle S\rangle$ is a group, and that F is free on S, with the obviously induced homomorphism $F \to G$. Let $K = \ker(F \to G)$, and assume that $K = \langle\langle R\rangle\rangle$. Then it is customary to say that G has *generators* S and *relations* R, or that G has *presentation*

$$G \;=\; \langle S|\; r = e, r \in R\rangle.$$

A simple example is in order here. Let D be a dihedral group of order $2k$; thus D is generated by elements $n, k \in D$ such that $n^k = h^2 = e,\ hnh = n^{-1}$. Let F be the free group on the set $S = \{x, y\}$. The kernel of the homomorphism $F \to D$ determined by $x \mapsto n,\ y \mapsto h$ can be shown to be $\langle\langle x^k, y^2, (yx)^2\rangle\rangle$ (we'll prove this below). Thus D has presentation

$$D \;=\; \langle x, y|\; x^k = y^2 = (xy)^2 = e\rangle.$$

One need not always write each "relation" in the form $r = e$. Indeed, the above presentation might just as well have been written as

$$D \;=\; \langle x, y|\; x^k = y^2 = e, yxy = x^{-1}\rangle.$$

The concept of generators and relations is meaningful in isolation, i.e., without reference to a given group G. Thus, if one were to write "Consider the group

$$G \;=\; \langle x, y|\; x^4 = y^2 = (xy)^2 = e\rangle,"$$

then one means the following. Let F be the free group on the set $S = \{X, Y\}$ and let $K = \langle\langle X^4, Y^2, (XY)^2\rangle\rangle$. Then G is the quotient group F/K, and the elements x, y are simply the cosets $XK, YK \in G/K$.

Presented groups, i.e., groups of the form $\langle S|R\rangle$ are nice in the sense that if H is any group and if $\phi : S \to H$ is any function, then ϕ determines a uniquely defined homomorphism $\langle S|R\rangle \to H$ precisely when ϕ "kills all elements of R." This fact is worth displaying conspicuously.

THEOREM 1.8.3 *Let $\langle S|\ R\rangle$ be a presented group, and let $\phi : S \to H$ be a function, where H is a group. Then ϕ extends uniquely to a homomorphism $\langle S|\ R\rangle \to H$ if and only if*

$$\phi(s_2)\phi(s_2)\cdots\phi(s_r) \;=\; e$$

whenever $s_1 s_2 \cdots s_r \in R$.

To see this in practice, consider the presented group $G = \langle x, y | x^2 = y^3 = (xy)^3 = e\rangle$, and let $H = A_4$, the alternating group on 4 letters. Let ϕ be the assignment

$$\phi : \ x \mapsto (1\ 2)(3\ 4);\ y \mapsto (1\ 2\ 3);$$

since $((1\ 2)(3\ 4))^2 = (1\ 2\ 3)^3 = ((1\ 2)(3\ 4)(1\ 2\ 3))^3 = e$, the above theorem guarantees that ϕ extends to a homorphism $\phi : \langle x, y | x^2 = y^3 = (xy)^3 = e\rangle \to A_4$. Furthermore, since $A_4 = \langle (1\ 2)(3\ 4), (1\ 2\ 3)\rangle$, we conclude that ϕ is onto. That ϕ is actually an isomorphism is a little more difficult (see *Exercise* 11); we turn now to issues of this type.

Consider again the dihedral group $D = \langle n, h\rangle$ of order $2k$, where $n^k = h^2 = e,\ hnh = n^{-1}$. Set $G = \langle x, y |\ x^k = y^2 = (xy)^2 = e\rangle$. We have immediately that the map $x \mapsto n,\ y \mapsto h$ determines a surjective homomorphism $G \to D$. Since $|D| = 2k$, we will get an isomorphism as soon as we learn that $|G| \leq 2k$. This isn't too hard to show. Indeed, note that the relation $(xy)^2 = e$ implies that $yx = x^{-1}y$. From this it follows easily that any element of G can be written in the form $x^a y^b$. Furthermore, as $x^k = e = y^2$, we see also that every element of G can be written as $x^a y^b$, where $0 \leq a \leq k-1,\ 0 \leq b \leq 1$. Thus it follows immediately that $|G| \leq 2k$, and we are done.

The general question of calculating the order of a group given by generators and relations is not only difficult, but, in certain instances, can be shown to be impossible. (This is a consequence of the unsolvability of the so-called *word problem* in group theory.) Consider the following fairly simple example: $G = \langle x, y |\ xy = y^2x, yx = x^2y\rangle$. We get

$$y^{-1}xy = y^{-1}y^2x = yx = x^2y = xxy,$$

so that $y^{-1} = x$. But then

$$e = xy = y^2x = y(yx) = y,$$

so $y = e$, implying that $x = e$. In other words, the relations imposed on the generating elements of G are so destructive that the group defined is actually the trivial group.

Exercises 1.8

1. Show that if F is free on the set S via the map $\phi : S \to F$, then

(a) ϕ is injective.

(b) $F = \langle \phi(S) \rangle$.

2. Let $|S| = 1$, and let F be free on S. Prove that $F \cong (\mathbb{Z}, +)$.

3. Let $|S| \geq 2$, and let F be free on S. Prove that F is not abelian.

4. Let F be free on the set S, and let F_0 be the subgroup of F generated by $S_0 \subseteq S$. Prove that F_0 is free on S_0.

5. Prove that $\langle x, y, z |\ yxy^2z^4 = e \rangle$ is a free group. (Hint: it is free on $\{y, z\}$.)

6. Prove that $\langle x, y |\ yx = x^2y, xy^3 = y^2x \rangle = \{e\}$.

7. Prove that $\langle x, y |\ xy^2 = y^3x, x^2y = yx^3 \rangle = \{e\}$.

8. Let G be a free group on a set of more than one element. Prove that G/G' is infinite.

9. Compute the structure of G/G' for each finitely presented group below.

(i) $\langle x, y |\ x^6 = y^4 = e, x^3 = y^2 \rangle$,

(ii) $\langle x, y |\ x^3 = y^2 = e \rangle$,

(iii) $\langle x, y |\ x^2 = y^3 = (xy)^3 = e \rangle$,

(iv) $\langle x, y |\ x^2 = y^3 = (xy)^4 = e \rangle$,

(v) $\langle x, y |\ x^2 = y^3 = (xy)^5 = e \rangle$.

10. Prove that

$$\langle x, y |\ x^4 = e, y^2 = x^2, yxy^{-1} = x^{-1} \rangle \cong \langle r, s, t | r^2 = s^2 = t^2 = rst \rangle.$$

11. Show that $|\langle x, y |\ x^2 = y^3 = (xy)^3 = e \rangle| \leq 12$. Conclude that $A_4 \cong \langle x, y |\ x^2 = y^3 = (xy)^3 = e \rangle$.

12. (a) Show that $|\langle x, y |\ x^2 = y^3 = (xy)^4 = e \rangle| = 24$.

(b) Show that $|\langle x, y |\ x^2 = y^3 = (xy)^5 = e \rangle| = 60$.

13. Let D be the dihedral group of order 6 or 8. Prove that $\mathrm{Aut}(D) \cong D$. Do the same for the *infinite* dihedral group D, with presentation $D = \langle x, y \,|\, x^2 = y^2 = e \rangle$.

14. It is *not* the case that for every dihedral group D, $\mathrm{Aut}(D) \cong D$. Show this. (An easy counterexample to $\mathrm{Aut}(D) \cong D$ is where D is dihedral of order 4. Find other examples.)

15. The *binary dihedral groups*, $\langle 2,2,n\rangle$ are given by the presentation

$$\langle 2,2,n\rangle = \langle a,b,c \mid a^2 = b^2 = c^n = abc\rangle.$$

Show that $\langle a,b,c\rangle$ is finite of order $4n$. Show that $\langle 2,2,2\rangle \cong Q_8$, the quaternion group of order 8.

16. Let k,l,m be positive integers and set

$$D = D(k,l,m) = \langle \alpha,\beta \mid \alpha^k = \beta^l = (\alpha\beta)^m = e\rangle,$$

$$\Delta = \Delta(k,l,m) = \langle a,b,c \mid a^2 = b^2 = c^2 = (ab)^l = (bc)^l = (ac)^m = e\rangle.$$

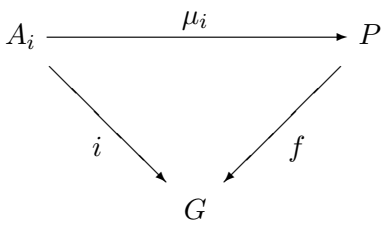
Prove that D is isomorphic with a subgroup of index 2 in Δ.

17. Let $Q_{2^{n+1}}$ be the generalized quaternion group of order 2^{n+1}. Show that $Q_{2^{n+1}}$ has presentation

$$Q_{2^{n+1}} \;=\; \langle x,y \mid x^{2^a} = e, y^4 = x^{2^{a-1}}, yxy^{-1} = x^{-1}\rangle.$$

(Hint: see *Exercise* 11.)

18. *The Free Product of Groups.* Let A_i, $i \in \mathcal{I}$ be a family of groups. A *free product* of the groups A_i, $i \in \mathcal{I}$ is a group P, together with a family of homomorphisms $\mu_i : A_i \to P$, such that if $\theta_i : A_i \to G$ is any family of homomorphisms of the groups A_i into a group G, then there exists a unique homomorphism $f : P \to G$ making the diagram below commute for each $i \in \mathcal{I}$:



Prove that the free product of the groups A_i, $i \in \mathcal{I}$ exists and is unique up to isomorphism. (Hint: the uniqueness is just the usual categorical

nonsense. For the existence, consider this: let $X_i, i \in \mathcal{I}$ be a family of pairwise disjoint sets, with X_i in bijective correspondence with A_i, $i \in \mathcal{I}$, say with bijection $\phi_i : X_i \to A_i$. Now form the free group $F(X)$ on the set $X = \cup_{i\in\mathcal{I}} X_i$. Similarly, for each $i \in \mathcal{I}$, we let $F(X_i)$ be the free group on the set X_i, and set $K_i = \ker F(X_i) \to A_i$, $i \in \mathcal{I}$. Set $K = \langle\langle K_i |\ i \in \mathcal{I}\rangle\rangle$, set $P = F(X)/K$ and define $\mu_i : A_i \to P$ via the composition

$$A_i \xrightarrow{\sim} F(X_i)/K_i \to P,$$

where $F(X_i)/K_i \to P$ is induced by $X_i \hookrightarrow X$. Now prove that P satisfies the necessary universal mapping property. The group P, so constructed, is generally denoted $*_{i\in\mathcal{I}} A_i$. The free product of two groups A and B is denoted $A * B$.)

19. Let $A \cong Z_3$ and let $B \cong Z_2$. Prove that

$$A * B \ \cong\ \langle x, y |\ x^3 = y^2 = e\rangle.$$

(In fact, it turns out that the above group is isomorphic with $\mathrm{PSL}_2(\mathbb{Z})$.)

20. Let S be a set, and define groups indexed by S by setting $A_s = \mathbb{Z}$ (the additive group of the integers) for each $s \in S$. Prove that the free group on S is isomorphic with $*_{s\in S} A_i$.

Chapter 2

Field and Galois Theory

2.1 Basics

We assume that the reader is familiar with the definition of a *field*; typically in these notes a field will be denoted in bold face notation: $\mathbb{F}, \mathbb{K}, \mathbb{E}$, and the like. The reader should also be familiar with the concept of the *characteristic* of a field.

If $\mathbb{F}$ and $\mathbb{K}$ are fields with $\mathbb{F} \subseteq \mathbb{K}$, we say that $\mathbb{K}$ is an *extension* of $\mathbb{F}$. Of fundamental importance here is the observation that if $\mathbb{F} \subseteq \mathbb{K}$ is an extension of fields, then $\mathbb{K}$ can be regarded as a vector space over $\mathbb{F}$. It is customary to call the $\mathbb{F}$-dimension of $\mathbb{K}$ the *degree* of $\mathbb{K}$ over $\mathbb{F}$, and to denote this degree by $[\mathbb{K} : \mathbb{F}]$. The following simple result is fundamental.

PROPOSITION 2.1.1 *Let $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ be an extension of fields. Then $[\mathbb{K} : \mathbb{F}] < \infty$ if and only if each of $[\mathbb{K} : \mathbb{E}]$, $[\mathbb{E} : \mathbb{F}] < \infty$, in which case*

$$[\mathbb{K} : \mathbb{F}] \;=\; [\mathbb{K} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{F}].$$

If $\mathbb{F} \subseteq \mathbb{K}$ is a field extension, and if $\alpha \in \mathbb{K}$, we write $\mathbb{F}(\alpha)$ for the smallest subfield of $\mathbb{K}$ containing $\mathbb{F}$ and α. Similarly, we write $\mathbb{F}[\alpha]$ for the smallest subring of $\mathbb{K}$ containing both $\mathbb{F}$ and α. Clearly,

$$\mathbb{F}(\alpha) \;=\; \left\{ \frac{f(\alpha)}{g(\alpha)} |\; f(x), g(x) \in \mathbb{F}[x],\; g(\alpha) \neq 0 \right\},$$
$$\mathbb{F}[\alpha] \;=\; \{ f(\alpha) |\; f(x) \in \mathbb{F}[x] \}.$$

We say that α is *algebraic* over $\mathbb{F}$ if there is a non-zero polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\alpha) = 0$. When $\mathbb{F} = \mathbb{Q}$, the field of rational numbers, and α is

algebraic over $\mathbb{Q}$, we say that α is an *algebraic number*. If α is algebraic over $\mathbb{F}$, then there is a unique monic polynomial of least degree in $\mathbb{F}[x]$, called the *minimal polynomial of* α, and denoted $m_\alpha(x)$, such that $m_\alpha(\alpha) = 0$. Clearly $m_\alpha(x)$ is irreducible in $\mathbb{F}[x]$. If $\deg m_\alpha(x) = n$, we say that α has *degree* n over $\mathbb{F}$.

The following is frequently useful.

LEMMA 2.1.2 *Let $\mathbb{F} \subseteq \mathbb{K}$, and let $\alpha \in \mathbb{K}$. Then α is algebraic over $\mathbb{F}$ if and only if $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$.*

PROPOSITION 2.1.3 *Let $\mathbb{F} \subseteq \mathbb{K}$ be a field extension, and let $\alpha \in \mathbb{K}$ be algebraic over $\mathbb{F}$, with minimal polynomial $m_\alpha(x)$ of degree n.*

(a) The map $x \mapsto \alpha$ of $\mathbb{F}[x] \to \mathbb{K}$ induces an isomorphism $\mathbb{F}[x]/(m_\alpha(x)) \cong \mathbb{F}(\alpha)$.

(b) $\mathbb{F}(\alpha) = \mathbb{F}[\alpha] = \{f(\alpha) |\ f(x) \in \mathbb{F}[x],$ and $\deg f(x) < n\}$.

(c) $[\mathbb{F}(\alpha) : \mathbb{F}] = n$.

(d) $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an $\mathbb{F}$-basis for $\mathbb{F}(\alpha)$.

In general, if $\mathbb{F} \subseteq \mathbb{K}$ is a field extension, and if $\mathbb{K} = \mathbb{F}(\alpha)$, for some $\alpha \in \mathbb{K}$, we say that $\mathbb{K}$ is a *simple field extension* of $\mathbb{F}$. Thus, a very trivial example is that of $\mathbb{C} \supseteq \mathbb{R}$; since $\mathbb{C} = \mathbb{R}(i)$, we see that $\mathbb{C}$ is a simple field extension of $\mathbb{R}$. We shall see in *Section* 2.10 that any finite extension of a field of characteristic 0 is a simple extension (this is the so-called *Primitive Element Theorem*).

The result of the above proposition can be reversed, as follows. Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$ be an irreducible polynomial. Set $\mathbb{K} = \mathbb{F}[x]/(f(x))$ (*which is a field since $f(x)$ is irreducible*), and regard $\mathbb{F}$ as a subfield of $\mathbb{K}$ via the injection $\mathbb{F} \to \mathbb{K}, a \mapsto a + (f(x)), a \in \mathbb{F}$.

PROPOSITION 2.1.4 *Let $\mathbb{F}, \mathbb{K}$ be as above, and set $\alpha = x + (f(x)) \in \mathbb{K}$. Then α is a root of $f(x)$, and $[\mathbb{K} : \mathbb{F}] = \deg f(x)$.*

The point of the above proposition is, of course, that given any field $\mathbb{F}$, and any polynomial $f(x) \in \mathbb{F}[x]$, we can find a field extension of $\mathbb{F}$ in which $f(x)$ has a root.

By repeated application of *Proposition* 2.1.4, we see that if $f(x) \in \mathbb{F}[x]$ is any polynomial, then there is a field $\mathbb{K} \supseteq \mathbb{F}$ such that $f(x)$ splits completely into linear factors in $\mathbb{K}$. By definition, a *splitting field over* $\mathbb{F}$ for

the polynomial $f(x) \in \mathbb{F}[x]$ is a field extension of $\mathbb{F}$ which is minimal with respect to such a splitting. Thus it is clear that splitting fields exist; indeed, if $\mathbb{K} \supseteq \mathbb{F}$ is such that $f(x)$ splits completely in $\mathbb{K}[x]$, and in $\alpha_1, \alpha_2, \ldots, \alpha_k$ are the distinct roots of $f(x)$ in $\mathbb{K}$, then $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_k) \subseteq \mathbb{K}$ is a splitting field for $f(x)$ over $\mathbb{F}$. In particular, we see that the degree of a splitting field for $f(x)$ over $\mathbb{F}$ has degree at most $n!$ over $\mathbb{F}$, where $n = \deg f(x)$. In the next section we will investigate the uniqueness of splitting fields.

The next result is easy.

PROPOSITION 2.1.5 *If $\mathbb{F}$ is a field, and if $f(x)$ is a polynomial $\mathbb{F}[x]$ of degree n, then $f(x)$ can have at most n distinct roots in $\mathbb{F}$.*

From the above, one can immediately deduce the following interesting consequence.

COROLLARY 2.1.5.1 *Let $Z \leq \mathbb{F}^\times$ be a finite subgroup of the multiplicative group of the field $\mathbb{F}$. Then Z is cyclic.*

EXERCISES 2.1

1. Compute the minimal polynomials over $\mathbb{Q}$ of the following complex numbers.
   (a) $\sqrt{2} + \sqrt{3}$.
   (b) $\sqrt{2} + \zeta$, where $\zeta = e^{2\pi i/3}$.
2. Let $\mathbb{F} \subseteq \mathbb{K}$ be a field extension with $[\mathbb{K} : \mathbb{F}]$ odd. If $\alpha \in \mathbb{K}$, prove that $\mathbb{F}(\alpha^2) = \mathbb{F}(\alpha)$.
3. Assume that $\alpha = a + bi \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, where a is rational and b is real. Prove that $m_\alpha(x)$ has even degree.
4. Let $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) \subseteq \mathbb{C}$. Compute $[\mathbb{K} : \mathbb{Q}]$.
5. Let $\mathbb{K} = \mathbb{Q}(\sqrt[4]{2}, i) \subseteq \mathbb{C}$. Show that
   (a) $\mathbb{K}$ contains all roots of $x^4 - 2 \in \mathbb{Q}[x]$.
   (b) Compute $[\mathbb{K} : \mathbb{Q}]$.

6. Let $\mathbb{F} = \mathbb{C}(x)$, where $\mathbb{C}$ is the complex number field and x is an indeterminate. Assume that $\mathbb{F} \subseteq \mathbb{K}$ and that $\mathbb{K}$ contains an element y such that $y^2 = x(x-1)$. Prove that there exists an element $z \in \mathbb{F}(y)$ such that $\mathbb{F}(y) = \mathbb{C}(z)$, i.e., $\mathbb{F}(y)$ is a "simple transcendental extension" of $\mathbb{C}$.

7. Let $\mathbb{F} \subseteq \mathbb{K}$ be a field extension. If the subfields of $\mathbb{K}$ containing $\mathbb{F}$ are totally ordered by inclusion, prove that $\mathbb{K}$ is a simple extension of $\mathbb{F}$. (Is the converse true?)

8. Let $\mathbb{Q} \subseteq \mathbb{K}$ be a field extension. Assume that $\mathbb{K}$ is closed under taking square roots, i.e., if $\alpha \in \mathbb{K}$, then $\sqrt{\alpha} \in \mathbb{K}$. Prove that $[\mathbb{K} : \mathbb{Q}] = \infty$. (Compare with *Exercise* 5, *Section* 2.10.)

9. Let $\mathbb{F}$ be a field, contained as a subring of the integral domain R. If every element of R is algebraic over $\mathbb{F}$, show that R is actually a field. Give an example of a non-integral domain R containing a field $\mathbb{F}$ such that every element of R is algebraic over $\mathbb{F}$. Obviously, R cannot be a field.

10. Let $\mathbb{F} \subseteq \mathbb{K}$ be fields and let $f(x),\ g(x) \in \mathbb{F}[x]$ with $f(x)|g(x)$ in $\mathbb{K}[x]$. Prove that $f(x)|g(x)$ in $\mathbb{F}[x]$.

11. Let $\mathbb{F} \subseteq \mathbb{K}$ be fields and let $f(x),\ g(x) \in \mathbb{F}[x]$. If $d(x)$ is the greatest common denominator of $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, prove that $d(x)$ is the greatest common denominator of $f(x)$ and $g(x)$ in $\mathbb{K}[x]$.

12. Let $\mathbb{F} \subseteq \mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{E}$ be fields. Define $\mathbb{E}_1\mathbb{E}_2 \subseteq \mathbb{E}$ to be the smallest field containing both $\mathbb{E}_1$ and $\mathbb{E}_2$. $\mathbb{E}_1\mathbb{E}_2$ is called the *composite* (or *compositum*) of the fields $\mathbb{E}_1$ and $\mathbb{E}_2$. Prove that if $[\mathbb{E} : \mathbb{F}] < \infty$, then $[\mathbb{E}_1\mathbb{E}_2 : \mathbb{F}] \leq [\mathbb{E}_1 : \mathbb{F}] \cdot [\mathbb{E}_2 : \mathbb{F}]$.

13. Given a complex number α it can be quite difficult to determine whether α is algebraic or transcendental. It was known already in the nineteenth century that π and e are transcendental, but the fact that such numbers as e^π and $2^{\sqrt{2}}$ are transcendental is more recent, and follows from the following deep theorem of Gelfond and Schneider: *Let α and β be algebraic numbers. If*

$$\eta = \frac{\log \alpha}{\log \beta}$$

is irrational, then η is transcendental. (See E. Hille, American Mathematical Monthly, vol. 49(1042), pp. 654-661.) Using this result, prove that $2^{\sqrt{2}}$ and e^{π} are both transcendental. (For $2^{\sqrt{2}}$, set $\alpha = 2^{\sqrt{2}}$, $\beta = 2$.)

2.2 Splitting Fields and Algebraic Closure

Let $\mathbb{F}_1$, $\mathbb{F}_2$ be fields, and assume that $\psi : \mathbb{F}_1 \to \mathbb{F}_2$ is a field homomorphism. Define the homomorphism $\hat{\psi} : \mathbb{F}_1[x] \to \mathbb{F}_2[x]$ simply by applying ψ to the coefficients of polynomials in $\mathbb{F}_1[x]$. We have the following two results.

PROPOSITION 2.2.1 *Let $\mathbb{F}_1$ be a field and let $\mathbb{K}_1 = \mathbb{F}_1(\alpha_1)$, where α_1 is algebraic over $\mathbb{F}_1$, with minimal polynomial $f_1(x) \in \mathbb{F}_1[x]$. Suppose we have*

$$\psi : \mathbb{F}_1 \xrightarrow{\cong} \mathbb{F}_2,$$

$$\hat{\psi} : \mathbb{F}_1[x] \xrightarrow{\cong} \mathbb{F}_2[x],$$

where $\hat{\psi}$ is defined as above. Let $\mathbb{K}_2 = \mathbb{F}_2(\alpha_2) \supseteq \mathbb{F}_2$, where α_2 is a root of $f_2(x) = \hat{\psi}(f_1(x))$. Then there exists an isomorphism

$$\bar{\psi} : \mathbb{K}_1 \xrightarrow{\cong} \mathbb{K}_2,$$

such that $\bar{\psi}(\alpha_1) = \alpha_2$, and $\bar{\psi}|_{\mathbb{F}_1} = \psi$.

PROPOSITION 2.2.2 *Let $\mathbb{F}_1$ be a field, let $f_1(x) \in \mathbb{F}_1[x]$, and let $\mathbb{K}_1$ be a splitting field over $\mathbb{F}_1$ for $f_1(x)$. Let*

$$\psi : \mathbb{F}_1 \xrightarrow{\cong} \mathbb{F}_2,$$

let $f_2(x) = \hat{\psi}(f_1(x)) \in \mathbb{F}_2[x]$, and let $\mathbb{K}_2$ be a splitting field over $\mathbb{F}_2$ for $f_2(x)$. Then there is a commutative diagram

$$\begin{array}{ccc} \mathbb{K}_1 & \xrightarrow{\bar{\psi}} & \mathbb{K}_2 \\ \uparrow & & \uparrow \\ \mathbb{F}_1 & \xrightarrow{\psi} & \mathbb{K}_2 \end{array}$$

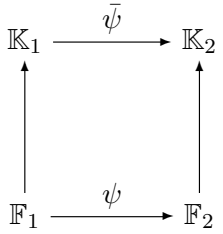
where the vertical maps are inclusions, and where $\bar{\psi}$ is an isomorphism.

Let $\mathbb{F}$ be a field and let $\mathcal{F} \subseteq \mathbb{F}[x]$. By a *splitting field* for $\mathcal{F}$ we mean a field extension $\mathbb{K} \supseteq \mathbb{F}$ such that every polynomial in $\mathcal{F}$ splits completely in $\mathbb{K}$, and $\mathbb{K}$ is minimal in this respect.

PROPOSITION 2.2.3 *Let $\mathbb{F}_1$ be a field, let $\mathcal{F}_1 \subseteq \mathbb{F}_1[x]$, and let $\mathbb{K}_1$ be a splitting field over $\mathbb{F}_1$ for $\mathcal{F}_1$. Let*

$$\psi : \mathbb{F}_1 \xrightarrow{\cong} \mathbb{F}_2,$$

let $\mathcal{F}_2 = \hat{\psi}(\mathcal{F}_1) \subseteq \mathbb{F}_2[x]$, and let $\mathbb{K}_2$ be a splitting field a over $\mathbb{F}_2$ for $\mathcal{F}_2$. Then there is commutative diagram



where the vertical maps are the obvious inclusions, and where $\bar{\psi}$ is an isomorphism.

COROLLARY 2.2.3.1 *Let $\mathbb{F}$ be a field and let $\mathcal{F} \subseteq \mathbb{F}[x]$. Then any splitting field for $\mathcal{F}$ over $\mathbb{F}$ is unique, up to an isomorphism fixing $\mathbb{F}$ element-wise.*

If $\mathcal{F} = \mathbb{F}[x]$, then a splitting field for $\mathcal{F}$ over $\mathbb{F}$ is called an *algebraic closure* of $\mathbb{F}$. Furthermore, if every polynomial $f(x) \in \mathbb{F}[x]$ splits completely in $\mathbb{F}[x]$, we call $\mathbb{F}$ *algebraically closed* .

LEMMA 2.2.4 *Let $\bar{\mathbb{F}} \supseteq \mathbb{F}$ be an algebraic closure. Then $\bar{\mathbb{F}}$ is algebraically closed.*

THEOREM 2.2.5 *Let $\mathbb{F}$ be a field. Then there exists an algebraic closure of $\mathbb{F}$.*

The idea of the proof of the above is first to construct a "very large" algebraically closed field $\mathbb{E} \supseteq \mathbb{F}$ and then let $\bar{\mathbb{F}}$ be the subfield of $\mathbb{F}$ generated by the roots of all polynomials $f(x) \in \mathbb{F}$.

Note that the algebraic closure of the field $\mathbb{F}$, whose existence is guaranteed by the above theorem, is essentially unique (in the sense of *Corollary* 10, above).

EXERCISES 2.2

1. Let $f(x) = x^n - 1 \in \mathbb{Q}[x]$. In each case below, construct a splitting field $\mathbb{K}$ over $\mathbb{Q}$ for $f(x)$, and compute $[\mathbb{K} : \mathbb{Q}]$.

   (i) $n = p$, a prime.

   (ii) $n = 6$.

   (iii) $n = 12$.

   Any conjectures? We'll discuss this problem in *Section* 8.

2. Let $f(x) = x^n - 2 \in \mathbb{Q}[x]$. Construct a splitting field for $f(x)$ over $\mathbb{Q}$. (Compare with *Exercise* 5 of *Section* 2.1.)

3. Let $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$.

   (a) Prove that $f(x)$ is irreducible.

   (b) Prove that if $\alpha \in \mathbb{C}$ is a root of $f(x)$, so is $\alpha^2 - 2$.

   (c) Let $\mathbb{K} \supseteq \mathbb{Q}$ be a splitting field over $\mathbb{Q}$ for $f(x)$. Using part (b), compute $[\mathbb{K} : \mathbb{Q}]$.

4. Let $\zeta = e^{2\pi i/7} \in \mathbb{C}$, and let $\alpha = \zeta + \zeta^{-1}$. Show that $m_\alpha(x) = x^3 + x^2 - 2x - 1$ (as in *Exercise* 3 above), and that $\alpha^2 - 2 = \zeta^2 + \zeta^{-2}$.

5. If $\zeta = e^{2\pi i/11}$ and $\alpha = \zeta + \zeta^{-1}$, compute $m_\alpha(x) \in \mathbb{Q}[x]$.

6. Let $\mathbb{K} \subseteq \mathbb{F}$ be a splitting field for some set $\mathcal{F}$ of polynomials in $\mathbb{F}[x]$. Prove that $\mathbb{K}$ is algebraic over $\mathbb{F}$.

2.3 Galois Extensions, Galois Groups and the Fundamental Theorem of Galois Theory

We begin with the following observation. Let $\mathbb{K}$ be a field, let S be a set, and let $\mathbb{K}^S$ be the set of mappings $S \to \mathbb{K}$. We may give $\mathbb{K}^S$ a $\mathbb{K}$-vector space structure by pointwise operations.

In terms of the above, we state the following important result.

LEMMA 2.3.1 *[Dedekind Independence Lemma]*

(i) Let $\mathbb{E}, \mathbb{K}$ be fields, and let $\sigma_1, \sigma_2, \cdots, \sigma_r$ be distinct monomorphisms $\mathbb{E} \to \mathbb{K}$. Then $\sigma_1, \sigma_2, \cdots, \sigma_r$ are $\mathbb{K}$-linearly independent in $\mathbb{K}^{\mathbb{E}}$.

(ii) Let $\mathbb{E}$ be a field, and let G be a group of automorphisms of $\mathbb{E}$. We may regard each $x \in \mathbb{E}$ as an element of $\mathbb{E}^G$ via $\sigma \mapsto \sigma(x) \in \mathbb{E}$, $\sigma \in G$. Now set $\mathbb{K} = inv_G(\mathbb{E})$ and assume that we are given $\mathbb{K}$-linearly independent elements $x_1, x_2, \cdots, x_r \in \mathbb{E}$. Then $x_1, x_2, \cdots, x_r$ are $\mathbb{E}$-linearly independent elements of $\mathbb{E}^G$.

If $\mathbb{F} \subseteq \mathbb{K}$ is a field extension, we set $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \{\text{automorphisms } \sigma : \mathbb{K} \to \mathbb{K} |\ \sigma|_{\mathbb{F}} = 1_{\mathbb{F}}\}$. We call $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ the *Galois group* of $\mathbb{K}$ *over* $\mathbb{F}$. Note that if $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is a subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$. For the next couple of results we assume a fixed extension $\mathbb{E} \supseteq \mathbb{F}$, with Galois group $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

PROPOSITION 2.3.2 *Assume that $\mathbb{E} \supseteq \mathbb{E}_1 \supseteq \mathbb{E}_2 \supseteq \mathbb{F}$, and set $H_1 = Gal(\mathbb{E}/\mathbb{E}_1)$, $H_2 = Gal(\mathbb{E}/\mathbb{E}_2)$. If $[\mathbb{E}_1 : \mathbb{E}_2] < \infty$, then*

$$[H_2 : H_1] \leq [\mathbb{E}_1 : \mathbb{E}_2].$$

PROPOSITION 2.3.3 *Let $\mathbb{E} \supseteq \mathbb{F}$, and set $G = Gal(\mathbb{E}/\mathbb{F})$. Assume that $1 \leq H_1 \leq H_2 \leq G$, and let $\mathbb{E}_1 = inv_{H_1}(\mathbb{E})$, $\mathbb{E}_2 = inv_{H_2}(\mathbb{E})$. If $[H_2 : H_1] < \infty$, then*

$$[\mathbb{E}_1 : \mathbb{E}_2] \leq [H_2 : H_1].$$

COROLLARY 2.3.3.1 *Let $\mathbb{E} \supseteq \mathbb{F}$ be a field extension, let $G = Gal(\mathbb{E}/\mathbb{F})$, and let $\mathbb{F}_0 = inv_G(\mathbb{E})$.*

(i) If $[\mathbb{E} : \mathbb{F}_0] < \infty$, then $|G| < \infty$ and $[\mathbb{E} : \mathbb{F}_0] = |G|$.

(ii) If $|G| < \infty$, then $[\mathbb{E} : \mathbb{F}_0] < \infty$ and $[\mathbb{E} : \mathbb{F}_0] = |G|$.

Next set

$$\Omega_{\mathbb{E}/\mathbb{F}} = \{\text{subfields } \mathbb{K} |\ \mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}\},$$

$$\Omega_G = \{\text{subgroups } H \leq G\}.$$

We have the maps

$$\mathrm{Gal}(\mathbb{E}/\bullet) : \Omega_{\mathbb{E}/\mathbb{F}} \longrightarrow \Omega_G,$$

$$\mathrm{inv}_\bullet(\mathbb{E}) : \Omega_G \longrightarrow \Omega_{\mathbb{E}/\mathbb{F}}.$$

Note that *Propositions* 14 and 15 say that $\mathrm{Gal}(\mathbb{E}/\bullet)$ and $\mathrm{inv}_\bullet(\mathbb{E})$ are "contractions" relative to $[\cdot\ ,\cdot]$.

We now define two concepts of "closure."

(i) If $\mathbb{K} \in \Omega_{\mathbb{E}/\mathbb{F}}$, set

$$cl_{\mathbb{E}}(\mathbb{K}) = \mathrm{inv}_{\mathrm{Gal}(\mathbb{E}/\mathbb{K})}(\mathbb{E}),$$

the *closure* of $\mathbb{K}$ in $\mathbb{E}$. If $\mathbb{K} = cl_{\mathbb{E}}(\mathbb{K})$, say that $\mathbb{K}$ is *closed* in $\mathbb{E}$.

(ii) If $H \leq G$, set

$$cl_G(H) = \mathrm{Gal}(\mathbb{E}/\mathrm{inv}_H(\mathbb{E})),$$

the *closure* of H in G. If $H = cl_G(H)$, say that H is *closed* in G.

Corollary 2.3.3.2

(i) Let $\mathbb{E} \supseteq \mathbb{E}_1 \supseteq \mathbb{E}_2 \supseteq \mathbb{F}$, and assume that $[\mathbb{E}_1 : \mathbb{E}_2] < \infty$ and that $\mathbb{E}_2$ is closed in $\mathbb{E}$. Then $\mathbb{E}_1$ is closed in $\mathbb{E}$.

(ii) Let $\{e\} \leq H_1 \leq H_2 \leq G$ and assume that $[H_2 : H_1] < \infty$ and that H_1 is closed in G. Then H_2 is closed in G.

Theorem 2.3.4 *Let $\mathbb{E} \supseteq \mathbb{F}$ be an algebraic extension with $\mathbb{F}$ closed in $\mathbb{E}$. Then every element of $\Omega_{\mathbb{E}/\mathbb{F}}$ is closed in $\mathbb{E}$.*

The field extension $\mathbb{E} \supseteq \mathbb{F}$ is called a *Galois* extension (we sometimes say that $\mathbb{E}$ is *Galois* over $\mathbb{F}$) if $\mathbb{F}$ is closed in $\mathbb{E}$. Let $\mathbb{E} \supseteq \mathbb{F}$ be a field extension with Galois group G, and let $\mathbb{K} \in \Omega_{\mathbb{E}/\mathbb{F}}$. We say that $\mathbb{K}$ is *stable* if $\sigma\mathbb{K} = \mathbb{K}$ for each $\sigma \in G$. We denote by Ω_G^c the *closed* subgroups of G.

Theorem 2.3.5 (Fundamental Theorem of Galois Theory) *Let $\mathbb{E} \supseteq \mathbb{F}$ be an algebraic Galois extension.*

(i) The mappings

$$Gal(\mathbb{E}/\bullet) : \Omega_{\mathbb{E}/\mathbb{F}} \to \Omega_G^c, \quad inv_\bullet : \Omega_G^c \to \Omega_{\mathbb{E}/\mathbb{F}}$$

are inverse isomorphisms.

(ii) Let $\mathbb{K} \in \Omega_{\mathbb{E}/\mathbb{F}}$ correspond to the closed subgroup $H \leq G$ under the above correspondence. Then $\mathbb{K}$ is stable in $\mathbb{E}$ if and only if $H \lhd G$. In this case, $\mathbb{K}$ is Galois over $\mathbb{F}$ and

$$Gal(\mathbb{K}/\mathbb{F}) \cong G/H.$$

The next result, the so-called "Theorem on Natural Irrationalities," is frequently useful in computations.

THEOREM 2.3.6 *Assume that we have an extension of fields $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$, where $\mathbb{E}$ is a Galois extension of $\mathbb{F}$. Assume that also $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$, and that $\mathbb{K}$ is the composite $\mathbb{EL}$. then $\mathbb{K}$ is a Galois extension of $\mathbb{L}$ and $Gal(\mathbb{K}/\mathbb{L}) \cong Gal(\mathbb{E}/\mathbb{E} \cap \mathbb{L})$.*

EXERCISES 2.3

1. Let $\mathbb{F} \subseteq \mathbb{K}$ be a finite Galois extension. Either prove the following statements, or give counterexample(s).
   (a) Any automorphism of $\mathbb{F}$ extends to an automorphism of $\mathbb{K}$.
   (b) Any automrophism of $\mathbb{K}$ restricts to an automomrphism of $\mathbb{F}$.
2. Recall the "Galois correspondence:"

$$\Gamma = \mathrm{Gal}(\mathbb{E}/\bullet) : \Omega_{\mathbb{E}/\mathbb{F}} \longrightarrow \Omega_G,$$
$$\iota = \mathrm{inv}_\bullet(\mathbb{E}) : \Omega_G \longrightarrow \Omega_{\mathbb{E}/\mathbb{F}}.$$

   Prove that $\Gamma \circ \iota \circ \Gamma = \Gamma$, and that $\iota \circ \Gamma \circ \iota = \iota$. Thus images under either map are always closed.
3. Let $\alpha = \sqrt[4]{2} \in \mathbb{R}$, and set $\mathbb{K} = \mathbb{Q}(\alpha)$. Compute the closure of $\mathbb{Q}$ in $\mathbb{K}$.

4. As in *Exercise* 3 of *Section* 2.2, let $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$, and let $\alpha \in \mathbb{C}$ be a root of $f(x)$. Compute the closure of $\mathbb{Q}$ in $\mathbb{Q}(\alpha)$.

5. If $\mathbb{E} \supseteq \mathbb{F}$ is a finite Galois extension, prove that every subgroup of $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is closed.

6. Let $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$ with $\mathbb{E} \supseteq \mathbb{F}$ algebraic. If $\mathbb{E}$ is Galois over $\mathbb{K}$ and $\mathbb{K}$ is Galois over $\mathbb{F}$, must it be true that $\mathbb{E}$ is Galois over $\mathbb{F}$?

7. Let $\mathbb{F} \subseteq \mathbb{E}$ be an extension of fields, with $\mathbb{E}$ an algebraically closed field. Assume that $\mathbb{F} \subseteq \mathbb{K}_1, \mathbb{K}_2 \subseteq \mathbb{E}$ are subfields, both algebraic and Galois over $\mathbb{F}$. If $\mathbb{K}_1$ and $\mathbb{K}_2$ are $\mathbb{F}$-isomorphic, then they are equal. Show that the result need not be true if $\mathbb{K}_1$ and $\mathbb{K}_2$ are not Galois over $\mathbb{F}$.

8. Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$ be an extension of fields with both $\mathbb{E}$ and $\mathbb{K}$ Galois over $\mathbb{F}$. Let $\alpha \in \mathbb{E}$, with minimal polynomial $m_\alpha(x) \in \mathbb{F}[x]$. If $m_\alpha(x) = f_1(x)f_2(x)\cdots f_r(x)$ is the prime factorization of $m_\alpha(x)$ in $\mathbb{K}[x]$, prove that $f_i(x) \neq f_j(x)$ when $i \neq j$, and that $\deg f_i(x) = \deg f_j(x)$ for all i, j.

9. Let $p_1, p_2, \ldots p_k$ be distinct prime numbers, and let $\mathbb{E} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k})$. Show that $\mathbb{E}$ is a Galois extension of $\mathbb{Q}$, whose Galois group is an elementary abelian group of order 2^k. (Hint: For each non-empty subset $M \subseteq \{1, 2, \ldots, k\}$, form the integer $q_M = \prod_{i \in M} p_i$. Thus the field $\mathbb{K}_M = \mathbb{Q}(\sqrt{q_M})$ is a subfield of $\mathbb{E}$; prove that if $M_1 \neq M_2$ then $\mathbb{K}_{M_1} \neq \mathbb{K}_{M_2}$. Since there are $2^k - 1$ nonempty subsets of $\{1, 2, \ldots, k\}$, one can apply *Exercise* 22 of *Section* 1.7.)

10. Retain the notation and assumptions of the above exercise. Prove that

$$\mathbb{Q}(\sqrt{p_1} + \sqrt{p_2} + \ldots + \sqrt{p_k}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}).$$

11. (The Galois group of a simple transcendental extension.) Let $\mathbb{F}$ be a field and let x be indeterminate over $\mathbb{F}$. Set $\mathbb{E} = \mathbb{F}(x)$, a simple transcendental extension of $\mathbb{F}$.

    (i) Let $\alpha \in \mathbb{E}$; thus $\alpha = f(x)/g(x)$, where $f(x), g(x) \in \mathbb{F}[x]$, and where $f(x)$ and $g(x)$ have no common factors. Write

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

where $a_n \neq 0$, or $b_n \neq 0$. Therefore, $n = \max\{\deg f(x), \deg g(x)\}$. Note that

$$(a_n - \alpha b_n)x^n + (a_{n-1} - \alpha b_{n-1})x^{n-1} + \cdots + (a_0 - \alpha b_0) = 0.$$

If we set

$$F(X) = \sum_{i=0}^{n}(a_i - \alpha b_i)X^i \in \mathbb{F}(\alpha)[X],$$

then x is a root of $F(X)$. Show that $F(X)$ is irreducible in $\mathbb{F}(\alpha)[X]$. (Hint: By Gauss' Lemma, $F(X)$ is irreducible in $\mathbb{F}(\alpha)[X]$ if and only if $F(X)$ is irreducible in $\mathbb{F}[\alpha][X] = \mathbb{F}[\alpha, X]$. However,

$$F(X) = F(\alpha, X) = f(X) - \alpha g(X)$$

which is linear in α. Therefore, the only factors of $F(\alpha, X)$ are common factors of $f(X)$ and $g(X)$; there are no nontrivial common factors.)

(ii) From part (i), we see that $[\mathbb{F}(x) : \mathbb{F}(\alpha)] = n$. This implies that any automorphism of $\mathbb{F}(x)$ must carry x to $f(x)/g(x)$ where one of $f(x)$ or $g(x)$ is linear, the other has degree less than or equal to 1, and where $f(x)$ and $g(x)$ have no common non-trivial factors:

$$x \mapsto \frac{a + bx}{c + dx}, \quad ad - bc \neq 0.$$

Conversely, any such choice of a, b, c, d determines an automorphism of $\mathbb{F}(x)$. Therefore, we get a surjective homomorphism

$$\mathrm{GL}_2(\mathbb{F}) \longrightarrow \mathrm{Gal}(\mathbb{F}(x)/\mathbb{F}).$$

Note that the kernel of the above homomorphism is clearly $Z(\mathrm{GL}_2(\mathbb{F}))$, the set of scalar matrices in $\mathrm{GL}_2(\mathbb{F})$. In other words,

$$\mathrm{Gal}(\mathbb{F}(x)/\mathbb{F}) \cong \mathrm{PGL}_2(\mathbb{F}).$$

12. Let $\mathbb{F} = \mathbb{F}_2$, the field of 2 elements, and let x be indeterminate over $\mathbb{F}$. From the above exercise, we know that $\mathrm{Gal}(\mathbb{F}(x)/\mathbb{F}) \cong \mathrm{PGL}_2(2) \cong \mathrm{GL}_2(2) \cong S_3$, a group of 6 elements. For each subgroup $H \leq G = \mathrm{Gal}(\mathbb{F}(x)/\mathbb{F})$, compute $\mathrm{inv}_H(\mathbb{F}(x))$. From this, compute the closure of $\mathbb{F}$ in $\mathbb{F}(x)$. (Hint: This takes a bit of work. For example, if $\sigma \in G$ is the involution given by $x \mapsto 1/x$, then one sees that $\mathrm{inv}_H(\mathbb{F}(x)) = \mathbb{F}(x + 1/x)$, where $H = \langle\sigma\rangle$. In turns out that $\mathrm{inv}_G(\mathbb{F}(x)) = \mathbb{F}(\frac{(x^3+x+1)(x^3+x^2+1)}{x^2(x^2+1)})$.)

2.4 Separability and the Galois Criterion

Let $f(x) \in \mathbb{F}[x]$ be an irreducible polynomial. We say that $f(x)$ is *separable* if $f(x)$ has no repeated roots in a splitting field. In general, a polynomial (not necessarily irreducible) is called *separable* if each is its irreducible factors is separable.

Next, if $\mathbb{F} \subseteq \mathbb{K}$ is a field extension, and if $\alpha \in \mathbb{K}$, we say that α is *separable* over $\mathbb{F}$ if α is algebraic over $\mathbb{F}$, and if $m_{\alpha,\mathbb{F}}(x)$ is a separable polynomial. Finally we say that the extension $\mathbb{F} \subseteq \mathbb{K}$ is a *separable extension* $\mathbb{K}$ is algebraic over $\mathbb{F}$ and if every element of $\mathbb{K}$ is separable over $\mathbb{F}$.

The following two results relate algebraic Galois extensions and separable extensions:

THEOREM 2.4.1 *Let $\mathbb{F} \subseteq \mathbb{K}$ be an algebraic extension of fields. Then $\mathbb{K}$ is Galois over $\mathbb{F}$ if and only if $\mathbb{K}$ is the splitting field over $\mathbb{F}$ for some set of separable polynomials in $\mathbb{F}[x]$.*

COROLLARY 2.4.1.1 *Let $\mathbb{K} \supseteq \mathbb{F}$ be generated over $\mathbb{F}$ by a set of separable elements. Then $\mathbb{K}$ is a separable extension of $\mathbb{F}$.*

PROPOSITION 2.4.2 *Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$ be an algebraic extension with $\mathbb{K}$ separable over $\mathbb{F}$. If $\alpha \in \mathbb{E}$ is separable over $\mathbb{K}$, then α is separable over $\mathbb{F}$.*

If $\mathbb{F} \subseteq \mathbb{E}$ is an algebraic extension of fields such that no element of $\mathbb{E} - \mathbb{F}$ is separable over $\mathbb{F}$, then we say that $\mathbb{E}$ is a *purely inseparable* extension of $\mathbb{F}$. If $\alpha \in \mathbb{E}$ is such that $\mathbb{F}(\alpha)$ is a purely inseparable extension of $\mathbb{F}$, we say that α is a *purely inseparable element* over $\mathbb{F}$.

THEOREM 2.4.3 *Let $\mathbb{F} \subseteq \mathbb{E}$ be an algebraic extension. Then there exists a unique maximal subfield $\mathbb{E}_{sep} \subseteq \mathbb{E}$ such that $\mathbb{E}_{sep}$ is separable over $\mathbb{F}$ and $\mathbb{E}$ is purely inseparable over $\mathbb{E}_{sep}$.*

Given $f(x) = \sum a_i x^i \in \mathbb{F}[x]$, we may define its (formal) derivative by setting $f'(x) = \sum i a_i x^{i-1}$. One has the usual product rule: $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$.

The following is quite simple.

LEMMA 2.4.4 *Let $f(x) \in \mathbb{F}[x]$.*

(i) If g.c.d.$(f(x), f'(x)) = 1$, then $f(x)$ has no repeated roots in any splitting field. (Note: this is stronger than being separable.)

(ii) If $f(x)$ is irreducible, then $f(x)$ is separable if and only if $f'(x) \neq 0$.

(iii) If $\mathbb{F}$ has characteristic $p > 0$, and if $f(x) \in \mathbb{F}[x]$ is irreducible but not separable, then $f(x) = g(x^p)$ for some irreducible $g(x) \in \mathbb{F}[x]$.

Obviously, it follows that if char $\mathbb{F} = 0$ then every polynomial $f(x) \in \mathbb{F}[x]$ is separable.

LEMMA 2.4.5 *Let $\mathbb{F} \subseteq \mathbb{K}$ be an algebraic extension of fields where $\mathbb{F}$ has characteristic $p > 0$. If $\alpha \in \mathbb{K}$, then α is separable over $\mathbb{F}$ if and only if $\mathbb{F}(\alpha) = \mathbb{F}(\alpha^p)$.*

PROPOSITION 2.4.6 *Let $\mathbb{F} \subseteq \mathbb{K}$ be an algebraic extension, where $\mathbb{F}$ is a field of characteristic $p > 0$. Let $\alpha \in \mathbb{K}$ be an inseparable element over $\mathbb{F}$. The following are equivalent:*

(i) α is purely inseparable over $\mathbb{F}$.

(ii) The minimal polynomial has the form $m_\alpha(x) = x^{p^e} - a \in \mathbb{F}[x]$, for some positive integer e and for some $a \in \mathbb{F}$.

(iii) The minimal polynomial $m_\alpha(x) \in \mathbb{F}[x]$ has a unique root in any splitting field, viz., α.

Let $\mathbb{F}$ be a field of characteristic $p > 0$. We may define the p-th power map $(\cdot)^p : \mathbb{F} \to \mathbb{F}$, $\alpha \mapsto \alpha^p$. Clearly $(\cdot)^p$ is a monomorphism of $\mathbb{F}$ into itself. We say that the field $\mathbb{F}$ is *perfect* if one of the following holds:

(i) $\mathbb{F}$ has characteristic 0, or

(ii) $\mathbb{F}$ has characteristic $p > 0$ and
$(\cdot)^p : \mathbb{F} \to \mathbb{F}$ is an automorphism of $\mathbb{F}$.

COROLLARY 2.4.6.1 *Let $\mathbb{F}$ be a perfect field. Then any algebraic extension of $\mathbb{F}$ is a separable extension.*

We can apply the above discussion to extensions of finite fields. Note first that if $\mathbb{F}$ is a finite field, it obviously has positive characteristic, say p. Thus $\mathbb{F}$ is a finite dimensional vector space over the field $\mathbb{F}_p$ (alternatively

denoted $\mathbb{Z}/(p)$, the integers, modulo p). From this it follows immediately that if n is the dimension of $\mathbb{F}$ over $\mathbb{F}_p$, then $|\mathbb{F}| = p^n$. Note furthermore that by *Corollary* 2.1.5.1 of *Section* 2.1, $\mathbb{F}^\times$ is a cyclic group, and so the elements of $\mathbb{F}$ are precisely the roots of $x^q - x$, where $q = p^n$. In other words,

$\mathbb{F}$ is a splitting field over $\mathbb{F}_p$ for the polynomial $x^q - x$. From this we infer immediately the following.

PROPOSITION 2.4.7 *Two finite fields $\mathbb{F}_1$ and $\mathbb{F}_2$ are isomorphic if and only if they have the same order.*

The only issue left unsettled by the above is whether for any prime p and any integer n, there really exists a finite field of order p^n. The answer is yes, and is very easily demonstrated. Indeed, let $q = p^n$, and let $f(x) = x^q - x \in \mathbb{F}_p[x]$. By *Lemma* 2.4.4, part (i) $f(x)$ is separable. Thus if $\mathbb{F} \supseteq \mathbb{F}_p$ is a splitting field, then it's easy to see that $\mathbb{F}$ consists wholly of the q roots of $f(x)$. Thus:

PROPOSITION 2.4.8 *For any prime p, and any integer n, there exists a field of order p^n.*

Thus, for any prime power $q = p^n$ there exists a unique (up to isomorphism) field of order q. We denote such a field simply by $\mathbb{F}_q$.

Finally, we'll say a few words about Galois groups in this setting. Let $\mathbb{F} = \mathbb{F}_q$ be the finite field of order q, and let $\mathbb{K} = \mathbb{F}_{q^n}$ be an extension of degree n. Since $\mathbb{K}$ is the splitting field over $\mathbb{F}$ for the separable polynomial $x^{q^n} - x$, we conclude that $\mathbb{K}$ is a Galois extension of $\mathbb{F}$.

Define the map

$$F : \mathbb{K} \longrightarrow \mathbb{K},$$

$$\alpha \longmapsto \alpha^q.$$

Then F is easily seen to be an $\mathbb{F}$-automorphism of $\mathbb{K}$, often called the *Frobenius automorphism* of $\mathbb{K}$. The following is easy to prove.

THEOREM 2.4.9 *In the notation above, Gal($\mathbb{K}/\mathbb{F}$) is cyclic of order n and is generated by the Frobenius automorphism F.*

EXERCISES 2.4

1. Let $\mathbb{F} \subseteq \mathbb{E}$ be an algebraic Galois extension and let $f(x) \in \mathbb{F}[x]$ be a separable polynomial. Let $\mathbb{K} \supseteq \mathbb{E}$ be the splitting field for $f(x)$ over $\mathbb{E}$. Prove that $\mathbb{K}$ is Galois over $\mathbb{F}$.

2. Let $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$, and let $\mathbb{K} \supseteq \mathbb{Q}$ be a splitting field for $f(x)$ over $\mathbb{Q}$ (cf. *Exercise* 3 of *Section* 2.2). Compute $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$.

3. Let $\mathbb{K} = \mathbb{Q}(\sqrt{2+\sqrt{2}})$

   (a) Show that $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$.

   (b) Show that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong Z_4$.

4. Let $\mathbb{K} = \mathbb{Q}(\sqrt{2},\sqrt{3}, u)$, where $u^2 = (9 - 5\sqrt{3})(2 - \sqrt{2})$.

   (a) Show that $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$.

   (b) Compute $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

5. Let b be an even positive integer of the form $2m$, m odd, and set $a = \frac{1}{2}b^2$. Set $\mathbb{K} = \mathbb{Q}(\sqrt{b - \sqrt{a}})$. Compute $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

6. Let q be a prime power and let $[\mathbb{E} : \mathbb{F}_q] = n$. Let F be the Frobenius automorphism of $\mathbb{E}$, given by $F(\alpha) = \alpha^q$. Define the *norm map*

$$N = N_{\mathbb{E}/\mathbb{F}_q} : \mathbb{E} \longrightarrow \mathbb{F}_q$$

   by setting

$$N(\alpha) = \alpha \cdot F(\alpha) \cdot F^2(\alpha) \cdots F^{n-1}(\alpha).$$

   Note that N restricts to a mapping

$$N : \mathbb{E}^\times \longrightarrow \mathbb{F}_q^\times.$$

   (a) Show that $N : \mathbb{E}^\times \to \mathbb{F}_q^\times$ is a group homomorphism.

   (b) Show that $|ker N| = \frac{q^n - 1}{q - 1}$.

7. Let p be a prime and let r be a positive integer. Prove that there exists an irreducible polynomial of degree r over $\mathbb{F}_p$.

8. Let p be prime, n a positive integer and set $q = p^n$. If $f(x) \in \mathbb{F}_p[x]$ is irreducible of degree m, show that $f(x) | x^q - x$. More generally, show that if $f(x)$ is irreducible of degree n, where $n|m$, then again, $f(x) | x^q - x$.

9. Let $f(x) \in \mathbb{F}[x]$ and assume that $f(x^n)$ is divisible by $(x-a)^k$, where $0 \neq a \in \mathbb{F}$. Prove that $f(x^n)$ is also divisible by $(x^n - a^n)^k$. (Hint: If $F(x) = f(x^n)$ is divisible by $(x-a)^k$, then $F'(x) = f'(x^n)nx^{n-1}$ is divisible by $(x-a)^{k-1}$, i.e., $f'(x^n)$ is divisible by $(x-a)^{k-1}$. Continue in this fashion to argue that that $f^{(k-1)}(x^n)$ is divisible by $x-a$, from which one concludes that $f(x)$ is divisible by $(x-a^n)^k$.)

10. This, and the next exercise are devoted to finding a formula for the number of irreducible polynomials over $\mathbb{F}_q$, where q is a prime power. The key rests on the so-called *Inclusion-Exclusion Principle* of combinatorial theory. To this end, define the function $\mu : \mathbb{N} \to \mathbb{Z}$ by setting

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ factors into } k \text{ distinct primes,} \\ 0 & \text{if not.} \end{cases}$$

(i) Show that if k, l are integers with $k|l$, then

$$\sum_{k|n|l} \mu(\frac{n}{k}) \;=\; \begin{cases} 1 & \text{if } k = l, \\ 0 & \text{if not.} \end{cases}$$

(ii) Now let $f, g : \mathbb{N} \to \mathbb{R}$ be real-valued functions, and assume that for each $n \in \mathbb{N}$, we have

$$f(n) \;=\; \sum_{k|n} g(k).$$

Prove that for each $n \in \mathbb{N}$,

$$g(n) \;=\; \sum_{k|n} \mu(\frac{n}{k}) f(k).$$

(Hint: For any $m|n$ we have

$$f(m) \;=\; \sum_{k|m} g(k).$$

Next, multiply the above by $\mu(\frac{n}{m})$ and sum over $m|n$:

$$\sum_{m|n} \mu(\frac{n}{m}) f(m) \;=\; \sum_{k|m|n} \mu(\frac{n}{m}) g(k) \;=\; g(n).)$$

11. For any integer n, let D_n be the number of irreducible polynomials of degree n in $\mathbb{F}_q[x]$. Prove that

$$D_n \;=\; \frac{1}{n}\sum_{k|n}\mu(\frac{n}{k})q^k.$$

(Hint: Simply note that, by *Exercise* 8, $q^n \;=\; \sum_{k|n} k \cdot D_k$.)

12. The following is really a group theory exercise, but since it involves inclusion-exclusion, I've put it here. Namely, let p be prime and prove that

$$\sum_a a \;=\; \mu(p-1) \,(\mathrm{mod}\, p),$$

where $a \in \mathbb{Z}$ ranges over a set of representatives of generators of the cyclic group $(\mathbb{Z}/(p))^\times$.

2.5 Brief Interlude: the Krull Topology

Let let $\mathbb{E} \supseteq \mathbb{F}$ be an algebraic Galois extension. We introduce into $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ a topology, as follows. If $\alpha_1, \alpha_2, \cdots, \alpha_k \in \mathbb{E}$, and if $\sigma \in G$, set

$$\mathcal{O}(\alpha_1, \alpha_2, \cdots, \alpha_k; \sigma) = \{\tau \in G |\ \tau(\alpha_i) = \sigma(\alpha_i), 1 \leq i \leq k\}.$$

Then the collection $\{\mathcal{O}(\alpha_1, \alpha_2, \cdots, \alpha_k; \sigma)\}$ forms a base for a topology on G; call this topology the *Krull topology*.

Another way to describe the above basic open sets is as follows. If $\alpha_1, \alpha_2, \cdots, \alpha_k$ are in $\mathbb{E}$, then $\mathbb{K} := \mathbb{F}(\alpha_1, \alpha_2, \cdots, \alpha_k)$ is a finite extension of $\mathbb{F}$, and so $H := \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is a subgroup of G of finite index. One easily sees that

$$\{\mathcal{O}(\alpha_1, \alpha_2, \cdots, \alpha_k; \sigma)\} = \sigma H.$$

From this it follows that the basic open sets in the Krull topology on G are precisely the cosets of subgroups of finite index in G.

LEMMA 2.5.1 *Let $\sigma \in G$ and let $\mu_\sigma : G \to G$ be left multiplication by σ. Then μ_σ is continuous.*

PROPOSITION 2.5.2 *Let $\mathbb{E} \supseteq \mathbb{F}$ be an algebraic Galois extension with Galois group G, and let $H \leq G$. Then*

$$cl_G(H) = \overline{H}, \quad \textit{(Krull Closure)}.$$

THEOREM 2.5.3 *Let $\mathbb{E} \supseteq \mathbb{F}$ be an algebraic Galois extension, with Galois group G. Then G is compact.*

EXERCISES 2.5

1. Prove that multiplication $\mu : G \times G \to G$ ($\mu(\sigma, \tau) = \sigma\tau$) and inversion $\iota : G \to G$ ($\iota(\sigma) = \sigma^{-1}$) are continuous. Thus G, together with the Krull topology, is a topological group.
2. Prove that G is Hausdorff.
3. Prove that G is *totally discontinuous* .

2.6 The Fundamental Theorem of Algebra

The following result is an important component of any "serious" discussion of Galois Theory. However, it is a moot point as to whether it *really is* a theorem of *algebra*.

THEOREM 2.6.1 *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

2.7 The Galois Group of a Polynomial

Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$ be a separable polynomial. Let $\mathbb{E}$ be a splitting field over $\mathbb{F}$ for the polynomial $f(x)$, and set $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Since $\mathbb{E}$ is uniquely determined up to $\mathbb{F}$-isomorphism by $f(x)$, then G is uniquely determined up to isomorphism by $f(x)$. We'll call G the *Galois group* of the polynomial $f(x)$, and denote it $\mathrm{Gal}(f(x))$.

PROPOSITION 2.7.1 *Let $f(x) \in \mathbb{F}[x]$ be a separable polynomial, and let G be the corresponding Galois group. Assume that $f(x)$ factors into irreducibles as*

$$f(x) \;=\; \prod f_i(x)^{e_i} \in \mathbb{F}[x].$$

Let $\mathbb{E}$ be a splitting field over $\mathbb{E}$ of $f(x)$, and let Λ_i be the set of roots in $\mathbb{E}$ for $f_i(x)$. Then G acts transitively on each Λ_i.

Thus if we set $\Lambda = \bigcup \Lambda_i$, then we have a natural *injective* homomorphism

$$G \longrightarrow S_\Lambda.$$

An interesting question which naturally occurs is whether $G \leq A_\Lambda$, where we have identified G with its image in S_Λ. To answer this, we introduce the *discriminant* of the separable polynomial $f(x)$. Thus let $f(x) \in \mathbb{F}[x]$, where *char* $\mathbb{F} \neq 2$, and let $\mathbb{E}$ be a splitting field over $\mathbb{F}$ for $f(x)$. Let $\{\alpha_1, \alpha_1, \cdots, \alpha_k\}$ be the set of distinct roots of $f(x)$ in $\mathbb{E}$. Set

$$\delta = \prod_{1 \le j < i \le k} (\alpha_i - \alpha_j) = \det \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdot & \cdot & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdot & \cdot & \alpha_2^{k-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \alpha_k & \alpha_k^2 & \cdot & \cdot & \alpha_k^{k-1} \end{bmatrix},$$

and let $D = \delta^2$. We call D the *discriminant* of the polynomial $f(x)$. Note that $D \in \mathrm{inv}_G(\mathbb{E})$; since $f(x)$ is separable, $D \in \mathbb{F}$.

PROPOSITION 2.7.2 *Let $f(x) \in \mathbb{F}[x]$, with discriminant D defined as above. Let G be the Galois group of $f(x)$, regarded as a subgroup of S_n, where $\{\alpha_1, \cdots, \alpha_n\}$ is the set of roots in a splitting field $\mathbb{E}$ over $\mathbb{F}$ for $f(x)$. If $A = G \cap A_n$, then $inv_A(\mathbb{E}) = \mathbb{F}(\delta)$.*

COROLLARY 2.7.2.1 *Let G be the Galois group of $f(x) \in \mathbb{F}[x]$. If D is the square of an element in $\mathbb{F}$, then $G \le A_n$.*

The following is occasionally useful in establishing that the Galois group of a polynomial is the full symmetric group.

PROPOSITION 2.7.3 *Let $f(x) \in \mathbb{Q}[x]$ be irreducible, of prime degree p, and assume that $f(x)$ has exactly 2 non-real roots. Then $G_f = S_p$.*

There are straightforward formulas for the discriminants of quadratics and cubics.

PROPOSITION 2.7.4

(a) If $f(x) = x^2 + bx + c$, then $D_f = b^2 - 4c$.

(b) If $f(x) = x^3 + ax^2 + bx + c$, then

$$D_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

For a general "trinomial," there is a wonderful formula, due to R.G. Swan (Pacific Journal, vol 12, pp. 1099-1106, **MR** 26 #2432. (1962); see also Gary Greenfield and Daniel Drucker, On the discriminant of a trinomial, *Linear Algebra Appl.* **62** (1984), 105-112.), given as follows.

PROPOSITION 2.7.5 *Let $f(x) = x^n + ax^k + b$, and let $d = g.c.d.(n,k)$, $N = \frac{n}{d}$, $K = \frac{k}{d}$. Then*

$$D_f = (-1)^{\frac{1}{2}n(n-1)} b^{k-1} [n^N b^{N-k} - (-1)^N (n-k)^{N-K} k^K a^N]^d.$$

EXERCISES 2.6

1. Let $f(x) \in \mathbb{F}[x]$ be a separable polynomial. Show that $f(x)$ is irreducible if and only if $\mathrm{Gal}(f(x))$ acts transitively on the roots of $f(x)$.
2. Let ζ be a primitive n-th root of unity. Show that
$$1 + \zeta^i + \cdots + \zeta^{(n-1)i} = \begin{cases} n & \text{if } n|i \\ 0 & \text{if not.} \end{cases}$$
3. Show that
$$D_{(x^n-1)} = \det \begin{bmatrix} n & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & \cdot & n \\ 0 & 0 & \cdot & \cdot & n & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & n & \cdot & \cdot & \cdot \\ 0 & n & \cdot & \cdot & \cdot & 0 \end{bmatrix} = (-1)^{\frac{1}{2}(n-1)(n-2)} n^n.$$
4. Prove that
$$D_{(x^n-a)} = a^{n-1} n^n (-1)^{\frac{1}{2}(n-1)(n-2)}.$$
5. Compute the discriminant of $x^7 - 154x + 99$. (This polynomial has $PSL(2,7)$ as Galois group.)
6. Find an irreducible cubic polynomial whose discriminant is a square in $\mathbb{Q}$. (One example is $x^3 - 9x + 9$.)
7. Compute discriminants of $x^7 - 7x + 3$, $x^5 - 14x^2 - 42$.
8. Let $f(x) \in \mathbb{Q}[x]$ be irreducible, and assume that $\mathrm{Gal}(f(x)) \cong Q_8$, the quaternion group of order 8. Prove that $\deg f(x) = 8$.

9. Prove that for each $n \geq 1$, the Galois group over the rationals of the polynomial $f(x) = x^3 - 3^{2n}x + 3^{3n-1}$ is cyclic of order 3.

10. Suppose that $f(x) \in \mathbb{Q}[x]$ has degree 4, is monic, irreducible, and has negative discriminant. Prove that $f(x)$ cannot have a cyclic Galois group.

11. If $f(x) = x^6 - 4x^3 + 1$, prove that $G_f \cong D_{12}$.

12. Let G be the Galois group of the polynomial $x^5 - 2 \in \mathbb{Q}[x]$; thus, if $\mathbb{K}$ is the splitting field, then $\mathbb{K} = \mathbb{Q}(\sqrt[5]{2}, \zeta)$, where $\zeta = e^{2\pi i/5}$. Explicitely construct an element of order 4 in the Galois group, and show what it does to $\sqrt[5]{2}$ and to ζ.

13. Let G be the Galois group of the polynomial $x^8 - 2 \in \mathbb{Q}[x]$. Thus, if $\mathbb{K}$ is the splitting field, then $\mathbb{K} = \mathbb{Q}(\sqrt[8]{2}, \zeta)$, where $\zeta = e^{2\pi i/8}$. Show that G has order 16. Also, compute the kernel of the action of G on the four roots of $x^4 + 1$.

14. Let $f_1(x) = x^8 - 2$ and let $f_2(x) = x^8 - 3$. Prove that $G_{f_1} \ncong G_{f_2}$.

2.8 The Cyclotomic Polynomials

Let n be a positive integer, and let ζ be the complex number $\zeta = e^{2\pi i/n}$. Set

$$\Phi_n(x) = \prod_d (x - \zeta^d),$$

where $1 \leq d \leq n$, and $gcd(d, n) = 1$. We call $\Phi_n(x)$, the n-th *cyclotomic polynomial*. A little thought reveals that

$$x^n - 1 = \prod_{d|n} \Phi_d(x);$$

in particular, we have (using induction) that $\Phi_n(x) \in \mathbb{Z}[x]$.

PROPOSITION 2.8.1 *$\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$.*

PROPOSITION 2.8.2 *Let $\mathbb{F}$ be a field, and let $f(x) = x^n - 1 \in \mathbb{F}[x]$. If G is the Galois group of $f(x)$, then G is isomorphic to a subgroup of the group U_n of units in the ring $\mathbb{Z}/(n)$ of integers modulo n.*

COROLLARY 2.8.2.1 *Same hypotheses as above, except that $\mathbb{F} = \mathbb{Q}$. Then G is also the Galois group of $\Phi_n(x)$, and is isomorphic to U_n.*

As an application of the above simple result, we have the following result.

PROPOSITION 2.8.3 *Let A be any abelian group. Then there exists a finite Galois extension $\mathbb{K} \supseteq \mathbb{Q}$ such that Gal$(\mathbb{K}/\mathbb{Q}) \cong A$. In fact, there exists an integer n such that $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/n}$.*

We can easily outline the proof here, we will. The main ingredient is the following special case of the so-called *Dirichlet Theorem on Primes in an Arithmetic Progression*, namely, if n is any integer, then there are infinitely many primes p such that $p \equiv 1 \bmod n$. Assuming this result, the proof proceeds as follows. If A is an abelian group, then A can be decomposed as a product of cyclic groups:

$$A \;\cong\; Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_k}.$$

Choose distinct primes $p_1, p_2, \ldots p_k$ such that $p_i \equiv 1 \bmod n_i$, $i = 1, 2, \ldots, k$. Now set $n = p_1 p_2 \cdots p_k$, $\zeta = e^{2\pi i/n}$. Then

$$\text{Gal } (\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U_n \cong Z_{p_1-1} \times Z_{p_2-1} \times \cdots \times Z_{p_k-1}.$$

Choose generators $\sigma_1, \sigma_2, \ldots, \sigma_k$ in each of the factors and let $H = \langle \sigma_1^{(p_1-1)/n_1}, \sigma_2^{(p_2-1)/n_2}, \ldots, \sigma_k^{(p_k-1)/n_k} \rangle$; setting $\mathbb{K} = \mathrm{inv}_H(\mathbb{Q}(\zeta))$ we get

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathrm{Gal}\ \mathbb{Q}(\zeta)/H \cong A.$$

EXERCISES 2.7

1. Compute $\Phi_n(x),\ 1 \leq n \leq 20$.
2. Suppose that p is prime and that $n \geq 1$. Show that
$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n, \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \not| \ n. \end{cases}$$
3. Show that if n is a positive odd integer, then $\Phi_{2n}(x) = \Phi_n(-x)$.
4. (For those who know Möbius inversion). Show that
$$\Phi_n(x) \ = \ \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$
5. Let $\zeta = e^{2\pi i/5}$. Show that $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\sqrt{5})$
6. Let n be a positive integer and let $\zeta = e^{2\pi i/n}$, a primitive n-th root of unity. Let $n = 2^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ is the prime factorization of n, and compute the structure of $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q})$. (Use *Exercises* 1 and 2 of *Section* 1.5 of *Chapter* 1.)
7. Let n be a positive integer. Show that
   (a) If $8|n$, then $\mathbb{Q}(\cos 2\pi/n) = \mathbb{Q}(\sin 2\pi/n)$;
   (b) If $4|n,\ 8 \not| \ n$, but $n \neq 4$, then $\mathbb{Q}(\sin 2\pi/n) \subseteq \mathbb{Q}(\cos 2\pi/n)$, and $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}(\sin 2\pi/n)] = 2$;
   (c) If $4 \not| \ n$, but $n \neq 1, 2$ then $\mathbb{Q}(\cos 2\pi/n) \subseteq \mathbb{Q}(\sin 2\pi/n)$, and $[\mathbb{Q}(\sin 2\pi/n) : \mathbb{Q}(\cos 2\pi/n)] = 2$.

8. Show that if $n \neq 1, 2$, then the degree of the minimal polynomial of $\cos 2\pi/n$ is $\phi(n)/2$. Using *Exercise* 7, compute the degree of the minimal polynomial of $\sin 2\pi/n$. (The minimal polynomial of $\cos 2\pi/n$ can be computed in principle in terms of the so-called *Chebychev polynomials.*)[1]

9. Let $n \geq 3$, and set $\alpha_{n-2} = e^{2\pi i/2^n} + e^{-2\pi i/2^n} \in \mathbb{R}$. Show that $\alpha_1 = \sqrt{2}, \alpha_2 = \sqrt{2+\sqrt{2}}, \ldots, \alpha_n = \sqrt{2+\sqrt{2+\sqrt{\cdots+\sqrt{2}}}}$ (n times). (Show that $\alpha_n^2 = 2 + \alpha_{n-1},\ n \geq 2$.)

10. Notation as above. Show that $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_n)$ is a Galois extension whose Galois group has order $2^n,\ n = 1, 2, \ldots$. (This will require *Exercise* 2, of *Section* 1.5.)

11. Let m, n be relatively prime positive integers, and set $\zeta = e^{2\pi i/n}$. Show that $\Phi_m(x)$ is irreducible in $\mathbb{Q}(\zeta)[x]$.

[1] See W. WATKINS and J. ZEITLIN, The minimal polynomial of $\cos 2\pi/2$, *Amer. Math. Monthly* **100**, (1993), no. 5, 474-474, MR **94b:12001**.

2.9 Solvability by Radicals

For the sake of simplicity, we shall assume throughout this section that all fields have characteristic 0. Let $\mathbb{F}$ be a field and let $\mathbb{E}$ be an extension of $\mathbb{F}$. If $\mathbb{E} = \mathbb{F}(\alpha)$ for some $\alpha \in \mathbb{E}$ satisfying $\alpha^n \in \mathbb{F}$, for some integer n, then $\mathbb{E}$ is called a *simple radical extension* of $\mathbb{F}$. Let $f(x) \in \mathbb{F}[x]$, and let $\mathbb{E}$ be a splitting field for $f(x)$ over $\mathbb{F}$. Assume also that there is a sequence

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r \supseteq \mathbb{E},$$

where each $\mathbb{F}_k$ is a simple radical extension of $\mathbb{F}_{k-1}$. (We call the tower $\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r$ a *root tower* .) Then we say that the polynomial $f(x)$ is *solvable by radicals* .

LEMMA 2.9.1 *Assume that the polynomial $f(x) \in \mathbb{F}[x]$ is solvable by radicals, and let $\mathbb{E}$ be a splitting field for $f(x)$ over $\mathbb{F}$. Then there exists a root tower*

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_r \supseteq \mathbb{E}$$

where $\mathbb{F}_r$ is Galois over $\mathbb{F}$.

LEMMA 2.9.2

(a) *Let $\mathbb{E} = \mathbb{F}(a)$ be a simple radical extension, where $a^n \in \mathbb{F}$. Assume that the polynomial $x^n - 1$ splits completely in $\mathbb{F}[x]$. Then Gal$(\mathbb{E}/\mathbb{F})$ is cyclic.*

(b) *Let $\mathbb{E} \supseteq \mathbb{F}$ be a Galois extension of prime degree q, and assume that $x^q - 1$ splits completely in $\mathbb{F}[x]$. Then $\mathbb{E}$ is a simple radical extension of $\mathbb{F}$.*

We are now in a position to state E. Galois' famous result.

THEOREM 2.9.3 *Let $\mathbb{F}$ be a field of characteristic 0, and let $f(x) \in \mathbb{F}[x]$, with Galois group G. Then $f(x)$ is solvable by radicals if and only if G is a solvable group.*

2.10 The Primitive Element Theorem

Let $\mathbb{F} \subseteq \mathbb{E}$ be a field extension. We say that this extension is *simple* , or that $\mathbb{E}$ has a *primitive element* over $\mathbb{F}$ if there exists $\alpha \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{F}(\alpha)$.

THEOREM 2.10.1 *Let $\mathbb{F} \subseteq \mathbb{E}$ be a field extension with $[\mathbb{E} : \mathbb{F}] < \infty$. Then $\mathbb{E}$ has a primitive element over $\mathbb{F}$ if and only if there are only a finite number of fields between $\mathbb{F}$ and $\mathbb{E}$.*

Let $\mathbb{F} \subseteq \mathbb{E}$ be a field extension, and let $\alpha \in \mathbb{E}$. We say that α is *separable* over $\mathbb{F}$ if its minimal polynomial $m_\alpha(x) \in \mathbb{F}[x]$ is separable. If every element of $\mathbb{E}$ is separable over $\mathbb{F}$, then we call $\mathbb{E}$ a *separable extension* of $\mathbb{F}$.

COROLLARY 2.10.1.1 *[Primitive Element Theorem] Let $\mathbb{F} \subseteq \mathbb{E}$ be a finite dimensional separable field extension. Then $\mathbb{E}$ contains a primitive element over $\mathbb{F}$.*

EXERCISES 2.8

1. Find a primitive element for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$
2. Find a primitive element for a splitting field for $x^4 - 2$ over $\mathbb{Q}$.
3. Let $\mathbb{F} \subseteq \mathbb{E}$ be a finite Galois extension with Galois group G. If $\alpha \in \mathbb{E}$, prove that
$$[\mathbb{F}(\alpha) : \mathbb{F}] \;=\; [G : \mathrm{Stab}_G(\alpha)].$$
4. Let $\mathbb{F}$ be any field and let x be an indeterminate over $\mathbb{F}$. Let $\mathbb{E} = \mathbb{F}(x)$. Let y be an indeterminate over $\mathbb{E}$, and let $\mathbb{K} = \mathbb{E}[y]/(y^2 - x(x-1))$, regarded as an extension field of $\mathbb{E}$. Show that $\mathbb{K}$ is a simple extension of $\mathbb{F}$ (though obviously not of finite dimension).
5. Let $\mathbb{Q} \subseteq \mathbb{K}$ be a field extension. Assume that whenever $\alpha \in \mathbb{Q}$, then $\sqrt{\alpha} \in \mathbb{K}$. Prove that $[\mathbb{K} : \mathbb{Q}] = \infty$. (Compare with *Exercise* 8 of *Section* 2.1.)
6. Let $\mathbb{F}$ be a field and let x be indeterminate over $\mathbb{F}$. Are there finitely or infinitely many subfields between $\mathbb{F}$ and $\mathbb{F}(x)$?

7. Let $\mathbb{F} \subseteq \mathbb{E}$ be a field extension such that there are finitely many subfields between $\mathbb{F}$ and $\mathbb{E}$. Prove that $\mathbb{E}$ is a finite extension of $\mathbb{F}$.

8. Let $\mathbb{F} \subseteq \mathbb{E}$ be a finite separable extension and assume that $\mathbb{E} = \mathbb{F}(\alpha, \beta)$ for some $\alpha, \beta \in \mathbb{E}$. Prove that $\mathbb{E} = \mathbb{F}(\alpha + a\beta)$ for all but finitely many $a \in \mathbb{F}$.

Chapter 3

Elementary Factorization Theory

3.1 Basics

Throughout this section, all rings shall be assumed to be commutative and to have (multiplicative) identity. I shall denote the identity element by 1.

Let R be a commutative ring (I'll probably be redundant for awhile), and let $0 \neq a \in R$. If there exists $b \in R,\ b \neq 0$ such that $ab = 0$, we say that a is a *zero-divisor* . (Thus, b is also a zero-divisor.) If R has no zero divisors, then R is called an *integral domain* .

Let R be a ring and let $I \subseteq R$ be an ideal. We call I a *prime ideal* if whenever $a, b \in R$ and $ab \in I$, then one of a or b is in I. The following is basic.

PROPOSITION 3.1.1 *I is a prime ideal if and only if the quotient ring R/I is an integral domain.*

If $I \subseteq R$ is an ideal not properly contained in any other proper ideal, then I is called a *maximal ideal* . The following is easy.

LEMMA 3.1.2 *A maximal ideal is always prime.*

PROPOSITION 3.1.3 *I is a maximal ideal if and only if the quotient ring R/I is a field.*

Let R be a ring and let $a \in R$. The set $(a) = \{ra|\ r \in R\}$ is an ideal in R, called the *principal ideal* generated by a. Sometimes we shall write Ra

(or aR) in place of simply writing (a) if we want to emphasize the ring R. More generally, if $a_1, a_2, \ldots, a_k \in R$, we shall denote by $(a_1, a_2, \ldots, a_k)$ the ideal $\{\sum r_i a_i |\ r_1, r_2, \ldots, r_k \in R\}$.

Exercises

1. Assume that the commutative ring R has zero divisors, *but only finitely many*. Prove that R itself must be finite. (Hint: Let $a \in R$ be a zero divisor and note that each non-zero element of (a) is also a zero divisor. Now consider the homomorphism of additive abelian groups $R \to (a),\ r \mapsto ra$. Every non-zero element of the kernel of this map is also a zero divisor. Now what?)

2. For which values of n is $\mathbb{Z}/(n)$ an integral domain?

3. Prove that if R is a finite integral domain, then R is actually a field.

4. Prove that if R is an integral domain, and if x is an indeterminate over R, then the polynomial ring $R[x]$ is an integral domain.

5. Let R be a commutative ring and let $I,\ J \subseteq R$ be ideals. If we define

$$I\ +\ J\ =\ \{r + s |\ r \in I,\ s \in J\},$$

$$IJ\ =\ \{\sum r_i s_i |\ r_i \in I,\ s_i \in J\},$$

   then $I + J$ and IJ are both ideals of R. Note that $IJ \subseteq I \cap J$.

6. Again, let R be a commutative ring and let $I,\ J$ be ideals of R. We say that $I,\ J$ are *relatively prime* (or are *comaximal*) if $I + J = R$. Prove that if $I,\ J$ are relatively prime ideals of R, then $IJ = I \cap J$.

7. Prove the *Chinese Remainder Theorem*: Let R be a commutative ring and let $I,\ J$ be relatively prime ideals of R. Then the ring homomorphism $R \to R/I \times R/J$ given by $r \mapsto ([r]_I, [r]_J)$ determines an isomorphism

$$R/(IJ)\ \cong\ R/I \times R/J.$$

   More generally, if $I_1, I_2, \ldots, I_r \subseteq R$ are pairwise relatively prime, then the ring homomorphism $R \to R/I_1 \times R/I_2 \times \cdots \times R/I_r,\ r \mapsto ([r]_{I_1}, [r]_{I_2}, \ldots, [r]_{I_r})$ determines an isomorphism

$$R/(IJ)\ \cong\ R/I_1 \times R/I_2 \times \cdots \times R/I_r.$$

8. Let $P \subseteq R$ be a prime ideal, and let $I, J \subseteq R$ be ideals with $IJ \subseteq P$. If $I \not\subseteq P$, prove that $J \subseteq P$.

9. Let R be a commutative ring and let $I \subseteq R$ be an ideal. If $I \subseteq P_1 \cup P_2 \cup \cdots \cup P_r$, where $P_1, P_2, \ldots P_r$ are prime ideals, show that $I \subseteq P_j$ for some index j. (Hint: use induction on r.)

10. *Residual Quotients.* Let R be a commutative ring and let $I, J \subseteq R$ be ideals. Define the *residual quotient* of I by J by setting

$$I : J \ = \ \{c \in R |\ cJ \subseteq I\}.$$

    (a) Prove that $I : J$ is an ideal of R.

    (b) Prove that $I \subseteq I : J$.

    (c) Prove that $(I : J)J \subseteq I$; in fact, $I : J$ is the largest ideal $K \subseteq R$ satisfying $KJ \subseteq I$.

    (d) For ideals $I, J, K \subseteq R$, $(I : J) : K = I : (JK)$.

11. *Primary Ideals.* Let $Q \subseteq R$ be an ideal. We say that Q is *primary* if $ab \in Q$ and $a \notin Q$ implies that $b^n \in Q$ for some positive integer n. Prove the following for the primary ideal $Q \subseteq R$:

    (a) If $P = \{r \in R |\ r^m \in Q \text{ for some positive integer } m\}$, then P is a prime ideal containing Q. In fact P is the smallest prime ideal containing Q. (In this case we call Q a *P-primary* ideal.)

    (b) If Q is a P-primary ideal, $ab \in Q$, and $a \notin P$, then $b \in Q$.

    (c) If Q is a P-primary ideal and I, J are ideals of R with $IJ \subseteq Q$, $I \not\subseteq P$, then $J \subseteq Q$.

    (d) If Q is a P-primary ideal and if I is an ideal $I \not\subseteq P$, then $Q : I = Q$.

12. Suppose that P and Q are ideals of R satisfying the following:

    (a) $P \supseteq Q$.

    (b) If $x \in P$ then for some positive integer n, $x^n \in Q$.

    (c) If $ab \in Q$ and $a \notin P$, then $b \in Q$.

    Prove that Q is a P-primary ideal.

13. Assume that $Q_1, Q_2, \ldots Q_r$ are all P-primary ideals. Show that $Q_1 \cap Q_2 \cap \ldots \cap Q_r$ is a P-primary ideal.

14. Let R be a ring and let $Q \subseteq R$ be an ideal. Prove that Q is a primary ideal if and only if the only zero divisors of R/Q are nilpotent elements. (An element r of a ring is called *nilpotent* if $r^n = 0$ for some positive integer n.)

15. Consider the ideal $I = (n, x) \subseteq \mathbb{Z}[x]$, where $n \in \mathbb{Z}$. Prove that I is a maximal ideal of $\mathbb{Z}[x]$ if and only if n is a prime.

16. If R is a commutative ring and $x \in \cap\{M |\ M$ is a maximal ideal$\}$, show that $1 + x \in \mathcal{U}(R)$.

3.2 Unique Factorization Domains

In this section R is always an integral domain. If $u \in R$ is an element having a multiplicative inverse, we call u a *unit* . The set $\mathcal{U}(R)$, with respect to multiplication, is obviously an abelian group, called the *group of units* of R.

Let $a, b \in R,\ a \neq 0$. If $b = qa$ for some $q \in R$, we say that a *divides* b, and write $a|b$. Obviously, if $u \in \mathcal{U}(R)$, and if $b \in R$, then $u|b$. If $a, b \in R$. Say that a, b are *associates* if there exists $u \in \mathcal{U}(R)$ such that $a = ub$. If $a, b \in R$ and d is a common divisor of both, we say that d is a *greatest common divisor* if any other divisor of both a and b also divides d. In the same vein, if l is a multiple of both a and b, and if any multiple of both is also a multiple of a and b, we say that l is a *least common multiple* of a and b. Note that if a greatest common divisor exists, it is unique up to associates, and it makes sense to write $d = g.c.d.(a, b)$ for the greatest common divisor of a and b; the same is true for a least common multiple, and we write $l = l.c.m(a, b)$ for the least common multiple of a and b.

Let $p \in R,\ p \notin \mathcal{U}(R)$. We say that p is *irreducible* if $p = ab$ implies that $a \in \mathcal{U}(R)$ or $b \in \mathcal{U}(R)$. We say that p is *prime* if the ideal $(p) \subseteq R$ is a prime ideal in R. The following is elementary.

PROPOSITION 3.2.1 *Let $p \in R$. If p is prime, then p is irreducible.*

The converse of the above fails; here's an example. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}|\ a, b \in \mathbb{Z}\}$. Then 3 is easily checked to be irreducible, but $(4 + \sqrt{-5})(4 - \sqrt{-5}) \in (3)$, whereas $(4 + \sqrt{-5}), (4 - \sqrt{-5}) \notin (3)$.

We say the integral domain R is a *unique factorization domain* (*u.f.d.*) if

(i) Every irreducible element is prime.

(ii) If $0 \neq a \in R$, and if a is not a unit, then there exist primes $p_1, p_2, \ldots, p_n \in R$ such that $a = p_1 p_2 \cdots p_n$.

We remark that it is possible for either one of the above conditions to hold in an integral domain without the other also being valid. For instance, for a ring satisfying (ii) but not (i), see *Exercise* 4. For a ring satisfying (i) but not (ii), consult *Exercise* 8, below.

PROPOSITION 3.2.2 *Let R be a unique factorization domain, and let $a \in R$, $a \notin \mathcal{U}(R)$. Then there exist unique (up to associates) primes $p_1, p_2, \ldots, p_k \in R$, and unique exponents $e_1, e_2, \ldots, e_k \in \mathbb{N}$ such that $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.*

The above explains the terminology "unique" in unique factorization domain.

The reader should note that the ring of the above example is not a unique factorization domain. One can show, however, that every non-unit in R can be factored as a product of irreducibles. (See *Exercise* 4.) From this example, I hope that the reader can get some idea of the subtlety of unique factorization domains.

Let R be a *u.f.d.*, and let $a, b \in R$. In this setting the greatest common divisor and least common multiple of a, b both exist in R, and can be constructed as follows: If we factor a and b into primes:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r},$$

(where possibly some of the e_i's or f_j's are 0), we set

$$d = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}, \quad t_i = \min\{e_i, f_i\}, \ i = 1, 2, \ldots, r;$$

Then d is the *greatest common divisor* of a and b, denoted $d = \text{g.c.d.}(a, b)$. Likewise, if we set

$$q = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}, \quad s_i = \max\{e_i, f_i\}, \ i = 1, 2, \ldots, r,$$

then q is the *least common multiple* of a and b, and denoted $q = \text{l.c.m.}(a, b)$

It is assumed that the reader has already had a previous course in abstract modern algebra, where one typically learns that two paradigm examples of unique factorization domains are the ring $\mathbb{Z}$ of integers and the polynomial ring $\mathbb{F}[x]$ over the field $\mathbb{F}$. That these rings are both unique factorization domains will be proved again in *Section* 3.4 below, independently of the present section. For what follows, we shall use the fact that $\mathbb{F}[x]$ is a *u.f.d.*

For the remainder of the section, we shall be concerned with the study of the polynomial ring $R[x]$, where R is an integral domain. Note that in this case it is easy to see that $R[x]$ is also an integral domain. It shall be convenient to move back and forth between $R[x]$ and $\mathbb{F}[x]$, where $\mathbb{F} = \mathcal{F}(R)$ is the field of fractions of R. As remarked above, $\mathbb{F}[x]$ is a unique factorization domain. Note that $\mathcal{U}(R[x]) = \mathcal{U}(R)$ the group of units of R.

Henceforth, we shall assume that R is a unique factorization domain. Our goal is to supply the necessary ingredients to prove that $R[x]$ is again a unique factorization domain.

We say that the polynomial $f(x) \in R[x]$ is *primitive* if the greatest common divisor of the coefficients of $f(x)$ is 1. More generally, if If $g(x) \in R[x]$, and if $c \in R$ is the greatest common divisor of the coefficients of $g(x)$, then we may write $g(x) = cf(x)$ where $f(x)$ is a primitive polynomial in $R[x]$. The element $c \in R$ is called the *content* of $g(x)$; note that it is well-defined, up to associates.

LEMMA 3.2.3 (GAUSS' LEMMA) *If $f(x), g(x) \in R[x]$ are primitive polynomials, then so is $f(x)g(x)$.*

LEMMA 3.2.4 *Let R be a u.f.d. with fraction field $\mathbb{F}$. Assume that $f(x), g(x) \in R[x]$ are primitive polynomials and that $f(x), g(x)$ are associates in $\mathbb{F}[x]$. Then $f(x), g(x)$ are associates in $R[x]$.*

LEMMA 3.2.5 *Let $f(x) \in R[x]$ be primitive, and assume that $f(x) \,\big|\, cg(x)$, where $c \in R$, and $g(x) \in R[x]$ is also primitive. Then $f(x) \,\big|\, g(x)$.*

LEMMA 3.2.6 *If $f(x) \in R[x]$ is irreducible, then $f(x)$ is still irreducible in $\mathbb{F}[x]$.*

With the above results in place, one can now prove the following:

THEOREM 3.2.7 *If R is a unique factorization domain, so is the polynomial ring $R[x]$.*

In particular, it follows that if R is a unique factorization domain, and if $x_1, x_2, \ldots, x_r$ are indeterminates over R, then $R[x_1, x_2, \ldots, x_r]$ is again a unique factorization domain.

Before closing this section, I can't resist throwing in the following batch of examples. Let n be a positive integer and let $\zeta = e^{2\pi i/n}$; set $R = \mathbb{Z}[\zeta] \subseteq \mathbb{C}$. The importance of these rings is that there exist early (but incorrect) proofs of the famous Fermat conjecture ("Fermat's Last Theorem;" recently

proved by Andrew Wiles), based on the assumption that R is a unique factorization domain for every value of n. Unfortunately, this assumption is false; the first failure occurs for $n = 23$. (In the ring $\mathbb{Z}[e^{2\pi i/23}]$, one has that the number 2 is irreducible, but not prime.) This result came as a shock to many mathematicians; on the other hand, it led to many new and interesting avenues of research, leading to the development of "algebraic number theory." We shall touch on this area in the next chapter.

Exercises

1. Compute $\mathcal{U}(R)$ in each case below.
   (a) $R = \mathbb{Z}$.
   (b) $R = \mathbb{Z}/(n)$.
   (c) $R = \mathbb{Z}[i] = \{a + bi |\ a, b \in \mathbb{Z}\}$ $(i^2 = -1)$.
   (d) $R = \mathbb{Z}[\zeta] = \{a + b\zeta |\ a, b \in \mathbb{Z}\}$ $(\zeta = e^{2\pi i/3})$.
2. Let $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} |\ a, b \in \mathbb{Z}\}$. Prove that $\mathcal{U}(R)$ is infinite.
3. Let $\mathbb{F}$ be a field and let x be indeterminate over $\mathbb{F}$. Prove that the ring $R = \mathbb{F}[x^2, x^3]$ is not a *u.f.d.* (Consider the equation $(x^2)^3 = (x^3)^2$.)
4. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\}$. Then every non-unit of R can be factored as a product of irreducibles. (Hint: Define a "norm" map on R by setting $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Note that if $r, s \in R$, then $N(rs) = N(r)N(s)$. So what?)
5. As above, let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\}$. Show that it need not happen that any pair of non-units in R has a greatest common divisor. (In fact, one can show that 21 and $7(4+\sqrt{-5})$ have no greatest common divisor.)
6. Let n be a square-free integer (i.e., is not divisible by the square of any integer > 1) such that $n \equiv 1 \pmod 4$ and let $R = \mathbb{Z}[\sqrt{n}]$. Prove that 2 is an irreducible element but is not prime. (Hint: note that $(1 + \sqrt{n})(1 - \sqrt{n})/4 \in \mathbb{Z}$.) Conclude that R cannot be a *u.f.d.*
7. Let R be an integral domain in which every pair of elements has a greatest common divisor. Prove that every irreducible element is prime. (Hint: Let $p \in R$ be irreducible and assume that $p \,|\, ab$ but that

$p \not| a$. Then the elements ab and ap have a greatest common divisor d. Thus $p \mid d$ and $d \mid ap$, forcing $d = pa'$ for some divisor $a' \mid a$. Similarly $d = ab'$ for some divisor $b' \mid b$. From $pa' = ab'$ we get $p = b'(a/a')$; since p is irreducible, we have $b' \in \mathcal{U}'(R)$ or $a/a' \in \mathcal{U}'(R)$ Now what?)

8. Consider the integral domain $D = \mathcal{O}(\mathbb{C})$ of holomorphic functions on the complex plane. Prove that every irreducible element of D is prime, but that D is not a *u.f.d.* More precisely, prove that

   (a) The irreducibles in D are the functions of the form $f(z) = z - z_0$ (and their associates), where $z_0 \in \mathbb{C}$.

   (b) Irreducibles are primes.

   (c) The function $f(z) = \sin z$ cannot be factored into irreducibles.

9. Prove *Eisenstein's Irreducibility Criterion.* Namely, let R be a *u.f.d.* and let $f(x) \in R[x]$. Write

$$f(x) \;=\; a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

   Assume that there exists a prime $p \in R$ such that

   (a) $p \not| a_n$;

   (b) $p \mid a_i,\ 0 \le i \le n-1$;

   (c) $p^2 \not| a_0$.

   Then $f(x)$ is irreducible.

10. Let $x_1, x_2, \ldots, x_{n^2}$ be indeterminates and consider the matrix

$$A \;=\; \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_{n+1} & x_{n+2} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ \cdot & \cdot & \cdots & x_{n^2} \end{bmatrix}.$$

    Show that $\det A$ is an irreducible polynomial in $\mathbb{C}[x_1, x_2, \ldots, x_{n^2}]$. (Hint:

$$\det \begin{bmatrix} y & 0 & 0 & \cdots & 0 & x \\ 1 & y & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & y \end{bmatrix} = y^n \pm x.)$$

11. Let R be a *u.f.d.* and let $x_1, x_2, \ldots$ be indeterminates over R. Prove that $R[x_1, x_2, \ldots]$ is a *u.f.d.*

3.3 Noetherian Rings and Principal Ideal Domains

Let R be a ring (commutative, remember?). We call R *Noetherian* if whenever we have a chain

$$I_1 \subseteq I_2 \subseteq \cdots$$

of ideals, then there exists an integer N such that if $n \geq N$, then $I_n = I_N$.

If $I \subseteq R$ is an ideal, we say that I is *finitely generated* if there exist $a_1, a_2, \ldots, a_k \in R$ such that $I = (a_1, a_2, \ldots, a_k)$, i.e., if every element of I is of the form $\sum r_i a_i,\ r_i \in R$.

The following is basic and quite useful.

THEOREM 3.3.1 *Let R be a commutative ring. The following are equivalent.*

(i) R is Noetherian.

(ii) Every ideal in R is finitely generated.

(iii) Every collection of ideals has a maximal element with respect to inclusion.

The next result result is not only intrinsically interesting, it is also a fundamental tool in the study of algebraic geometry and commutative algebra.

THEOREM 3.3.2 (HILBERT BASIS THEOREM) *If R is Noetherian, so is the polynomial ring $R[x]$.*

An important, but rather "small" class of examples of Noetherian rings is as follows. Let R be an integral domain. We say that R is a *principal ideal domain* (*p.i.d.*) if every ideal of R is generated by a single element. Thus if $I \subseteq R$ is an ideal, then there exists $a \in R$ such that $I = (a)$. The "canonical" examples are

(i) $\mathbb{Z}$, and

(ii) The polynomial rings $\mathbb{F}[x]$, where $\mathbb{F}$ is a field.

However, that these really are examples is the result of their satisfying an even stronger condition, as discussed in the next section.

THEOREM 3.3.3 *If R is* a p.i.d.*, then R is Noetherian.*

THEOREM 3.3.4 *If R is a* p.i.d., *then R is a* u.f.d..

Exercises

1. Prove that if R is Noetherian, and if I is an ideal in R, then R/I is Noetherian.
2. Let $R \subseteq S$ be integral domains, with R Noetherian. If $s_1, s_2, \ldots s_r \in S$, prove that $R[s_1, s_2, \ldots s_r] \subseteq S$ is Noetherian.
3. Let R be a ring and let $x_1, x_2, \ldots$ be infinitely many indeterminates over R. Prove that the polynomial ring $R[x_1, x_2, \ldots]$ is not Noetherian.
4. Let R be a *u.f.d.* in which every prime ideal is maximal. Prove that R is actually a *p.i.d.* (Start by showing that every prime ideal is principal.)
5. Let R be a commutative ring and assume that the polynomial ring $R[x]$ is a *p.i.d.* Prove that R is, in fact, a field.
6. An integral domain R such that every non-unit $a \in R$ can be factored into irreducibles is called an *atomic domain*. Prove that every Noetherian domain is atomic. (This factorization might not be unique, however. Note that the converse is not true: see *Exercise* 11 of *Section* 3.2 and *Exercise* 3, above.)
7. Show that in the ring $R = \mathbb{Z}[\sqrt{-5}]$, the ideal $P = (3, 4 + \sqrt{-5}) \subseteq R$ is a non-principal prime ideal.
8. Let R be a Noetherian ring in which every pair of elements has a greatest common divisor. Prove that R is a *u.f.d.* (Use *Exercise* 6 above and *Exercise* 7 of *Section* 3.2.)
9. Let R be a *p.i.d.*
   (a) If $a, b \in R$, with $d =$ g.c.d.(a, b), show that there exist $r, s \in R$, such that $ra + sb = d$.
   (b) If $a, b \in R$ with $q =$ l.c.m.(a, b), show that $(q) = (a) \cap (b)$.
   (c) Show that $((a) + (b))((a) \cap (b)) = (a)(b)$.
   (d) Which of the above are true if R is only assumed to be a *u.f.d.*?

10. Let R be a *u.f.d.* and assume that whenever $a, b \in R$ and are relatively prime, then there exist elements $s, t \in R$ with $sa + tb = 1$. Prove that every finitely generated ideal in R is principal. [1] In particular, if R is Noetherian, then R is a *p.i.d.* (Hint: Let $I \subseteq R$ be an ideal and let $a, b \in I$. Let d be the greatest common divisor of a and b; thus if $a' = a/d$ and $b' = b/d$ then a' and b' are relatively prime. Use the condition to show that $(a, b) = (d)$. Now use induction.)

11. Let R be a Noetherian ring and let $Q \subseteq R$ be a primary ideal (see *Exercise* 11 of *Section* 3.1). If $IJ \subseteq Q$ and $I \not\subseteq Q$, then there exists $n \geq 1$ such that $J^n \subseteq Q$.

12. Let R be a Noetherian ring and let $Q \subseteq R$ be a P-primary ideal (see *Exercise* 11a of *Section* 3.1). Show that there exists some $n \geq 1$ such that $P^n \subseteq Q$.

[1] It is interesting to note that a slight variant of this result applies to the ring $\mathcal{O}(\mathbb{C})$, introduced in *Exercise* 8 of *Section* 3.2, despite the fact that $\mathcal{O}(\mathbb{C})$ is not a *u.f.d.* The relevant result is that if f, g are two holomorphic functions on $\mathbb{C}$ with no common zeros, then there exist holomorphic functions s, t satisfying $sf + tg = 1$, identically on $\mathbb{C}$. From this fact, the reader should have no difficulty in showing that finitely generated ideals in $\mathcal{O}(\mathbb{C})$ are principal. For details, consult R.B. Burckel's *An Introduction to Classical Complex Analysis*, Vol. 1, Birkhäuser, Basel and Stuttgart, 1979, *Corollary* 11.42, *p.* 393.

3.4 Principal Ideal Domains and Euclidean Domains

Let R be an integral domain, and let $d : R - \{0\} \to \mathbb{N} \cup \{0\}$ be a function satisfying the so-called *division algorithm*

Given $a, b \in R,\ a \neq 0$, there exist $q, r \in R$ such that $b = qa + r$ and either $r = 0$ or $d(r) < d(a)$.

If the above holds we say that R (or more precisely the pair (R, d)) is a *Euclidean domain*. The function d is often called an *algorithm* . It is possible for a Euclidean domain to have more than one algorithm; see *Exercises* 7, 9. Furthermore, we have not insisted that the elements q (*quotient*) and r (*remainder*) are unique. However, this is the case in the following two prototypical examples below:

(i) $R = \mathbb{Z},\ d(n) = |n|$.

(ii) $R = \mathbb{F}[x]$, where $\mathbb{F}$ is a field, and $d(f(x)) = \deg f(x)$.

There are others; see *Exercises* 1, 4.

In most textbook treatments of Euclidean domains, one requires the algorithm d to satisfy a submultiplicativity condition:

$$d(a) \leq d(ab) \text{ for all } a, b \in R - \{0\}.$$

Such an algorithm is called a *submultiplicative algorithm*; this assumption is unnecessary; see *Exercise* 6, below.

As I remarked in *Section* 3.3, these domains are *p.i.d.*'s:

THEOREM 3.4.1 *If R is a Euclidean domain, then R is a principal ideal domain.*

From *Theorem* 3.3.4, *Section* 3.3, we conclude the following.

THEOREM 3.4.2 (FUNDAMENTAL THEOREM OF ARITHMETIC) $\mathbb{Z}$ *is a* u.f.d.

Finding principal ideal domains which are not Euclidean domains is tricky. Here's an example. (For details, see Larry Grove, *Algebra*, Academic Press, New York, 1983, *pages* 63, 66.) Let

$$R = \{(a + b\sqrt{-19})/2 |\ a, b \in \mathbb{Z},\ a \equiv b (\text{mod } 2)\}.$$

Then R is a *p.i.d.* but is not Euclidean. (If you are wondering about the "2" in the denominators of elements of R, good! In the next chapter we'll see that nature forces this on us.)

Exercises

1. The ring of *Gaussian integers* is defined by setting $R = \{a + bi |\ a, b \in \mathbb{Z}\}$. If we set $d(a + bi) = a^2 + b^2$, show that d gives R the structure of a Euclidean domain. (Hint: Let $a, b \in R, a \neq 0$. Do the division in the field $\mathbb{Q}[i]$; say
$$\frac{b}{a} \ = \ h \ + \ ki, \quad h, k \in \mathbb{Q}.$$
Now choose integers x, y such that $|x - h|, |y - k| \leq \frac{1}{2}$, and set $q = x + yi,\ r = b - qa$. Show that $d(r) \leq \frac{1}{2} d(a)$.) Note that relative to the algorithm d, quotient and remainder need not be unique.

2. The above method can actually be used to prove that the domain $R = \{a + b\sqrt{n} |\ a, b \in \mathbb{Z}\},\ n = -2, -1, 2, 3$ is a Euclidean domain. Prove this.

3. Express the following ideal as principal ideals:
   (a) $(3 + i) + (7 + i) \subseteq \mathbb{Z}[i]$.
   (b) $\{4a + 2b\sqrt{2} |\ a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}[\sqrt{2}]$.

4. Let $\zeta = e^{2\pi i/3}$. Show that the domain $R = \{a + b\zeta |\ a, b \in \mathbb{Z}\}$ is Euclidean.

5. Prove that $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1)$.

6. Let (R, d) be a Euclidean domain. Define a new function $d' : R - \{0\} \to N \cup \{0\}$ by setting
$$d'(r) \ = \ \min_{s \in Rr - \{0\}} d(s), \quad r \in R.$$
Prove that d' is a submultiplicative algorithm.

7. Consider the following function on the ring $\mathbb{Z}$ of integers.
$$d(n) \ = \ \begin{cases} |n| & \text{if } n \neq 1 \\ 2 & \text{if } n = 1 \end{cases}$$
Prove that d is a non-submultiplicative algorithm on $\mathbb{Z}$.

8. Let R be an integral domain, and define subsets $R_i,\ i = 0, 1, \ldots$ inductively, as follows:

   (i) $R_0 = \{0\}$.

   (ii) If $i > 0$ set $R_i' = \cup_{j<i} R_j$. Define

   $$R_i \ = \ \{0\} \cup \{r \in R |\ R_i' \to R/(r) \text{ is surjective}\}.$$

   Prove that R is Euclidean if and only if $R = \cup_{i \geq 0} R_i$, in which case we can take $d(r) = i$ if and only if $r \in R_i - R_i'$. (For a detailed discussion of the above result, see P. Samuel, *About Euclidean rings*, J. Algebra, **19**, 282-301 (1971).)

9. Let $R = \mathbb{Z}$, the ring of integers. Show that the map d, constructed as in *Exercise* 8 above is given by

   $$d(n) \ = \ \text{number of binary digits of } |n|.$$

10. This exercise contains an algorithm similar to that of *Exercise* 8 (for details, see T. Motzkin, *The Euclidean algorithm*, Bull. Amer. Math. Soc. **55**, 1142-1146 (1949)). Define subsets $R^i,\ i = 0, 1, \ldots$ inductively, as follows:

    (i) $R^0 = R - \{0\}$.

    (ii) If $i > 0$ set

    $$R^{i+1} = \{r \in R^i |\ \text{there exists } a \in R \text{ with } a + Rr \subseteq R^i\}.$$

    Prove that R is Euclidean if and only if $\cap_{i \geq 0} R^i = \emptyset$, in which case we can take $d(r) = i$ if and only if $r \in R^i - R^{i+1}$.

11. Let $R = \mathbb{Z}$, the ring of integers. Show that the map d, constructed as in *Exercise* 8 above is given by

    $$d(n) \ = \ \text{number of binary digits of } |n|.$$

Chapter 4

Dedekind Domains

4.1 A Few Remarks About Module Theory

Although we won't embark on a systematic study of modules until *Chapter* 5, it will be quite useful for us to gather together a few elementary results concerning modules for our immediate use.

We start with the appropriate definitions. Let R be a ring (with identity 1) and let M be an abelian group, written additively. Suppose we have a map $R \times M \to M$, written as scalar multiplication $(r, m) \mapsto r \cdot m$ (or just rm), satisfying

(i) $(r_1 + r_2)m = r_1 m + r_2 m$;

(ii) $(r_1 r_2)m = r_1(r_2 m)$;

(iii) $r(m_1 + m_2) = rm_1 + rm_2$;

(iv) $1 \cdot m = m$,

for all $r, r_1, r_2 \in R$, and all $m, m_1, m_2 \in M$. Then we say that M has the structure of a *left* R-module. Naturally, one can analogously define the concept of a *right* R-module (scalar multiplications are on the right). In case R is a commutative ring (as it shall be throughout this chapter) any left R-module M can be made into a right R-module simply by defining $m \cdot r = r \cdot m,\ r \in R,\ m \in M$. (If R is not commutative, one can't be so simple-minded; why?) For the remainder of this chapter since we'll be dealing exclusively with commutative rings, we shall simply use the term

"module" without saying "left" or "right," since the above shows that it doesn't matter whether we apply scalar multiplication on the left or on the right.

The reader will immediately see that an R-module is just like a vector space, except that the field of scalars is replaced by an arbitrary ring. However, this comparison is a bit misleading, as vector spaces are really quite special, with many linear algebraic questions being reducible to questions about bases and/or dimension. In general, modules don't have bases, so a more delicate approach to the theory is necessary.

For now, the most important example of a module over a commutative ring R is obtained as any ideal $I \subseteq R$. While this may seem a bit trite, this viewpoint will eventually pay great dividends.

If M is an R-module and $N \subseteq M$, then N is said to be an R-submodule of M if it is closed addition and under the R-scalar multiplications. If $S \subseteq M$ is a subset of M, we may set

$$R\langle S\rangle \ = \ \{\sum r_i s_i |\ r_1 \in M,\ s_i \in S\};$$

note that $R\langle S\rangle$ is a submodule of M, called the *submodule of M generated by S*. If $N \subseteq M$ is a submodule of the form $N = R\langle S\rangle$ for some *finite* subseteq $S \subseteq M$, then we say that N is a *finitely generated submodule* of M.

A map $\phi : M_1 \to M_2$ of R-modules is called a *module homomorphism* if ϕ is a homomorphism of the underlying abelian groups and if $\phi(rm) = r\phi(m)$, for all $r \in R$ and all $m \in M$. If $\phi : M_1 \to M_2$ is a homomorphism of R-modules, and if we set $\ker \phi = \{m \in M_1 |\ \phi(m) = 0\}$, then $\ker \phi$ is a submodule of M_1. Similarly, one defines the image $\text{im } \phi$ in the obvious way as a submodule of M_2. In analogy with group theory, if $K \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is a sequence of homomorphisms of R-modules, we say that the sequence is *exact* (at M) if $\text{im } \alpha = \ker \beta$. An exact sequence of the form $0 \to K \to M \to N \to 0$, is called a *short exact sequence* . Note that if M_1, M_2 are R-modules, and if we define the *external direct sum* $M_1 \oplus M_2$ is the obvious way, then there is always a short exact sequence of the form

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0.$$

If M is an R-module, and if $N \subseteq M$ is a submodule of M, we may give the quotient group M/N the structure of an R-module exactly as in linear algebra: $r \cdot (m + N) = r \cdot m + N,\ r \in R,\ m \in M$. The reader should have no difficulty in verifying that the scalar multiplication so defined, is well-defined and that it gives M/N the structure of an R-module.

The following simple result turns out to be quite useful.

LEMMA 4.1.1 (MODULAR LAW) *Let R be a ring, and let M be an R-module. Assume that M_1, M_2 and N are submodules of M with $M_1 \supseteq M_2$. Then*

$$M_2 + (N \cap M_1) \;=\; (M_2 + N) \cap M_1.$$

In analogy with ring theory, an R-module M is said to be *Noetherian* if whenever we have a chain

$$M_1 \subseteq M_2 \subseteq \cdots$$

of submodules, then there exists an integer N such that if $n \geq N$, then $M_n = M_N$. Note that if R is a Noetherian ring, regarded as a module over itself in the obvious way, then R is a Noetherian R-module. The following lemma is a direct generalization of *Theorem* 3.3.1 of *Chapter* 3.

PROPOSITION 4.1.2 *Let R be a ring, and let M be an R-module. The following are equivalent for M.*

(i) M is Noetherian.

(ii) Every submodule of M is finitely generated.

(iii) If $\mathcal{S}$ is any collection of submodules of M, then $\mathcal{S}$ contains a maximal element with respect to inclusion.

PROPOSITION 4.1.3 *Let $0 \to K \to M \to N \to 0$ be a short exact sequence of R-modules. Then M is Noetherian if and only if K and N both are.*

COROLLARY 4.1.3.1 *Let R be a Noetherian ring, and let M be a finitely generated R-module. Then M is Noetherian.*

Exercises

1. Let R be a commutative ring and let M be an R-module. Set

$$\mathrm{Ann}_R(M) \;=\; \{r \in R |\; rM = 0\}.$$

(Note that $\mathrm{Ann}_R(M)$ is an ideal of R.) Prove that the following two conditions are equivalent for the R-module M.

(i) $\mathrm{Ann}_R(N) = \mathrm{Ann}_R(M)$ for all submodules $N \subseteq M,\ N \neq 0$.

(ii) $IN = 0 \Rightarrow IM = 0$ for all submodules $N \subseteq M, N \neq 0$, and all ideals $I \subseteq R$. (Here, if $I \subseteq R$ is an ideal, and if M is an R-module, $IM = \{\text{finite sums } \sum s_i m_i |\ s_i \in I,\ m_i \in M\}$.)

A module satisfying either of the above conditions is called a *prime module*.

2. (i) Show that if $P \subseteq R$ is an ideal, then P is a prime ideal $\iff$ R/P is a prime module.

   (ii) Show that if M is a prime module then $\mathrm{Ann}_R(M)$ is a prime ideal.

3. Let M be a Noetherian R-module, and suppose that $\phi : M \to M$ is a surjective R-module homomorphism. Show that ϕ is injective. (Hint: for each $n > 0$, let $K_n = \ker \phi^n$. Then we have an ascending chain $K_0 \subseteq K_1 \subseteq \cdots$ of R-submodules of M. Thus, for some positive integer k, $K_k = K_{k+1}$. Now let $a \in K_1 = \ker \phi$. Since $\phi : M \to M$ is surjective, so is $\phi^k : M \to M$. So $a = \phi^k(b)$, for some $b \in M$. Now what? Incidently, the above result remains valid without assuming that R is Noetherian; one only needs that R is commutative, see *Lemma* 5.2.8 of *Section* 5, below.)

4. Let R be a ring and let M be an R-module. If $N \subseteq M$ is an R-submodule, and if $N,\ M/N$ are finitely generated, show that M is finitely generated.

5. Let M be an R-module, and let $M_1, M_2 \subseteq M$ be submodules. If $M = M_1 + M_2$ with $M_1 \cap M_2 = 0$, we say that M is the *internal direct sum* of M_1 and M_2. In this case, prove that the map $M_1 \oplus M_2 \to M$, $(m_1, m_2) \mapsto m_1 + m_2$ is an isomorphism.

6. Let $0 \to K \xrightarrow{\mu} M \to N \to 0$ be a short exact sequence of R-modules. Say that the short exact sequence *splits* if M can be expressed as an internal direct sum of the form $M = \mu K + M'$ for some submodule $M' \subseteq M$. Show that in this case $M' \cong N$, and so $M \cong K \oplus N$.

7. $0 \to K \xrightarrow{\mu} M \xrightarrow{\epsilon} N \to 0$ be a short exact sequence of R-modules. Prove that the following conditions are equivalent:

   (a) $0 \to K \xrightarrow{\mu} M \xrightarrow{\epsilon} N \to 0$ splits;

(b) There exists a module homomorphism $r : M \to K$ such that $r \circ \mu = 1_K$;

(c) There exists a module homomorphism $\rho : N \to M$ such that $\epsilon \circ \rho = 1_N$.

8. Let M be an R-module and assume that there is a short exact sequence of the form $0 \to K \to M \to R \to 0$. Show that this short exact sequence splits.

4.2 Algebraic Integer Domains

Let $\alpha \in \mathbb{C}$ be an algebraic number. If α satisfies a monic polynomial with integral coefficients, then α is called an *algebraic integer* . More generally, suppose that $R \subseteq S$ are integral domains and that $\alpha \in S$. Say that α is *integral* over R if α satisfies a monic polynomial in $R[x]$. Thus, the algebraic integers are precisely the complex numbers which are integral over $\mathbb{Z}$.

LEMMA 4.2.1 *Let $R \subseteq S$ be integral domains, and let $\alpha \in S$. Then α is integral over R if and only if $R[\alpha]$ is a finitely generated R-module.*

Note that the proof of the above actually reveals the following.:

LEMMA 4.2.2 *Let $R \subseteq S$ be integral domains. If S is a finitely generated R-module, then every element of S is integral over R.*

LEMMA 4.2.3 *Let $R \subset S \subset T$ be integral domains. If T is a finitely generated S-module, and if S is a finitely generated R-module, then T is a finitely generated R-module.*

As an immediate consequence we have the following proposition.

PROPOSITION 4.2.4 *Let α, β be algebraic integers. Then $\alpha\beta$ and $\alpha + \beta$ are also algebraic integers.*

One could consider the ring $\mathbb{Z}_{\text{alg}} \subseteq \mathbb{C}$ of all algebraic integers. However, this ring doesn't have very interesting factorization properties. For example, $\mathbb{Z}_{\text{alg}}$ has no primes. Indeed, if $a \in \mathbb{Z}_{\text{alg}}$, then $\sqrt{a} \in \mathbb{Z}_{\text{alg}}$. Rather than considering *all* algebraic integers, it is more appropriate to consider the following subrings of $\mathbb{Z}_{\text{alg}}$.

Definition. Let $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{C}$, where $[\mathbb{E} : \mathbb{Q}] < \infty$. Set

$$\mathcal{O}_{\mathbb{E}} = \{\text{algebraic integers } \alpha | \alpha \in \mathbb{E}\} = \mathbb{E} \cap \mathbb{Z}_{\text{alg}}.$$

Call the ring $\mathcal{O}_{\mathbb{E}}$ an *algebraic integer domain.*

Definition. Let R be an arbitrary integral domain. Say that R is *integrally closed* if, whevever $\alpha \in \mathcal{F}(R)$ and α is integral over R, then $\alpha \in R$. Here $\mathcal{F}(R)$ is the field of fractions of the integral domain R.

The following is a sufficient, but not a necessary condition for an integral domain to be integrally closed.

LEMMA 4.2.5 *If R is a* u.f.d.*, then R is integrally closed.*

PROPOSITION 4.2.6 *Let $\mathbb{E}$ be a field with $[\mathbb{E} : \mathbb{Q}] < \infty$, and set $R = \mathcal{O}_{\mathbb{E}}$.*

(a) If $\alpha \in \mathbb{E}$, then $n\alpha \in R$, for some $n \in \mathbb{Z}$.

(b) $\mathcal{F}(R) = \mathbb{E}$.

(c) R is integrally closed.

(d) $R \cap \mathbb{Q} = \mathbb{Z}$.

An important class of algebraic integer domains are the *quadratic integer domains* , defined as the domains of the form $\mathcal{O}_{\mathbb{E}}$, where $[\mathbb{E} : \mathbb{Q}] = 2$. We'll simplify the notation slightly, as follows. First note that $\mathbb{E} = \mathbb{Q}[\sqrt{m}]$, where m is a *square-free* integer. Thus, denote $\mathbb{Q}_m = \mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$.

PROPOSITION 4.2.7

$$\mathbb{Q}_m = \begin{cases} \{a + b\sqrt{m} |\ a, b \in \mathbb{Z}\} & \text{if } m \not\equiv 1 (mod\ 4) \\ \{\frac{a+b\sqrt{m}}{2} |\ a, b \in \mathbb{Z}, a \equiv b (mod\ 2)\} & \text{if } m \equiv 1 (mod\ 4) \end{cases}$$

Notice that the above proposition, together with *Lemma* 5, readily identifies many integral domains which cannot possibly be *u.f.d.*'s. Indeed, if m is square-free and satisfies $m \equiv 1 (mod\ 4)$, then the ring

$$R' = \{a + b\sqrt{m} | a, b \in \mathbb{Z}\}$$

is properly contained in $R = \mathbb{Q}_m$, and yet it is clear that $\mathcal{F}(R') = \mathcal{F}(R)$. Thus R' is not integrally closed and hence cannot be a *u.f.d.*

Perhaps unfortunately, not all quadratic integer domains are *u.f.d.*'s. The simplest example is the ring $R = \mathbb{Q}_{-5}$, which by the above proposition is simply the ring

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}.$$

We already observed in *Chapter* 3 that R is not a *u.f.d.*

Unsolved Problem: *Are there finitely or infinitely many real quadratic integer domains which are also* u.f.d*'s?*

In the next section we'll see that an algebraic integer domain is a *p.i.d* if and only if it is a *u.f.d.*

Exercises

1. Let $\mathbb{F}$ be a field and let x be indeterminate over $\mathbb{F}$. Prove that the ring $R = \mathbb{F}[x^2, x^3]$ is not integrally closed, hence is not a *u.f.d.*. (*C.f. Exercise* 3 of *Section* 3.2.)
2. Prove the above assertion that if a is an algebraic integer, so is $\sqrt{a}$.
3. Let $[\mathbb{E} : \mathbb{Q}] < \infty$, and set $G = Gal(\mathbb{E}/\mathbb{Q})$. If $a \in \mathcal{O}_{\mathbb{E}}$, and if $\tau \in G$, then $\tau(a) \in \mathcal{O}_{\mathbb{E}}$.
4. Show that $\mathbb{Q}_{-6}$ is not a *u.f.d.*.
5. Let $\alpha \in \mathbb{C}$, and assume that $f(\alpha) = 0$, for some monic polynomial $f(x) \in \mathbb{Z}[x]$. Prove that α is an algebraic integer.
6. Here's another proof of the fact that if α, β are algebraic integers, so are $\alpha + \beta$ and $\alpha\beta$. Let $f(x), g(x)$ be the minimal polynomials of α, β, respectively. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ be the roots of $f(x)$, and let $\beta_1 = \beta, \beta_2, \ldots, \beta_s$ be the roots of $g(x)$. If we set

$$h(x) \ = \ \prod_{j=i}^{s} f(x - \beta_j),$$

then argue that $h(x)$ is a monic polynomial $\mathbb{Z}[x]$. Then show that $h(\alpha + \beta) = 0$. Apply *Exercise* 5, above. Give a similar argument to show that $\alpha\beta$ is also an algebraic integer.

7. Show that if $m > 0$, and is square-free, then $U(\mathbb{Q}_m)$ is infinite.

8. ** Let $\zeta \in \mathbb{C}$ be a primitive n-th root of unity, and let $\mathbb{E} = \mathbb{Q}[\zeta]$. Show that $\mathcal{O}_{\mathbb{E}} = \mathbb{Z}[\zeta]$. (You probably won't get this one but give it a little thought. You should at least see how *Proposition* 4.2.7 above makes this statement true for $n = 3$.)

9. As we have seen, the ring $\mathbb{Q}_{-5} = \mathbb{Z}[\sqrt{-5}]$ is not a u.f.d. Many odd things happen in this ring. For instance, find an example of an irreducible element $\pi \in \mathbb{Z}[\sqrt{-5}]$ and an element $a \in \mathbb{Z}[\sqrt{-5}]$ such that π doesn't divide a, but π divides a^2. (Hint: look at factorizations of $9 = 3^2$.)

10. The following result is well-known to virtually every college student. Let $f(x) \in \mathbb{Z}[x]$, and let $\frac{a}{b}$ be a rational root of $f(x)$. If the fraction $\frac{a}{b}$ is in lowest terms, then a divides the constant term of $f(x)$ and b divides the leading coefficient of $f(x)$. If we ask the same question in the context of the ring $\mathbb{Z}[\sqrt{-5}]$, then the answer is negative. Indeed if we consider the polynomial $f(x) = 3x^2 - 2\sqrt{-5}x - 3 \in \mathbb{Z}[\sqrt{-5}]$, then the roots are $\frac{2+\sqrt{-5}}{3}$ and $\frac{-2+\sqrt{-5}}{3}$. Since both 3 and $\pm 2 + \sqrt{-5}$ are non-associated irreducible elements, then the fractions can be considered to be in lowest terms. Yet neither of the numerators divide the constant term of $f(x)$.

11. We continue on the theme set in *Exercise* 10, above. Let R be an integral domain with field of fractions $\mathcal{F}(R)$. Assume the following condition on the domain R: Let $f(x) = a_n x^n + \cdots + a_0 \in R[x]$, with $a_0, a_n \neq 0$, and assume that $\frac{a}{b} \in \mathcal{F}(R)$ is a fraction in lowest terms (i.e., no common non-unit factors) satisfying the polynomial $f(x)$. Then a divides a_0 and b divides a_n. Now prove that for such a ring every irreducible element is actually prime. (Hint: Let $\pi \in R$ be an irreducible element and assume that $\pi | uv$, but that π doesn't divide either u or v. Let $uv = r\pi,\ r \in R$, and consider the polynomial $ux^2 - (\pi + r)x + v \in R[x]$.)

12. Let $\mathbb{K}$ be a field such that $\mathbb{K}$ is the field of fractions of both $R_1, R_2 \subseteq \mathbb{K}$. Must it be true that $\mathbb{K}$ is the field of fractions of $R_1 \cap R_2$? (Hint: A counter-example can be found in the field $\mathbb{K} = \mathbb{F}(x)$.)

13. Let $\mathbb{Q} \subseteq \mathbb{K}$ be a finite algebraic extension. If $\mathbb{K}$ is the field of fractions of $R_1, R_2 \subseteq \mathbb{K}$, prove that $\mathbb{K}$ is also the field of fractions of $R_1 \cap R_2$.

14. Again, let $\mathbb{Q} \subseteq \mathbb{K}$ be a finite algebraic extension. This time, let $\{R_\alpha |\ \alpha \in \mathcal{A}\}$ consist of the subrings of $\mathbb{K}$ having $\mathbb{K}$ as field of fractions. Show that $\mathbb{K}$ is *not* the field of fractions of $\cap_{\alpha\in\mathcal{A}} R_\alpha$. (In fact, $\cap_{\alpha\in\mathcal{A}} R_\alpha = \mathbb{Z}$.)

4.3 $\mathcal{O}_{\mathbb{E}}$ is a Dedekind Domain

Definition. Let R be an integral domain. We say that R is a *Dedekind domain* if

(a) R is Noetherian,

(b) Every prime ideal of R is maximal, and

(c) R is integrally closed.

Thus, it follows immediately that every *p.i.d* is a Dedekind domain.

For the remainder of this section, let $[\mathbb{E} : \mathbb{Q}] < \infty$, and set $R = \mathcal{O}_{\mathbb{E}}$.

Lemma 4.3.1

(a) There exists $\alpha \in R$ such that $\mathbb{E} = \mathbb{Q}[\alpha]$.

(b) If α is as above and if $R_0 = \mathbb{Z}[\alpha]$, then there exists $d \in \mathbb{Z}$ with $d \cdot R \subseteq R_0$.

Proposition 4.3.2 *R is Noetherian.*

Proposition 4.3.3 *Every prime ideal of R is maximal.*

Corollary 4.3.3.1 *R is a Dedekind domain.*

Because of *Exercise* 4 of *Section* 3.3, we have the following result, promised in *Section* 4.2.

Corollary 4.3.3.2 *The algebraic integer domain R is a* p.i.d. *if and only if R is a* u.f.d..

4.4 Factorization Theory in Dedekind Domains and the Fundamental Theorem of Algebraic Number Theory

For the first three lemmas, assume that R is an arbitrary Dedekind domain.

LEMMA 4.4.1 *Assume that $P_1, P_2, \cdots, P_r, P$ are prime ideals in R with*

$$P_1 P_2 \cdots P_r \subseteq P.$$

Then $P = P_i$ for some i.

LEMMA 4.4.2 *Any ideal of R contains a product of prime ideals.*

Definition. Let R be a Dedekind domain. If $I \subseteq R$ is an ideal, we set

$$I^{-1} = \{\alpha \in \mathbb{E} |\ \alpha \cdot I \subseteq R\}.$$

Note that $R^{-1} = R$, for if $\alpha \cdot R \subseteq R$, then $\alpha = \alpha \cdot 1 \in R$. Next note that $I \subseteq J$ implies that $I^{-1} \supseteq J^{-1}$.

LEMMA 4.4.3 *If I is a proper ideal of R, then I^{-1} properly contains R.*

LEMMA 4.4.4 *If $I \subseteq R$ is an ideal then I^{-1} is a finitely generated R-module.*

PROPOSITION 4.4.5 *If $I \subseteq R$ is an ideal, then $I^{-1}I = R$.*

COROLLARY 4.4.5.1 *If $I, J \subseteq R$ are ideals, then $(IJ)^{-1} = I^{-1}J^{-1}$.*

The following theorem gives us basic factorization theory in a Dedekind domain.

THEOREM 4.4.6 *Let R be a Dedekind domain and let $I \subseteq R$ be an ideal. Then there exist prime ideals $P_1, P_2, \cdots, P_r \subseteq R$ such that*

$$I = P_1 P_2 \cdots P_r.$$

The above factorization is unique in that if also

$$I = Q_1 Q_2 \cdots Q_s,$$

where the Q_i's are prime ideals, then $r = s$ and $Q_i = P_{\pi(i)}$, for some permutation π of $1, 2, \cdots, r$.

The following theorem sometimes is called the *Fundamental Theorem of Algebraic Number Theory.*

COROLLARY 4.4.6.1 (FUNDAMENTAL THEOREM OF ALGEBRAIC NUMBER THEORY) *Let $\mathbb{E} \supseteq \mathbb{Q}$ be a finite field extension and let $R = \mathcal{O}_{\mathbb{E}}$. Then any ideal of R can be uniquely factored as a product of prime ideals.*

From the Fundamental Theorem of Algebraic Number Theory, we conclude that if $I,\ J \subseteq R$ are ideals that *share no prime ideal factors*, then it must happen that $I + J = R$, *i.e.*, the ideals $I,\ J$ are relatively prime. In particular let $I \subseteq R$ be an ideal and and factor I into a product of distinct prime ideals: $I = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$. Let $\alpha_i \in P_i^{e_i} - P_{i+1}^{e_i+1},\ i = 1, 2 \ldots, r$. Since $P_1^{e_1}, P_2^{e_2} \ldots, P_r^{e_r}$ are pairwise relatively prime, by the *Chinese Remainder Theorem* (see *Exercise* 7 of *Section* 3.1) there exists an element $\alpha \in R$ satisfying $\alpha \cong \alpha_i \bmod P_{i+1}^{e_i+1},\ i = 1, 2, \ldots, R$. Note that in particular $\alpha \in P_1^{e_1} \cap P_2^{e_2} \cap \cdots \cap P_r^{e_r} = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$ (see *Exercise* 2, below). This implies that if we factor the principal ideal (α) into a product of prime ideals, then we have $(\alpha) = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r} \cdot J$ where J is divisible by none of the prime ideals $P_1, P_2, \ldots, P_r$. In other words, we have a factorization $(\alpha) = IJ$, where $I,\ J$ are relatively prime.

Next, write $J = Q_1^{f_1} Q_2^{f_2} \cdots Q_s^{f_s}$; from the above we may infer that $I \not\subseteq Q_i,\ i = 1, 2, \ldots, s$, and so by *Exercise* 9 of *Section* 3.1 we may conclude that $I \not\subseteq Q_1 \cup Q_2 \cup \cdots \cup Q_s$. Now choose an element $\beta \in I - (Q_1 \cup Q_2 \cup \cdots \cup Q_s)$. Therefore the ideal $(\alpha, \beta) \subseteq R$ generated by α and β satisfies $(\alpha) \subseteq (\alpha, \beta) \subseteq I$. However, since $(\alpha, \beta) \not\subseteq Q_i,\ i = 1, 2 =, \ldots, s$, we may infer that in fact, $(\alpha, \beta) = I$. This proves the following:

PROPOSITION 4.4.7 *Let $\mathbb{E} \supseteq \mathbb{Q}$ be a finite field extension and let $R = \mathcal{O}_{\mathbb{E}}$. Then any ideal $I \subseteq R$ can be expressed as $I = (\alpha, \beta)$ for suitable elements $\alpha, \beta \in I$.*

Exercises

1. Let $\mathbb{E}$ be a finite extension of the rational field $\mathbb{Q}$, and set $R = \mathcal{O}_{\mathbb{E}}$. Let P be a prime ideal of R, and assume that $P \cap \mathbb{Z} = (p)$, for some prime number p. Show that we may regard $\mathbb{Z}/(p)$ as a subfield of R/P, and

that $[R/P : \mathbb{Z}/(p)] \leq [\mathbb{E} : \mathbb{Q}]$, with equality if and only if p remains prime in $\mathcal{O}_{\mathbb{E}}$.

2. Assume that R is a Dedekind domain and that $I = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$, $J = P_1^{f_1} P_2^{f_2} \cdots P_r^{f_r}$. Show that

$$I+J = P_1^{\min\{e_1,f_1\}} \cdots P_r^{\min\{e_r,f_r\}}, \ I \cap J = P_1^{\max\{e_1,f_1\}} \cdots P_r^{\max\{e_r,f_r\}}.$$

Conclude that $AB = (A+B)(A \cap B)$.

3. Let R be a Dedekind domain in which every prime ideal is principal. Prove that R is a *p.i.d.*

4. In the Dedekind domain $R = \mathbb{Z}[\sqrt{-5}]$ show that $(3) = (3, 4+\sqrt{-5})(3, 4-\sqrt{-5})$ is the factorization of the principal ideal (3) into a product of prime ideals.

4.5 The Ideal Class Group of a Dedekind Domain

We continue to assume that R is a Dedekind domain, with fraction field $\mathbb{E}$. An R-submodule $B \subseteq \mathbb{E}$ is called a *fractional ideal* if it is a finitely generated module.

LEMMA 4.5.1 *Let B be a fractional ideal. Then there exist prime ideals $P_1, P_2, \ldots, P_r, Q_1, Q_2, \ldots, Q_s$ such that $B = RP_1P_2\cdots P_rQ_1^{-1}Q_2^{-1}\cdots Q_s^{-1}$. (It is possible for either $r = 0$ or $s = 0$.)*

COROLLARY 4.5.1.1 *The set of fractional ideals in $\mathbb{E}$ forms an abelian group under multiplication.*

A fractional ideal $B \subseteq \mathbb{E}$ is called a *principal fractional ideal* if it is of the form $R\alpha$, for some $\alpha \in \mathbb{E}$. Note that in this case, $B^{-1} = R(\frac{1}{\alpha})$. It is easy to show that if R is a principal ideal domain, then every fractional ideal is principal (*Exercise* 1).

If $\mathcal{F}$ is the set of fractional ideals in $\mathbb{E}$ we have seen that $\mathcal{F}$ is an abelian group under multiplication, with identity R. If we denote by $\mathcal{P}$ the set of principal fractional ideals, then it is easy to see that $\mathcal{P}$ is a subgroup of $\mathcal{F}$; the quotient group $\mathcal{C} = \mathcal{F}/\mathcal{P}$ is called the *ideal class group* of R; it is trivial precisely when R is a principal ideal domain. If $R = \mathcal{O}_{\mathbb{E}}$ for a finite extension $\mathbb{E} \supseteq \mathbb{Q}$, then it is known that $\mathcal{C}$ is a finite group. The order $h = |\mathcal{C}|$ is called the *class number* of R (or of $\mathbb{E}$) and is a fundamental invariant in algebraic number theory.

Exercises

1. If R is a *p.i.d.,* prove that every fractional ideal of $\mathbb{E}$ is principal.
2. Let R be a Dedekind domain with fraction field $\mathbb{E}$. Prove that $\mathbb{E}$ itself is not a fractional ideal (except in the trivial case in which case R is a field to be begin with).
3. Let R be a Dedekind domain with ideal class group $\mathcal{C}$. Let $P \subseteq R$ be a prime ideal and assume that the order of the element $[P] \in \mathcal{C}$ is $k > 1$. If $P^k = (\pi)$, for some $\pi \in R$, show that π is irreducible but not prime.

4. Let R be a Dedekind domain with ideal class group of order at most 2. Prove that the number of irreducible factors in a factorization of an element $a \in R$ depends only on a.[1] (Hint: Note first that by *Exercise* 6 of *Section* 3.3, any non-unit of R can be factored into irreducibles. By induction on the minimal length of a factorization of $a \in R$ into irreducibles, we may assume that a has no prime factors. Next assume that $\pi \in R$ is a non-prime irreducible element. If we factor the principal ideal into prime ideals: $(\pi) = Q_1 Q_2 \cdots Q_r$ then the assumption guarantees that $Q_1 Q_2 = (\alpha)$, for some $\alpha \in R$. If $r > 2$, then (π) is properly contained in $Q_1 Q_2 = (\alpha)$ and so α is a proper divisor of π, a contradiction. Therefore, it follows that a principal ideal generated by a non-prime irreducible element factors into the product of two prime ideals. Now what?)

5. Let R be as above, *i.e.*, a Dedekind domain with ideal class group of order at most 2. Let $\pi_1, \pi_2 \in R$ be irreducible elements. As we seen in *Exercise* 4 above, any factorization of $\pi_1 \pi_2$ will involve exactly two irreducibles. Show that, up to associates, there can be at most three distinct factorizations of $\pi_1 \pi_2$ into irreducibles. (As a simple illustration, it turns out that the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$ has class group of order 2; correspondingly we have distinct factorizations: $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5})$.)

4.6 A Characterization of Dedekind Domains

In this final section we'll prove the converse of *Theorem* 4.4.6, thereby giving a characterization of Dedekind domains.

To begin with, let R be an arbitrary integral domain, with fraction field $\mathbb{E}$. In analogy with the preceeding section, if $I \subseteq R$ is an ideal, we set

$$I^{-1} = \{\alpha \in \mathbb{E} |\ \alpha I \subseteq R\}.$$

We say that I is *invertible* if $I^{-1} I = R$.

LEMMA 4.6.1 *Assume that $I \subseteq R$ and admits factorizations*

$$P_1 P_2 \cdots P_r = I = Q_1 Q_2 \cdots Q_s,$$

[1] See L. CARLITZ, A characterization of algebraic number fields with class number two, *Proc. Amer. Math. Soc.* **11** (1960), 391-392. In case R is the ring of integers in a finite extension of the rational field, Carlitz also proves the converse.

where the P_i's and the Q_j's are invertible prime ideals. Then $r = s$, and (possibly after re-indexing) $P_i = Q_i,\ i = 1, 2, \cdots, r$.

LEMMA 4.6.2 *Let R be an integral domain.*

(i) Any non-zero principal ideal is invertible.

(ii) If $0 \neq x \in R$, and if the principal ideal (x) factors into prime ideals as $(x) = P_1 P_2 \cdots P_r$, then each P_i is invertible.

Now assume that R is an integral domain satisying the following condition:

(*) If $I \subseteq R$ is an ideal of R, then there exist prime ideals $P_1, P_2, \cdots, P_r \subseteq R$ such that
$$I = P_1 P_2 \cdots P_r.$$

Note that no assumption is made regarding the uniqueness of the above factorization. We shall show that uniqueness automatically follows. (See *Corollary* 4.6.9.2 , below.) Of course, this is exactly analogous with what happens in unique factorization domains.

Our goal is to show that R is a Dedekind domain.

PROPOSITION 4.6.3 *Any invertible prime ideal of R is maximal.*

PROPOSITION 4.6.4 *Any prime ideal is invertible, hence maximal.*

COROLLARY 4.6.4.1 *Any ideal is invertible.*

COROLLARY 4.6.4.2 *Any ideal of R factors uniquely into prime ideals.*

PROPOSITION 4.6.5 *R is Noetherian.*

Our task of showing that R is a Dedekind domain will be complete as soon as we can show that R is integrally closed. To do this it is convenient to introduct certain "overrings" of R, described as below.

Let R be an arbitrary integral domain and let $\mathbb{E} = \mathcal{F}(R)$. If $P \subseteq R$ is a prime ideal of R we set
$$R_P = \{\alpha/\beta \in \mathbb{E} |\ \alpha, \beta \in R,\ \beta \notin P\}.$$

It should be clear (using the fact that P is a prime ideal) that R_P is a subring of $\mathbb{E}$ containing R. It should also be clear that $\mathcal{F}(R_P) = \mathbb{E}$. R_P is called the *localization* of R *at the prime ideal* P.

LEMMA 4.6.6 *Let I be an ideal of R, and let P be a prime ideal of R.*

(i) If $I \not\subseteq P$ then $R_P I = R_P$.

(ii) $R_P P^{-1}$ properly contains R_P.

LEMMA 4.6.7 *If $\alpha \in \mathbb{E}$ then either $\alpha \in R_P$ or $\alpha^{-1} \in R_P$.*

The following is now really quite trivial.

LEMMA 4.6.8 *R_P is integrally closed.*

PROPOSITION 4.6.9 *$R = \cap R_P$, the intersection taken over all prime ideals $P \subseteq R$.*

As an immediate result, we get

COROLLARY 4.6.9.1 *R is integrally closed.*

Combining all of the above we get the desired characterization of Dedekind domains:

COROLLARY 4.6.9.2 *R is a Dedekind domain if and only if every ideal of R can be factored into prime ideals.*

Exercises

1. A *valuation ring* is an integral domain R such that if I and J are ideals of R, then either $I \subseteq J$ or $J \subseteq I$. Prove that for an integral domain R, the following three conditions are equivalent:

   (i) R is a valuation ring.

   (ii) if $a, b \in R$, then either $(a) \subseteq (b)$ or $(b) \subseteq (a)$.

   (iii) If $\alpha \in \mathbb{E} := \mathcal{F}(R)$, then either $\alpha \in R$ or $\alpha^{-1} \in R$.

   (Thus, we see that the rings R_P, defined above, are valuation rings.)

2. Let R be a *Noetherian* valuation ring.

   (i) Prove that R is a *p.i.d.*

(ii) Prove that R contains a unique maximal ideal. (This is true even if R isn't Noetherian.)

(iii) Conclude that, up to units, R contains a unique prime element.

(A ring satisfying the above is often called a *discrete valuation ring* .)

3. Let R be a discrete valuation ring, as in *Exercise* 2, above, and let π be the prime, unique up to associates. Define $\nu(a) = r$, where $a = \pi^r b,\ \pi \not| \ b$. Prove that ν is an algorithm for R, giving R the structure of a Euclidean domain.

4. Let R be a Noetherian domain and let P be a prime ideal. Show that the localization R_P is Noetherian.

5. Let R be a ring in which every ideal $I \subseteq R$ is invertible. Prove that R is a Dedekind domain. (Hint: First, as in the proof of *Proposition* 4.6.5, R is Noetherian. Now let $\mathcal{C}$ be the set of all ideals that are not products of prime ideals. Since R is Noetherian, $\mathcal{C} \neq \emptyset$ implies that $\mathcal{C}$ has a maximal member J. Let $J \subseteq P$, where P is a maximal ideal. Clearly $J \neq P$. Then $JP^{-1} \subseteq PP^{-1} = R$ and so JP^{-1} is an ideal of R; clearly $J \subseteq JP^{-1}$. If $J = JP^{-1}$, then $JP^{-1} = P_1P_2 \cdots P_r$ so $J = PP_1P_2 \cdots P_r$. Thus $J = JP^{-1}$ so $JP = J$. This is a contradition, why?)

6. Here is an example of a non-invertible ideal in an integral domain R. Let
$$R \ = \ \{a + 3b\sqrt{-5} |\ a, b \in \mathbb{Z}\},$$
and let $I = (3, 3\sqrt{-5})$, i.e., I is the ideal generated by 3 and $3\sqrt{-5}$. Show that I is not invertible. (An easy way to do this is to let $J = (3)$, the principal ideal generated by 3, and observe that despite the fact that $I \neq J$, we have $I^2 = IJ$.)

Chapter 5

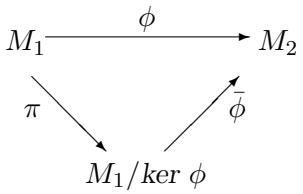
Module Theory

5.1 The Basic Homomorphism Theorems

In *Section* 4.1 we introduced some of the basics of module theory, as they were indespensible to our study of Dedekind domains. In the present chapter, we embark on a more systematic study of module theory; one very important difference here is that unless otherwise stated, the rings in question *need not be commutative.*

There are two basic homomorphism theorems worth mentioning here. The proofs are entirely routine and mimick the corresponding proofs for abelian groups (i.e.,$\mathbb{Z}$-modules).

THEOREM 5.1.1 (THE FUNDAMENTAL HOMOMORPHISM THEOREM) *Let R be a ring and let $\phi : M_1 \to M_2$ be a homomorphism of R-modules. Then ϕ admits a factorization, according to the commutative diagram below:*



where $\pi : M_1 \to M_1/ker\ \phi$ is the canonical projection, and where $\bar{\phi}(m_1 + ker\ \phi) = \phi(m_1),\ m_1 \in M_1$.

The next result is sometimes also called the *Second Isomorphism Theorem.*

THEOREM 5.1.2 (THE NOETHER ISOMORPHISM THEOREM) *Let R be a ring, and let M be an R-module. If $M_1,\ M_2$ are submodules of M, then*

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

At the risk of being repetitive, we'll state the modular law again, as it is a key ingredient in the "Third Isomorphism Theorem," below.

LEMMA 5.1.3 (MODULAR LAW) *Let R be a ring, and let M be an R-module. Assume that M_1, M_2 and N are submodules of M with $M_1 \supseteq M_2$. Then*

$$M_2 + (N \cap M_1) \ = \ (M_2 + N) \cap M_1.$$

The next result is considerably more esoteric and is variably called the *Butterfly Lemma, Third Isomorphism Theorem* or the *Zassenhaus Lemma.* This will be used in proving the Schreier Refinement Theorem; see *Proposition* 5.6.4, below.

THEOREM 5.1.4 *Let R be a ring, and let M be an R-module. Assume that we have submodules $N_2 \subseteq N_1 \subseteq M,\ M_2 \subseteq M_1 \subseteq M$. Then*

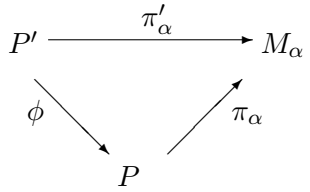
$$\frac{M_2 + (N_1 \cap M_1)}{M_2 + (N_2 \cap M_1)} \cong \frac{N_2 + (M_1 \cap N_1)}{N_2 + (M_2 \cap N_1)}.$$

Exercises

1. Let $K \subseteq M \subseteq N$ be R-modules. Prove that $(N/K)/(M/K) \cong N/M$.
2. Give examples of R-modules $M_1,\ M_2$ such that $M_1 \cong_{\mathbb{Z}} M_2$, but $M_1 \ncong_R M_2$.
3. Let M be an R-module and let $M_1 \subseteq M$ be a submodule. If $\phi : M \to N$ is a homomorphism of R-modules such that $\ker \phi \subseteq M_1$, prove that $M/M_1 \cong \phi M/\phi M_1$. Give a counterexample to show that this hypothesis is necessary.
4. Let R be a Dedekind domain with fraction field $\mathbb{E}$, and let $I, J \subseteq \mathbb{E}$ be fractional ideals representing classes $[I], [J] \in \mathcal{C}_R$, the ideal class group of R (See *Section* 4.5). If $[I] = [J]$, prove that $I \cong_R J$. (The converse is also true; see *Exercise* 12 of *Section* 7.2.)

5.2 Direct Products and Sums of Modules; Free Modules

Let $\{M_\alpha,\}_{\alpha\in\mathcal{A}}$ be a family of R-modules. Assume we are given a family $(P,\pi_\alpha)_{\alpha\in\mathcal{A}}$ consisting of an R-module P, and R-module homomorphisms $\pi_\alpha : P \to M_\alpha,\ \alpha\in\mathcal{A}$, satisfying the following universal property: If $(P',\pi'_\alpha)_{\alpha\in\mathcal{A}}$ is another family consisting of an R-module P' and R-module homomorphisms $\pi'_\alpha : P' \to M_\alpha,\ \alpha\in\mathcal{A}$, then there exists a unique R-module homomorphism $\phi : P' \to P$, making the triangle below commute, for each $\alpha\in\mathcal{A}$.



Then the family $(P,\pi_\alpha)_{\alpha\in\mathcal{A}}$ is called a *(direct) product* of the R-modules $M_\alpha,\ \alpha\in\mathcal{A}$. Sometimes we simplify the language a bit by simply calling P a direct product of the modules M_α, without explicitly referring to the mappings π_α.

The usual sort of "abstract nonsense" shows that if $(P,\pi_\alpha)_{\alpha\in\mathcal{A}}$ and $(P',\pi'_\alpha)_{\alpha\in\mathcal{A}}$ are both products of the family $M_\alpha,\ \alpha\in\mathcal{A}$, then $P\cong P'$. This leaves the question of existence of a product; however this is already afforded by the ordinary cartesian product:

$$P=\prod_{\alpha\in\mathcal{A}} M_\alpha.$$

To give this a module structure, recall first the definition of the cartesian product:

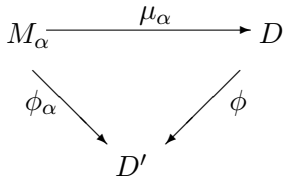
$$\prod_{\alpha\in\mathcal{A}} M_\alpha = \{f:\mathcal{A}\to\bigcup_{\alpha\in\mathcal{A}} M_\alpha |\ f(\alpha)\in M_\alpha \text{ for each } \alpha\in\mathcal{A}\}.$$

Now define addition and R-scalar multiplication in $\prod_{\alpha\in\mathcal{A}} M_\alpha$ pointwise: $(f+g)(\alpha)=f(\alpha)+g(\alpha),\ (r\cdot f)(\alpha)=r\cdot f(\alpha),\ \alpha\in\mathcal{A}, f,g\in\prod_{\alpha\in\mathcal{A}} M_\alpha, r\in R.$

The "projection maps" $\pi_\beta : \prod_{\alpha\in\mathcal{A}} M_\alpha \to M_\beta,\ \beta \in \mathcal{A}$ are defined by setting $\pi_\beta(f) = f(\beta), \beta \in \mathcal{A}$.

THEOREM 5.2.1 *The family* $(\prod_{\alpha\in\mathcal{A}} M_\alpha, \pi_\beta)$ *is a product of the family* $\{M_\alpha\}_{\alpha\in\mathcal{A}}$.

Dual to the above notion is that of the *direct sum* of the family $\{M_\alpha\}_{\alpha\in\mathcal{A}}$. The family $(D, \mu_\alpha)_{\alpha\in\mathcal{A}}$ is said to be a direct sum of the family $\{M_\alpha\}$, if there exist module homomorphisms $\mu_\alpha : M_\alpha \to D$, satisfying the following universal criterion: If D' is any other module, with homomorphisms $\mu'_\alpha : M_\alpha \to D'$, then there exists a unique homomorphism $\phi : D \to D'$, such that for each $\alpha \in \mathcal{A}$, the triangle below



commutes. Again, as in the case of the direct product, if the direct sum of the family $\{M_\alpha\}_{\alpha\in\mathcal{A}}$, exists, it is unique up to isomorphism.

Using the direct product $\prod_{\alpha\in\mathcal{A}} M_\alpha$, one can construct a direct sum, as follows. Namely, set

$$D \ = \ \{f \in \prod_{\alpha\in\mathcal{A}} M_\alpha |\ f(\beta) = 0 \text{ for all but finitely many } \beta \in \mathcal{A}\}.$$

Note that D is clearly an R-submodule of $\prod_{\alpha\in\mathcal{A}} M_\alpha$. Next we define R-module homomorphisms $\mu_\alpha : M_\alpha \to D$ by setting

$$\mu_\alpha(m_\alpha)(\beta) = \begin{cases} m_\alpha & \text{if } \alpha = \beta, \\ 0 & \text{if } \alpha \neq \beta. \end{cases}$$

Then one has the following:

PROPOSITION 5.2.2 *The direct sum of a family $\{M_\alpha\}$ exists and is constructed as above.*

We denote the direct sum of the family $\{M_\alpha\}$ by $\bigoplus_{\alpha\in\mathcal{A}} M_\alpha$. Note that if $\mu_\beta : M_\beta \to \bigoplus_{\alpha\in\mathcal{A}} M_\alpha$, are as above, then every element of $\bigoplus_{\alpha\in\mathcal{A}} M_\alpha$ can be uniquely written as a sum $\sum_{\alpha\in\mathcal{A}} \mu_\alpha(m_\alpha),\ \ m_\alpha \in M_\alpha$.

There is also an "internal" version of direct sum. Let M be an R-module, and assume that $\{M_\alpha\}$ is a family of submodules. For each $\alpha \in \mathcal{A}$, let $i_\alpha : M_\alpha \to M$ be the inclusion map. If $(M, i_\alpha)_{\alpha\in\mathcal{A}}$ satisfies the universal criterion above, we say that M is the *internal direct sum* of the submodules $M_\alpha,\ \alpha \in \mathcal{A}$, and write $M = \bigoplus_{\alpha\in\mathcal{A}} M_\alpha$.

Fortunately, there is a simple criterion for M to be an internal direct sum of submodules $M_\alpha,\ \alpha \in \mathcal{A}$.

PROPOSITION 5.2.3 *Let M be an R-module, and let $\{M_\alpha\},\ \alpha \in \mathcal{A}$ be a family of submodules. Then $M = \bigoplus_{\alpha\in\mathcal{A}} M_\alpha$, if and only if*

(i) $M = \sum_{\alpha\in\mathcal{A}} M_\alpha$, *and*

(ii) for each $\alpha \in \mathcal{A},\ \mathcal{M}_\alpha \cap \sum_{\beta\neq\alpha} \mathcal{M}_\beta = 0.$

Additional Terminology and Notation. Let $\{M_\alpha\}_{\alpha\in\mathcal{A}}$ be a family of R-modules. If $(\prod_{\alpha\in\mathcal{A}} M_\alpha, \pi_\alpha)_{\alpha\in\mathcal{A}}$ is a product, we frequently call the mappings $\pi_\alpha : \prod_{\beta\in\mathcal{A}} M_\beta \to M_\alpha$ *projection mappings.* Correspondingly, if $(\oplus_{\alpha\in\mathcal{A}} M_\alpha, \mu_\alpha)$ is a sum, we frequently call the mappings $\mu_\alpha : M_\alpha \to \oplus_{\beta\in\mathcal{A}} M_\beta$ *coordinate mappings.*

Next suppose that we have a collection of R-module homomorphisms $p_\alpha : P \to M_\alpha,\ \alpha \in \mathcal{A}$. Then we use the notation

$$\{p_\alpha\}_{\alpha\in\mathcal{A}} : P \longrightarrow \prod_{\alpha\in\mathcal{A}} M_\alpha$$

for the induced mapping. In particular, if $p_1 : P \to M_1,\ p_2 : P \to M_2$ is a pair of R-module homomorphisms into R-modules $M_1,\ M_2$, we have the induced mapping

$$\{p_1, p_2\} : P \longrightarrow M_1 \times M_2.$$

When we have a collection of R-module homomorphisms $i_\alpha : M_\alpha \to D,\ \alpha \in \mathcal{A}$, the we use the notation

$$\langle i_\alpha \rangle_{\alpha \in \mathcal{A}} : \oplus_{\alpha \in \mathcal{A}} M_\alpha \longrightarrow D$$

for the induced mapping. In particular, where we have a pair of maps $i_1 : M_1 \to D,\ i_2 : M_2 \to D$, the induced mapping is denoted

$$\langle i_1, i_2 \rangle : M_1 \oplus M_2 \longrightarrow D.$$

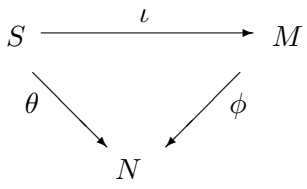
Finally, let $\{M_\alpha\}_{\alpha \in \mathcal{A}},\ \{M'_\alpha\}_{\alpha \in \mathcal{A}}$ be families of R-modules, indexed by the same index set $\mathcal{A}$. If we have R-module homomorphisms $\phi_\alpha M_\alpha \to M'_\alpha,\ \alpha \in \mathcal{A}$, there there is a naturally induced map

$$\prod \phi_\alpha : \prod_{\alpha \in \mathcal{A}} M_\alpha \longrightarrow \prod_{\alpha \in \mathcal{A}} M'_\alpha$$

induced by the composite maps $\prod_{\beta \in \mathcal{A}} M_\beta \stackrel{\pi_\alpha}{\to} M_\alpha \stackrel{\phi_\alpha}{\to} M'_\alpha,\ \alpha \in \mathcal{A}$. In an entirely analogous fashion, we get naturally induced homomorphisms

$$\oplus \phi_\alpha : \bigoplus_{\alpha \in \mathcal{A}} M_\alpha \longrightarrow \bigoplus_{\alpha \in \mathcal{A}} M'_\alpha.$$

There is another universal construction, reminiscent of that for free groups. Let M be an R-module, and let S be a set. Say that M is *free* on the set S if there exists a map $\iota : S \to M$, satisfying the following universal property. If N is any R-module, and if $\theta : S \to N$ is any map, then there is a unique R-module homomorphism $\phi : M \to N$ such that



commutes.

The following is easily anticipated.

PROPOSITION 5.2.4 *If S is any set, then there exists a free module M on the set S, which is unique up to isomorphism.*

In fact, the above construction is based on the direct sum construction, as follows. Given the set S and the ring R, let $R_s = R$ *regarded as a left R-module*, let $M = \bigoplus_{s\in S} R_s$, and let $\mu_{s'} : R_{s'} \to \bigoplus_{s\in S} R_s$ be the coordinate mappings. Define $\iota : S \to \bigoplus_{s\in S} R_s$ by setting $\iota(s) = \mu_s(1),\ s \in S$. Then M is the desired free module.

Again, there is an "internal" criterion for freeness, as follows. Let M be and R-module, and let $B \subseteq M$. If B spans M and is R-linearly independent, then B is called a *basis* for M. It need not happen that the R-module M admits a basis. A good example is the additive group (i.e. $\mathbb{Z}$-module) $\mathbb{Q}$ of rational numbers. Note first that $\mathbb{Q}$ is not a cyclic group and so it cannot have a basis consisting of one element. Next, let $r_1 = \frac{a_1}{b_1}, r_2 = \frac{a_2}{b_2} \in \mathbb{Q}$, with $r_1 \neq r_2$. Then $a_2b_1r_1 - a_1b_2r_2 = 0$, and so the set $\{r_1, r_2\}$ is $\mathbb{Z}$-linearly dependent. Therefore, it follows that any subset B of $\mathbb{Q}$ of cardinality greater than 1 is $\mathbb{Z}$-linearly dependent.

The significance of having a basis is as follows.

PROPOSITION 5.2.5 *The R-module M is free if and only if it has a basis.*

In case M is a free module over a *commutative* ring R, we can actually say more. Indeed, if $J \subseteq R$ is a maximal ideal then R/J is a field, and it's easy to see that the quotient module M/JM is acually an R/J-module, i.e., is an R/J-vector space. Furthermore, if $\{m_\alpha |\ \alpha \in \mathcal{A}\}$ is a basis for M, it is easy to check that the set $\{m_\alpha + JM |\ \alpha \in \mathcal{A}\}$ is a vector space basis for M/JM. Since any two bases of a fixed vector space have the same cardinality, we conclude the following result:

PROPOSITION 5.2.6 *If M is a free module over the commutative ring R, then any two bases have the same cardinality.*

Therefore, if M is a free module over the commutative ring R, we may speak of the *rank* of this module. In general, if R is a ring whose free

modules have well-defined ranks, we often say that R has *IBN* (*invariant basis number*); therefore, commutative rings have *IBN*. One can show that, more generally, any left Noetherian ring has *IBN*. (See Joseph Rotman, *An Introduction to Homological Algebra*, Academic Press, 1979, *Theorem* 4.9, *page* 111.)

LEMMA 5.2.7 *Let R be a commutative ring and let M be a finitely generated R-module. If $J \subseteq R$ is an ideal and $M{=}JM$, then $(1-x)M = 0$ for some $x \in J$.*

LEMMA 5.2.8 *Let R be a commutative ring and let M be a finitely generated R-module. If the R-module homomorphism $f : M \to M$ is surjective, then it is injective (and hence is an isomorphism).*

Note that the above generalizes *Exercise* 3 of *Section* 4.

The following shows again the rough similarity between free modules over a commutative ring and vector spaces.

THEOREM 5.2.9 *Let R be a commutative ring and let M be a free R-module of finite rank r. If $\{m_1, m_2, \ldots, m_r\}$ generates M, then it is a basis of M.*

Exercises

1. Let
$$0 \to M' \xrightarrow{\mu} M \xrightarrow{\epsilon} M'' \to 0$$
be an exact sequence of left R-modules. Show that the following two conditions are equivalent:
   (a) There exists a module homomorphism $\tau : M \to M'$ such that $\tau \circ \mu = 1_{M'}$.
   (b) There exists a module homomorphism $\rho : M'' \to M$ such that $\epsilon \circ \rho = 1_{M''}$.

   Show that if either of the above two cases hold, then $M \cong M' \oplus M''$. When this happens, we say that the exact sequence $0 \to M' \xrightarrow{\mu} M \xrightarrow{\epsilon} M'' \to 0$ *splits*.

2. Let M be an R-module. Prove that M is free if and only if M is isomorphic to the direct sum of copies of R.

3. Prove that any R-module is the homomorphic image of a free R-module.

4. Give an example of a free R-module M and a submodule N such that N is not free.

5. Prove that the direct sum of a family of free R-modules is also free.

6. Let F_1 be a free R-module on the set S_1, and let F_2 be a free R-module on the set S_2. If $S_1,\ S_2$ have the same cardinality, prove that $F_1 \cong F_2$.

7. Consider the diagram of R-modules and R-module homomorphisms:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A' & \xrightarrow{\phi'} & B' \end{array}$$

   From the above diagram, construct the sequence:

$$A \xrightarrow{\mu_{A'}\alpha+\mu_B\phi} A' \oplus B \xrightarrow{\langle -\phi', \beta\rangle} B',$$

   where $\mu_{A'} : A' \to A' \oplus B,\ \mu_B : B \to A' \oplus B$ are the coordinate maps. Show that the above square is commutative if and only if the above sequence is *differential*, i.e., $\langle -\phi', \beta\rangle \circ (\mu_{A'}\alpha + \mu_B\phi) = 0$.

8. Let $\{M_\alpha\}_{\alpha\in\mathcal{A}}$ be a family of R-modules. For each pair of indices $\alpha, \beta \in \mathcal{A}$, define homomorphisms $p_{\alpha\beta} : M_\alpha \to M_\beta$ by setting $p_{\alpha\beta} = 1_{M_\alpha}$, if $\alpha = \beta$ and $p_{\alpha\beta} = 0 : M_\alpha \to M_\beta$, if $\alpha \neq \beta$. Therefore, by universality of direct product, we get induced homomorphisms $\{p_{\alpha\beta}\}_\alpha : M_\beta \to \prod_{\alpha\in\mathcal{A}} M_\alpha,\ \beta \in \mathcal{A}$. In turn, we get an induced map

$$\langle\{p_{\alpha\beta}\}_\alpha\rangle_\beta : \bigoplus_{\beta\in\mathcal{A}} M_\beta \longrightarrow \prod_{\alpha\in\mathcal{A}} M_\alpha.$$

   Analogously, obtain induced maps

$$\{\langle p_{\alpha\beta}\rangle_\beta\}_\alpha : \prod_{\alpha\in\mathcal{A}} M_\alpha \longrightarrow \bigoplus_{\beta\in\mathcal{A}} M_\beta.$$

Show that the composition of the two maps $\bigoplus_{\beta\in\mathcal{A}} M_\beta \to \bigoplus_{\beta\in\mathcal{A}} M_\beta$ is the identity, by

(a) using the explicit constructions of $\bigoplus_{\beta\in\mathcal{A}} M_\beta$ and $\prod_{\alpha\in\mathcal{A}} M_\alpha$, and

(b) using the universality properties.

9. Let $N \xrightarrow{\mu} M \xrightarrow{\epsilon} N$ be R-module homomorphisms with $\epsilon\mu$ an automorphism of N. Prove that $M = \mu N \oplus \ker \epsilon$.

10. Let $\mathbb{F}$ be a field and let R be the ring

$$R = \left\{ \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ c & d & e \end{bmatrix} \mid a,b,c,d,e \in \mathbb{F} \right\},$$

let M be the left R-module

$$M = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \mid x,y,z \in \mathbb{F} \right\},$$

and let $N \subseteq M$ be the submodule

$$N = \left\{ \begin{bmatrix} 0 \\ 0 \\ z \end{bmatrix} \mid z \in \mathbb{F} \right\}.$$

Prove that M is not the direct sum of two proper submodules, but that the quotient $M/N \cong M_1 \oplus M_2$ for nontrivial submodules M_1 and M_2.

5.3 Modules over a Principal Ideal Domain

All modules in this section are modules over a principal ideal domain. The first result shows that rank behaves nicely with respect to submodules.

PROPOSITION 5.3.1 *Let M be a free module over the principal ideal domain R. If N is a submodule of M, then N is free, and rank $(N) \leq$ rank (M).*

The above result actually characterizes principal ideal domains, as follows from *Exercise* 1, below.

Let M be an R-module, R a *p.i.d.*, and let $m \in M$. Set Ann $(m) = \{r \in R |\ rm = 0\}$; note that Ann (m) is an ideal of R. Since R is a *p.i.d.*, we conclude that Ann $(m) = Ra$, for some $a \in R$. The element a, well defined up to associates, is called the *order* of m, and denoted $o(m)$. If $o(m) \neq 0$, m is called a *torsion element* of M. Note that the torsion elements of M form a submodule of M, called the *torsion submodule* of M, and is denoted $T(M)$. If $T(M) = 0$, M is called a *torsion-free* R-module. On the other hand, if every element of M is torsion, then M is called a *torsion module*. Finally, note that $M/T(M)$ is a torsion-free module.

PROPOSITION 5.3.2 *Let M be a finitely generated torsion-free R-module, where R is a principal ideal domain. Then M is free.*

Note that the condition of finite generation in the above proposition is crutial since the abelian group ($\mathbb{Z}$-module) $\mathbb{Q}$ is torsion-free, but not free.

PROPOSITION 5.3.3 *Let M be a finitely generated R-module, where R is a principal ideal domain. Then $M = F \oplus T(M)$, where F is a free submodule of M.*

From *Proposition* 5.3.3, it follows that in order to classify finitely generated modules over a *p.i.d.*, it suffices to classify finitely generated torsion modules over a *p.i.d.* Indeed, note that if M is finitely generated over the *p.i.d.* R, then by *Corollary* 4.1.3.1 of *Chapter* 4, $T(M)$ is also finitely generated.

Let M be an R-module and let $r \in R$. Define $M[r] = \{m \in M |\ rm = 0\}$. Clearly $M[r]$ is a submodule of M, and that every element of $M[r]$ has order dividing r. Assume that M is a finitely generated torsion R-module. Then $0 \neq$ Ann $(M) :=$ Ann $(M) = \{r \in R |\ rM = 0\}$; since Ann (M) is clearly an ideal of R, we conclude that Ann $(M) = Ra$, for some $0 \neq a \in R$. The element $a \in R$,

well defined up to associates, is called the *exponent* of M, and is sometimes denoted exp (M). It should be clear that if $N \subseteq M$ then exp (N) divides exp (M).

THEOREM 5.3.4 (PRIMARY DECOMPOSITION THEOREM) *Let M be a finitely generated torsion module over the principal ideal domain R. Let a be the exponent of M, and assume that $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the factorization of a into its prime powers. Then*

$$M = \bigoplus_{i=1}^{k} M[p_i^{e_i}].$$

Thus the problem of determining the structure of a finitely generated torsion R-module is reduced to that of determining the structure of a finitely generated R-module of prime-power exponent.

Recall that an R-module M is called *cyclic* if it is of the form Rx, for some $x \in M$. It should be clear that if $M = Rx$, and if $o(x) = a$, then exp $(M) = a$.

THEOREM 5.3.5 *Let M be a finitely generated R-module over the principal ideal domain R, and assume that exp $(M) = p^e$, where p is a prime in R. Then there exists a unique sequence $e_1 = e \geq e_2 \geq \ldots \geq e_l$, and cyclic submodules $Z_1, Z_2, \ldots, Z_l$, such that $M = \bigoplus_{i=1}^{l} Z_i$.*

COROLLARY 5.3.5.1 (ELEMENTARY DIVISOR THEOREM) *Let M be a finitely generated torsion R-module over the principal ideal domain R with $a =$ exp $(M) = p_1^{e_1} \cdots p_k^{e_k}$ (prime factorization). Then there exists unique sequences*

$$e_{i1} = e_i \geq e_{i2} \ldots \geq e_{il_i}, \quad i = 1, 2, \ldots k$$

such that

$$M = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} Z_{ij},$$

where each Z_{ij} is a cyclic submodule of exponent $p_i^{e_{ij}}$.

The prime powers $p_i^{e_{ij}}$ occurring in the above are often called the *elementary divisors* of the torsion module M, and the cyclic submodules Z_{ij}

are called *elementary components* . Thus, as a simple example, the abelian group $Z_{25} \oplus Z_5 \oplus Z_3 \oplus Z_3$ has $(25, 5, 3, 3)$ as its sequence of elementary divisors. The cyclic groups Z_{25}, Z_5, Z_3 occur as elementary components.

For many applications, the decomposition of a finitely generated torsion module into elementary components is too fine. Indeed, note the following:

LEMMA 5.3.6 *Let Z_1, Z_2 be cyclic R-modules of exponents a_1, a_2, and assume that a_1, a_2 are relatively prime in R. Then $Z_1 \oplus Z_2$ is cyclic of exponent $a_1 a_2$.*

As a result, we have the following.

THEOREM 5.3.7 (INVARIANT FACTOR THEOREM) *Let M be a finitely generated torsion module over the principal ideal domain R, and assume that $\exp(M) = a$. Then there exists a unique sequence*

$$a_1 = a, a_2, \ldots, a_r,$$

with $a_{i+1} | a_i$, $i = 1, \ldots, r-1$, and cyclic submodules $M_1, \ldots M_r$, $\exp(M_i) = a_i$, $i = 1, \ldots, r$, such that $M = \bigoplus_{i=i}^{r} M_i$.

The elements $a_1, a_2, \ldots, a_r$ in the above theorem are called the *invariant factors* of M.

Exercises

1. Let R be a commutative ring, and assume that every ideal of R is a free submodule of R. Prove that R is a *p.i.d.*
2. Let M be a finitely generated free module over the *p.i.d.* R, and let N be a submodule of M. Prove that M and N have the same rank if and only if the quotient module M/N is a torsion module.
3. Classify all the finite abelian groups of order 300.
4. For each prime p, define the subgroup T_p of the additive group of the rationals by setting

   $$T_p = \{a/p^i \in \mathbb{Q} |\ a, i \in \mathbb{Z}\}.$$

   Prove that the abelian groups $\mathbb{Q}$, T_p, p is prime are not finitely generated abelian groups.

5. Prove that the torsion abelian groups $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Z}(p^\infty) := T_p/\mathbb{Z}, p$ is prime are isomorphic to subgroups of the group $\mathbb{T}$, the multiplicative group of modulus 1 complex numbers.

6. Prove that the torsion abelian group $\mathbb{Q}/\mathbb{Z}$ admits a primary decomposition of the form $\mathbb{Q}/\mathbf{Z} = \bigoplus_{p \text{ prime}} \mathbb{Z}(p^\infty)$.

7. Prove that every finite subgroup of the abelian group $\mathbb{Z}(p^\infty)$ is cyclic.

8. Prove that $\mathbb{Z}(p^\infty)$ has no maximal subgroups.

9. Let R be a *p.i.d.*, and let M be a cyclic R-module of exponent $a \in R$. Prove that M is a free R/Ra-module.

10. Let M be a finitely generated torsion module over the *p.i.d.* R, and let $a \in R$ be the exponent of M. Prove that $\mathrm{Aut}_R(M)$ acts transitively on the elements of order a in M.

5.4 Calculation of Invariant Factors

In this section, R continues to be a principal ideal domain. If $A, B \in M_{m,n}(R)$, we say that $A,\ B$ are *Smith equivalent* (and write $A \sim_S B$) if there exist invertible matrices $P \in M_n(R),\ Q \in M_m(R)$ such that $B = QAP$. We say that the matrix $A = [a_{ij}] \in M_{m,n}(R)$ is in *Smith canonical form* if

(i) $i \neq j$ implies that $a_{ij} = 0$.

(ii) There exists r such that $a_{11}, a_{22}, \ldots, a_{rr} \neq 0$, and all $a_{ss} = 0$, if $s > r$.

(iii) If we set $a_i = a_{ii},\ i = 1, 2, \ldots, r$, then $a_i | a_{i+1},\ i = 1, 2, \ldots, r-1$.

THEOREM 5.4.1 *If $A \in M_{m,n}(R)$, then A is Smith equivalent to a matrix in Smith canonical form.*

We now discuss the relationship of the above with the structure of finitely generated R-modules, where R is a principal ideal domain. Thus, Let $M = R\langle x_1, x_2, \ldots, x_n\rangle$; if $F = R\langle e_1, e_2, \ldots, e_n\rangle$ is free with basis $\{e_1, e_2, \ldots, e_n\}$, then there is a unique homomorphism $\phi : F \to M$, with $e_i \mapsto x_i,\ i = 1, 2, \ldots, n$. Let $K = \ker \phi$; thus K is a free R module of F with generators

$$f_j = \sum_{i=1}^{n} a_{ji} e_i, \quad j = 1, 2, \ldots, m.$$

In other words, we have a presentation of the R-module M in much the same way as one has presentations of groups:

$$M \cong R\langle e_1, \ldots, e_n | \ \sum a_{ij} e_j = 0,\ i = 1, \ldots, m\rangle.$$

The matrix $A = [a_{ij}] \in M_{mn}(R)$ is called a *relations matrix* for the module M.

Conversely, given a matrix $A = [a_{ij}] \in M_{mn}(R)$, we define a module

$$M_A \ = \ R\langle e_1, \ldots, e_n | \ \sum a_{ij} e_j = 0,\ i = 1, \ldots, m\rangle.$$

Therefore, any finitely generated module over the *p.i.d.* R is isomorphic with M_A for some matrix A with coefficients in R.

PROPOSITION 5.4.2 *Let $A, B \in M_{mn}(R)$, and assume that A and B are Smith equivalent. Then $M_A \cong M_B$.*

In, particular, when $M \cong M_A$ and when D is Smith equivalent to A and is in Smith canonical form, the structure of M is obtained as follows:

THEOREM 5.4.3 *Let $M \cong M_A$ and assume that A is equivalent to $D = [d_{ij}]$, where S is in Smith canonical form. Set $d_i = d_{ii},\ i = 1, \ldots, min\ \{m, n\}$, and if $m < n$, set $d_{m+1}, \ldots, d_n = 0$. Then*

$$M \cong R/Rd_1 \oplus R/Rd_2 \oplus \cdots R/Rd_n.$$

Note that if $d_1, d_2, \ldots, d_r$ are non-zero non-units, then $d_1, d_2, \ldots, d_r$ are precisely the invariant factors of M.

COROLLARY 5.4.3.1 *Let $A \in M_{mn}(R)$ and assume that $D = [d_{ij}], D' = [d'_{ij}]$ are Smith equivalent to A and are in Smith canonical form. Then $d_{ij} \sim d'_{ij}$ (associates). Thus, the "Smith canonical form" of a matrix $A \in M_{mn}(R)$ is unique up to associates.*

The following result is sometimes convenient for "small" relations matrices. Let $A = [a_{ij}] \in M_{mn}(R)$. An i-rowed *minor* of A is simply the determinant of an $i \times i$ submatrix of A. Say that A is of *determinantal rank* r if there exists a non-zero r-rowed minor, but every $(r+1)$-rowed minor is 0. Let $\Delta = \Delta_i(A)$ be the greatest common divisor of all of the i-rowed minors of A. Note that $\Delta_i | \Delta_{i+1},\ i = 1, 2, \ldots, r-1$. We have

THEOREM 5.4.4 *Assume that A has determinantal rank r, and that $\Delta_1, \Delta_2, \ldots, \Delta_r$ are as above. Set*

$$d_1 = \Delta_1, d_2 = \Delta_2 \Delta_1^{-1}, \ldots, d_r = \Delta_r \Delta_{r-1}^{-1}.$$

Then $d_1, d_2, \ldots, d_r$ are the non-zero invariant factors of A.

Exercises

1. Suppose we have the finitely generated abelian group

$$G = \langle e_1, \ldots, e_n | \ \sum a_{ij} e_j = 0 \ \rangle,$$

where the relations matrix $A = [a_{ij}]$ is a square matrix. Show that G is finite if and only if det $(A) \neq 0$, in which case $|G| = |\text{det } (A)|$.

2. Compute the structure of the abelian group

$$\langle e_1, \ldots, e_n | \ \sum a_{ij} e_j = 0 \ \rangle,$$

given that

(a)

$$A = \begin{bmatrix} 6 & 2 & 3 \\ 2 & 3 & -4 \\ -3 & 3 & 1 \end{bmatrix}.$$

(b)

$$A = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix}.$$

(c)

$$A = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -2 & 2 \end{bmatrix}.$$

(d)

$$A = \begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & -1 \\ 0 & -1 & 2 & 0 \\ 0 & -1 & 0 & 2 \end{bmatrix}.$$

(e)

$$A = \begin{bmatrix} 2 & -1 & 0 & . & . & . & . \\ -1 & 2 & -1 & . & . & . & . \\ 0 & -1 & 2 & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & 2 & -1 & 0 \\ . & . & . & . & -1 & 2 & -1 \\ . & . & . & . & 0 & -1 & 2 \end{bmatrix}.$$

3. Let $A \in M_n(R)$. Show that $A \sim_S A^t$.

4. Suppose that

$$M = M_A = R\langle e_1, \ldots, e_n | \ \sum a_{ij} e_j = 0, \ i = 1, \ldots, m \rangle.$$

If $PAQ = D$ is in Smith canonical form, show how to obtain a generating set for $T(M)$, the torsion submodule of M, as R-linear combinations of the generators $e_1, e_2, \ldots e_n$ of M_A.

5. Let R be a *p.i.d.* and let $A, B \in \mathrm{M}_n(R)$, where B is an invertible matrix. If M is the $kn \times kn$ block matrix

$$M = \begin{bmatrix} A & 0 & . & . & 0 \\ B & A & . & . & 0 \\ 0 & B & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & B & A \end{bmatrix},$$

show that M and A^k have the same non-trivial (i.e., non-unit) invariant factors. Put differently, show that M and

$$M' = \begin{bmatrix} I & 0 & . & . & 0 \\ 0 & I & . & . & 0 \\ 0 & 0 & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & 0 & A^k \end{bmatrix},$$

are Smith equivalent.

6. Let $\mathbb{Z}[i]$ be the ring of Gaussian integers (see page 87) and let $a + bi \in \mathbb{Z}[i]$. If $I = (a + bi) \subseteq \mathbb{Z}[i]$ is the ideal in $\mathbb{Z}[i]$ generated by $a + bi$, show that a $\mathbb{Z}$-basis of I is $\{a + bi, -b + ai\}$. Conclude that $\mathbb{Z}[i]/I$ is a finite group of order $a^2 + b^2$.

5.5 Application to a Single Linear Transformation

Let V be a finite dimensional vector space over the field $\mathbb{F}$, and let T be a linear transformation on V. Using the above methods, we shall be able to compute the so-called rational canonical form of the transformation T.

The first important step is to regard V an an $\mathbb{F}[x]$-module, where x is an indeterminate. Indeed, simply take the scalar multiplication to be $f(x)\cdot v = f(T)(v)$, where $f(x) \in \mathbb{F}[x], v \in V$. This is easily checked to satisfy the requirements of a scalar multiplication. Note that since $\mathbb{F}[x]$ is a principal ideal domain, the results of the preceeding section apply. The following is quite simple, and provides the existence of the minimal polynomial of the linear transformation T:

LEMMA 5.5.1 *The $\mathbb{F}[x]$-module V defined above is a finitely generated torsion module.*

Indeed, the exponent of the $\mathbb{F}[x]$-module V is nothing other than the *minimal polynomial* of T.

Recall that the idea behind canonical forms for a linear transformation T is to find a basis for V relative to which T has a particularly simple form. Since the structure theory for finitely generated torsion modules over a *p.i.d.* rests on a decomposition into cyclic modules, it is appropriate to investigate first what happens when the $\mathbb{F}[x]$-module V is itself cyclic. The answer is provided below.

LEMMA 5.5.2 *Let V be an n-dimensional $\mathbb{F}$-vector space with linear transformation $T \in End_{\mathbb{F}}(V)$, and assume that the $\mathbb{F}[x]$-module V is cyclic. Then there exists a basis of V with respect to which T is represented by the matrix*

$$A = \begin{bmatrix} 0 & 0 & . & . & -a_0 \\ 1 & 0 & . & . & . \\ 0 & 1 & . & . & . \\ . & . & . & . & . \\ . & . & . & 0 & -a_{n-2} \\ . & . & . & 1 & -a_{n-1} \end{bmatrix},$$

where $f(x) = \sum_{i=0}^{n} a_i x^i$ is the exponent of the $\mathbb{F}[x]$-module V.

The matrix above is called the *companion matrix* of the polynomial $f(x)$.

Let V have basis $\{v_1, v_2, \ldots, v_n\}$, and let $T \in \mathrm{End}_{\mathbb{F}}(V)$. Assume that $T(v_i) = \sum \alpha_{ji} v_j,\ i = 1, 2 \ldots, n$. Let F be the free $\mathbb{F}[x]$-module with basis $\{e_1, e_2, \ldots, e_n\}$; there is an $\mathbb{F}[x]$-module homomorphism $F \to V$ with $e_i \mapsto v_i,\ i = 1, 2, \ldots, n$.

LEMMA 5.5.3 *If $K = ker(F \to V)$, then the elements*

$$f_i \ = \ xe_i - \sum_{j=1}^{n} \alpha_{ji} e_j, \quad i = 1, 2, \ldots, n,$$

generate K.

Note that by *Theorem* 5.2.9, together with *Exercise* 2 *Section* 5.3, we see that the above elements $f_1, \ldots, f_n$ actually comprise a basis of K. However, this fact is important for our purposes.

From the above theorem, we see that the matrix $(xI - A)^t$, where $A = [\alpha_{ij}]$, represents the linear transformation $T \in \mathrm{End}(V)$, is the relations matrix for the presentation of the $\mathbb{F}[x]$-module as a quotient of a free module. Furthermore, by *Exercise* 3 of *Section* 5.4, we see that in order to find the invariant factors of V as an $\mathbb{F}[x]$-module (i.e., the invariant factors of the linear transformation T), it suffices to compute the Smith canonical form of the matrix $(xI - A) \in M_n(\mathbb{F}[x])$. Therefore, if $f_1(x), f_2(x), \ldots, f_r(x)$ are the invariant factors, then there is a basis of V with respect to which T is represented by the block diagonal matrix

$$A = \begin{bmatrix} C_1 & 0 & . & 0 \\ 0 & C_2 & . & 0 \\ 0 & 0 & . & . \\ . & . & . & \\ 0 & 0 & . & C_r \end{bmatrix},$$

where C_i is the companion matrix of $f_i(x),\ i = 1, 2, \ldots, r$. The above matrix form is called the *rational canonical form* of the linear transformation $T \in \mathrm{End}(V)$.

Furthermore, note that each invariant factor $f_i(x)$ divides $\det(xI - A)$, i.e., each invariant factor divides the *characteristic polynomial* of the linear transformation T. In particular, one has

THEOREM 5.5.4 (CAYLEY-HAMILTON THEOREM) *Let T be a linear transformation on the finite-dimensional vector space V. If $m_T(x)$ and $c_T(x)$*

denote the minimal polynomial and characteristic polynomial, respectively, of T, then $m_T(x) \mid c_T(x)$.

As a simple example, we consider the transformation represented by the matrix

$$A = \begin{bmatrix} 5 & -8 & 4 \\ 6 & -11 & 6 \\ 6 & -12 & 7 \end{bmatrix}.$$

Note that $\det(xI - A) = (x-1)^2(x+1)$; thus the invariant factors of A are divisors of $(x-1)^2(x+1)$ (see *Theorem* 5.5.4, above). Let's compute them. After some work, one arrives at the Smith canonical form

$$A = \begin{bmatrix} 1 & 0 & \\ 0 & x-1 & \\ 0 & 0 & (x-1)(x+1) \end{bmatrix},$$

from which it follows that the rational canonical form for A is

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

As another type of example, suppose that we have a matrix A, taken over the rational field, whose determinant is $c_A(x) = (x-1)^2(x^2-x+1)(x^2+x+1)^3$. Thus A is a 10×10 matrix. We may list the possible invariant factors below

1) $(x-1)^2(x^2-x+1)(x^2+x+1)^3$

2) $(x-1), (x-1)(x^2-x+1)(x^2+x+1)^3$

3) $(x^2+x+1), (x-1)^2(x^2-x+1)(x^2+x+1)^2$

4) $(x-1)(x^2+x+1), (x-1)(x^2-x+1)(x^2+x+1)^2$

5) $(x^2+x+1), (x^2+x+1), (x-1)^2(x^2-x+1)(x^2+x+1)$

6) $(x^2+x+1), (x-1)(x^2+x+1), (x-1)(x^2-x+1)(x^2+x+1)$

(The reader is encouraged to find all possible sets of elementary divisors.)

Finally, we give a brief development of the so-called *Jordan canonical form* for a linear transformation $T : V \to V$, where V is finite dimensional

over the field $\mathbb{F}$. Here, however, we need to assume that the minimal polynomial splits completely into linear factors in $\mathbb{F}[x]$. Thus assume that $m_T(x) = (x-\lambda_1)^{e_1}(x-\lambda_2)^{e_2}\cdots(x-\lambda_r)^{e_r}$, with $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{F}$. By the *Primary Decomposition Theorem*, we may as well assume that $m_T(x) = (x-\lambda)^e$. Note that if we set $T' = T - \lambda$, them $m'_T(x) = x^e$; thus there exists a basis of V with respect to which T' is represented by a block diagonal matrix, whose diagonal blocks are of the form

$$\begin{bmatrix} 0 & 0 & . & . & 0 \\ 1 & 0 & . & . & 0 \\ 0 & 1 & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & 1 & 0 \end{bmatrix}.$$

From the above, we conclude that the original linear transformation T is represented by a block diagonal matrix, whose blocks are "Jordan blocks" of the form

$$J_k(\lambda) = \begin{bmatrix} \lambda & 0 & . & . & 0 \\ 1 & \lambda & . & . & 0 \\ 0 & 1 & . & . & . \\ . & . & . & . & . \\ 0 & 0 & . & 1 & \lambda \end{bmatrix},$$

where the index k above simply means that $J_k(\lambda)$ is a $k \times k$ matrix. The above representation of the linear transformation T as a block diagonal matrix consisting of Jordan blocks is called the *Jordan canonical form* of T.

Exercises

1. Find the rational canonical form for the matrix
$$A = \begin{bmatrix} 3 & -1 & 1 & -1 \\ 0 & 3 & -1 & 1 \\ 2 & -1 & 3 & -4 \\ 3 & -3 & 3 & -4 \end{bmatrix}.$$

2. Do the same for
$$A = \begin{bmatrix} 6 & 2 & 3 & 0 \\ 2 & 3 & -4 & 1 \\ -3 & 3 & 1 & 2 \\ -1 & 2 & -3 & 5 \end{bmatrix}.$$

3. Let A be a rational coefficient matrix with minimal polynomial $m_A(x) = (x+2)^2(x^2+1)^2(x^4-x^2+1)$. If A is a 16×16 matrix, find the possible lists of invariant factors.

4. Let A, B be $n \times n$ matrices over the field $\mathbb{F}$, and let $\mathbb{K} \supseteq \mathbb{F}$. If A, B are similar over $\mathbb{K}$, prove that they are similar over $\mathbb{F}$.

5. Let V be a finite dimensional vector space over the field $\mathbb{F}$, and let $T : V \to V$ be a linear transformation. Assume that $m_T(x) = p(x) \in \mathbb{F}[x]$, where $p(x)$ is irreducible. If we set $\mathbb{K} = \mathbb{F}[x]/(p(x))$, show that V can be regarded in a natural way as a $\mathbb{K}$-vector space in such a way that the $\mathbb{K}$-subspaces of V are in bijective correspondence with the T-invariant $\mathbb{F}$-subspaces of V. (Hint: define $\mathbb{K}$-scalar multiplication by setting $(f(x) + I) \cdot v = f(t)(v), f(x) \in \mathbb{F}[x]$, and where I is the principal ideal $I = (p(x))$.)

6. Let V be a finite dimensional vector space over the field $\mathbb{F}$, and let $T : V \to V$ be a linear transformation. Say that T is *semisimple* if and only every T-invariant subspace $W \subseteq V$ has a T-invariant subspace $U \subseteq V$ with $V = W \oplus U$. Prove that if the minimal polynomial of T factors into the product of *distinct* irreducible factors in $\mathbb{F}[x]$, then T is semisimple. (Hint: Let $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ be the primary decomposition of V, and let $W \subseteq V$ be a T-invariant subspace of V. Argue that $W = (W \cap V_1) \oplus (W \cap V_2) \oplus \cdots \oplus (W \cap V_r)$, and apply *Exercise* 5 to each component.)

7. Let $\mathbb{F}_q$ be the finite field of order q, and let $G = \mathrm{GL}_2(q)$.

   (a) Show that for every $\sigma \in G$, the minimal polynomial $m_\sigma(x)$ splits over $\mathbb{F}_{q^2}$.

   (b) Write down the conjugacy classes of G with representatives written in terms of their Jordan canonical forms over $\mathbb{F}_{q^2}$.

8. Let $\mathbb{F} = \mathbb{R}$ (real field). If $A \in \mathrm{M}_n(\mathbb{R})$, define $e^A = \sum_{k=0}^{\infty} A^k$.

   (a) Prove that $\sum_{k=0}^{\infty} A^k$ is an absolutely convergent series; thus e^A is well-defined for any matrix $A \in \mathrm{M}_n(\mathbb{R})$

   (b) If $A, B \in \mathrm{M}_n(\mathbb{R})$ with $AB = BA$, prove that $e^{A+B} = e^A e^B$.

   (c) If $J = J_3(\lambda)$ (3×3 Jordan block), compute e^J.

(d) In general, describe a procedure for computing e^A, for any matrix $A \in \mathrm{M}_n(\mathbb{R})$, in terms of matrices P, J, where $P^{-1}AP = J$, and where J is a matrix in Jordan canonical form.

5.6 Chain Conditions and Series of Modules

Recall that in *Section* 4.1 (see *Page* 91) we defined a *Noetherian module* to be a module M such that if

$$M_1 \subseteq M_2 \subseteq \cdots$$

is a chain of submodules, then there exists an integer N such that if $n \geq N$, then $M_n = M_N$. In other words, a Noetherian modules is one that satisfies the *ascending chain condition* (*a.c.c.*) on submodules. In a completely analogous way, we define an *Artinian* module to be one satisfying the *descending chain condition* (*d.c.c*) on submodules.

For convenience, we remind the reader of the following equivalent conditions for a module to be Noetherian (See *Proposition* 4.1.2 of *Section* 4.1.)

PROPOSITION 5.6.1 *The following conditions are equivalent for the R-module M.*

(i) M is Noetherian.

(ii) Every submodule of M is finitely generated.

(iii) Every nonempty collection of submodules of M contains a maximal element (relative to containment).

As one would expect, Artinian modules can be characterized as follows:

PROPOSITION 5.6.2 *The following conditions are equivalent for the R-module M.*

(i) M is Artinian.

(ii) Every nonempty collection of submodules of M contains a minimal element (relative to containment).

The following is proved very easily, using the *Modular Law*. (See *Lemma* 5.1.3, *Page* 108.)

PROPOSITION 5.6.3 *Let $0 \to K \to M \to N \to 0$ be a short exact sequence of R-modules.*

(a) M is Noetherian if and only if both K and N are.

(b) M is Artinian if and only if both K and N are.

Let $M \neq 0$ be an R-module. We say that M is *irreducible* (or is *simple*) if M contains no nontrivial submodules. Here are a few examples:

1. An irreducible $\mathbb{Z}$-module is simply a cyclic group of prime order.
2. The ring $\mathbb{Z}$ contains no nontrivial ideals that are also irreducible as $\mathbb{Z}$-modules.
3. Let R be the ring $M_2(\mathbb{F})$ of 2-by-2 matrices over a field $\mathbb{F}$. Let M be the "natural" R-module

$$M = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} \mid a, b \in \mathbb{F} \right\}.$$

   Then M is an irreducible R-module.
4. Let V be an $\mathbb{F}$-vector space, and let $T \in \mathrm{End}_{\mathbb{F}}(V)$. If V is an $\mathbb{F}[x]$-module in the usual way, then V is irreducible if and only if the minimal polynomial $m_T(x)$ is irreducible, and $\deg m_T(x) = \dim V$.

Let M be an R-module. A chain of submodules of M

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_r = M$$

is called a *composition series* if for each $i \geq 1$, M_i/M_{i-1} is an irreducible R-module.

Proposition 5.6.4 (Schreier Refinement Theorem) *Let $N \subseteq M$ be R- modules, and consider two chains of submodules:*

$$N = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M,$$

$$N = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_s = M.$$

Then both chains can be refined so that the resulting chains have the same length and isomorphic factors (in some order).

Corollary 5.6.4.1 (Jordan-Hölder Theorem) *Let M be an R-module with two composition series*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M,$$

$$0 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_s = M.$$

Then r=s and in some order, the successive factors are isomorphic.

Of course, the above theorem can also be proved as in the proof of *Theorem* 1.7.4 of *Section* 1.7. However, the Schreier Refinement Theorem gives a different approach.

THEOREM 5.6.5 *The R-module M has a composition series if and only if it is both Noetherian and Artinian.*

Exercises

1. State and prove the appropriate version of the Butterfly Lemma for groups.
2. Prove that the $\mathbb{Z}$-module $\mathbb{Q}$ is neither Noetherian nor Artinian.
3. Show that the $\mathbb{Z}$-module $\mathbb{Z}(p^\infty)$ p prime is Artinian but not Noetherian. (See *Exercise* 5 of *Section* 5.3.)
4. Let R be a principal ideal domain and let M be a finitely generated torsion R-module. Prove that M is both Artinian and Noetherian. What if M is torsion-free?

5.7 The Krull-Schmidt Theorem

A useful tool in this section is *Exercise* 9 of *Section* 5.2.

LEMMA 5.7.1 *Let $N \xrightarrow{\mu} M \xrightarrow{\epsilon} N$ be R-module homomorphisms with $\epsilon\mu$ an automorphism of N. Then $M = \mu N \oplus \ker \epsilon$.*

The following result should remind you of *Exercise* 3 of *Section* 4.

LEMMA 5.7.2 *Let M be an R-module and let $f \in End_R(M)$.*

(i) If M is Artinian and f is injective, then f is surjective.

(ii) If M is Noetherian and f is surjective, then f is injective.

LEMMA 5.7.3 (FITTING'S LEMMA) *Let the R-module M satisfy both chain conditions, and let $f \in End_R(M)$. Then for some positive integer n,*

$$M \;=\; f^n M \oplus \ker f^n.$$

Definition. An R-module M is called *indecomposable* if it cannot be written as $M = M_1 \oplus M_2$ for nontrivial proper submodules $M_1, M_2 \subseteq M$.

COROLLARY 5.7.3.1 *Let M be an indecomposable R-module satisfying both chain conditions, and let $f \in End_R(M)$. Then either f is nilpotent or f is an automorphism.*

COROLLARY 5.7.3.2 *Let M be an indecomposable R-module satisfying both chain conditions. If $f_1, f_2 \in End_R(M)$, and if $g = f_1 + f_2$ is an automorphism, then one of f_1, f_2 is an automorphism.*

COROLLARY 5.7.3.3 *If M is indecomposable and satisfies both chain conditions, then $End_R(M)$ is a local ring (i.e., has a unique maximal ideal).*

LEMMA 5.7.4 *Let $M = M_1 \oplus M_2$, $N = N_1 \oplus N_2$ be Artinian R-modules, and let $\lambda : M \to N$ be an R-module isomorphism. Write $\lambda(m_1, 0) = (\alpha(m_1), \beta(m_1))$, where $\alpha \in Hom_R(M_1, N_1)$, $\beta \in Hom_R(M_1, N_2)$. If $\alpha : M_1 \xrightarrow{\cong} N_1$, then $M_2 \cong N_2$.*

THEOREM 5.7.5 (KRULL-SCHMIDT THEOREM) *Let the R-module M be both Noetherian and Artinian, and assume that we are given decompositions*

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r,$$

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_s,$$

Where each M_i and each N_j is indecomposable. Then $r = s$, and, possibly after renumbering, $M_i \cong N_i$, $i = 1, 2 \ldots, r$.

Exercises

1. Let M be an irreducible R-module. Prove that $E = \mathrm{End}_R(M)$ is a *division ring* , i.e., each non-zero element of E is invertible. (This simple result is known as *Schur's Lemma*.)

2. Let M be an indecomposable R-module with a composition series $0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_r = M$. Assume that the composition factors are pairwise nonisomorphic. Prove that $\mathrm{End}_R(M)$ is a division ring. (Hint: let $\alpha \in \mathrm{End}_R(M)$ with $\alpha(M) \neq M$. Argue that $\ker \alpha \cap \alpha(M) \neq 0$. Thus $\ker \alpha$ and $\alpha(M)$ share a composition factor. Now what?)

3. Note that the $\mathbb{Z}$-module $\mathbb{Z}$ is an indecomposable module which is not irreducible. Give some other examples.

4. Let V be an $\mathbb{F}$-vector space and let $T \in \mathrm{End}_{\mathbb{F}}(V)$ be a *semisimple* linear transformation (see *Exercise* 6 of *Section* 5.5). Prove that the $\mathbb{F}[x]$-module V is irreducible if and only if it is indecomposable.

5. Let V be an $\mathbb{F}$-vector space and let $T \in \mathrm{End}_{\mathbb{F}}(V)$. Prove that the $\mathbb{F}[x]$-module V is indecomposable if and only if V is cyclic and $m_T(x) = p(x)^e$, where $p(x) \in \mathbb{F}[x]$ is irreducible and e is a positive exponent.

6. Let $\mathbb{F}$ be a field and let R be the ring

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{F} \right\}.$$

R acts in the obvious way on the vector space M, where

$$M = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} \mid a, b \in \mathbb{F} \right\}.$$

Prove that M is not an irreducible R-module, but it is indecomposable.

7. Let R and M be as above and let

$$L = \left\{ \begin{bmatrix} a \\ 0 \end{bmatrix} \mid a \in \mathbb{F} \right\}.$$

Prove that $0 \subseteq L \subseteq M$ is a composition series for the R-module M whose composition quotients are non-isomorphic (i.e., $L \ncong M/L$). Conclude from *Exercise* 2 that $\mathrm{End}_R(M)$ is a division ring.

8. Using the Krull-Schmidt Theorem, prove that the elementary divisors of a finitely generated torsion R-module (where R is a *p.i.d.*) are unique. (See *Exercise* 4 of *Section* 5.6.)

5.8 Injective and Projective Modules

Let R be a ring and let P be an R-module. We say that P is *projective* if every diagram of the form

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \phi} & & \\ M & \xrightarrow{\epsilon} & M'' & \longrightarrow & 0 \end{array} \qquad \text{(exact)}$$

can be embedded in a commutative diagram of the form

$$\begin{array}{ccccc} & & P & & \\ & \swarrow{\scriptstyle \bar{\phi}} & \downarrow{\scriptstyle \phi} & & \\ M & \xrightarrow{\epsilon} & M'' & \longrightarrow & 0 \end{array} \qquad \text{(exact)}$$

In an entirely dual sense, the R-module I is said to be *injective* if every diagram of the form

$$\begin{array}{ccccc} & & I & & \\ & & \uparrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\mu} & M \end{array} \qquad \text{(exact)}$$

can be embedded in a commutative diagram of the form

$$\begin{array}{ccccc} & & I & \overset{\bar{\theta}}{\nwarrow} & \\ & & \uparrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\mu} & M \end{array} \qquad \text{(exact)}$$

We have the following simple characterization of projective modules.

THEOREM 5.8.1 *The following conditions are equivalent for the R-module P.*

(i) P is projective.

(ii) Every short exact sequence $0 \to M' \to M \to P \to 0$ splits.

(iii) P is a direct summand of a free R-module.

The next result gives a very important class of projective R-modules. Assume that R is an integral domain with fraction field $\mathbb{E}$. Recall from our discussions of Dedekind domains that we defined, for any ideal $I \subseteq R$,

$$I^{-1} = \{\alpha \in \mathbb{E} |\ \alpha I \subseteq R\}.$$

Recall also that the ideal I was called *invertible* if $I^{-1}I = R$.

THEOREM 5.8.2 *Let R be an integral domain and let $I \subseteq R$ be an ideal.*

(i) If I is invertible, then I is a projective R-module.

(ii) If I is a finitely generated ideal and is projective, then I is invertible.

Note that the above theorem gives a great number of interesting examples of projective modules which aren't free. Indeed, if R is any Dedekind domain which isn't a principal ideal domain then there will be *non*-free ideals (cf. *Exercise* 12, Below) of R. However, we have seen that any ideal of a Dedekind domain is invertible, hence is a projective R-module.

In order to obtain a characterization of injective modules we need a concept dual to that of a free module. First, however, we need the concept of a *divisible* abelian group. An abelian group D is *divisible* if for every $d \in D$ and for every $0 \neq n \in \mathbb{Z}$, there is some $c \in D$ such that $nc = d$.

Example 1. The most obvious example of a divisible group is probably the additive group $(\mathbb{Q}, +)$ of rational numbers.

Example 2. A moment's thought should reveal that if $\mathbb{F}$ is any field of characteristic 0, then $(\mathbb{F}, +)$ is a divisible group.

Example 3. Note that any homomorphic image of a divisible group is divisible. Of paramount importance is the divisible group $\mathbb{Q}/\mathbb{Z}$.

Example 4. If p is a prime, the group $\mathbb{Z}(p^\infty)$ is a divisible group. (You should check this.)

The importance of divisible groups is the following.

THEOREM 5.8.3 *Let D be an abelian group. Then D is divisible if and only if D is injective.*

Let R be a ring, and let A be an abelian group. Define $M = \mathrm{Hom}_{\mathbb{Z}}(R, A)$; thus M is certainly an abelian group under pointwise operations. Give M the structure of a (left) R-module via

$$(a \cdot f)(b) \;=\; f(ba),\; a, b \in R,\; f \in M.$$

It is easy to check that the above recipe gives $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ the structure of a left R-module. (See *Exercise* 10.)

The importance of the above construction is found in the following.

PROPOSITION 5.8.4 *Let R be a ring and let D be a divisible abelian group. Then the R-module $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module.*

Recall that any free R-module is the direct sum of a number of copies of R, and that *any* R-module is a homomorphic image of a free module. We now define a *cofree* R-module to be the direct *product* (not *sum*!) of a number of copies of the injective module $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$. We then have

PROPOSITION 5.8.5 *Let M be an R-module. Then M can be embedded in a cofree R-module.*

Finally we have the analogue of *Theorem* 41, above.

THEOREM 5.8.6 *The following conditions are equivalent for the R-module I.*

(i) I is injective.

(ii) Every short exact sequence $0 \to I \to M \to M'' \to 0$ splits.

(iii) I is a direct summand of a cofree R-module.

Exercises

1. Prove that the direct sum $\bigoplus_{i \in \mathcal{I}} P_i$ is projective if and only if each P_i is.
2. Prove that the direct product $\prod_{i \in \mathcal{I}} I_i$ is injective if and only if each I_i is.

3. Let R be a ring, let A be a fixed R-module, and let $\phi : M \to N$ be a homomorphism of R-modules. Define

$$\phi_* : \mathrm{Hom}_R(A, M) \to \mathrm{Hom}_R(A, N),$$

$$\phi^* : \mathrm{Hom}_R(N, A) \to \mathrm{Hom}_R(M, A),$$

by setting $\phi_*(f) = \phi \circ f$, $f \in \mathrm{Hom}_R(A, M)$, $\phi^*(f) = f \circ \phi$, $f \in \mathrm{Hom}_R(N, A)$. Prove that ϕ_* and ϕ^* are both homomorphisms of abelian groups. (Warning: it need not be the case that either of $\mathrm{Hom}_R(A, M)$, $\mathrm{Hom}_R(M, A)$ is an R-module.)

4. Let P be an R-module. Prove that P is projective if and only if given any exact sequence $0 \to M' \xrightarrow{\mu} M \xrightarrow{\epsilon} M'' \to 0$, the induced sequence

$$0 \to \mathrm{Hom}_R(P, M') \xrightarrow{\mu_*} \mathrm{Hom}_R(P, M) \xrightarrow{\epsilon_*} \mathrm{Hom}_R(P, M'') \to 0$$

is exact.

5. Suppose we have a sequence $0 \to M' \xrightarrow{\mu} M \xrightarrow{\epsilon} M'' \to 0$ of R-modules. Prove that this sequence is exact if and only if the sequence

$$0 \to \mathrm{Hom}_R(P, M') \xrightarrow{\mu_*} \mathrm{Hom}_R(P, M) \xrightarrow{\epsilon_*} \mathrm{Hom}_R(P, M'') \to 0$$

is exact for every projective R-module P.

6. Let I be an R-module. Prove that I is injective if and only if given any exact sequence $0 \to M' \xrightarrow{\mu} M \xrightarrow{\epsilon} M'' \to 0$, the induced sequence

$$0 \to \mathrm{Hom}_R(M'', I) \xrightarrow{\epsilon^*} \mathrm{Hom}_R(M, I) \xrightarrow{\mu^*} \mathrm{Hom}_R(M', I) \to 0$$

is exact.

7. Suppose we have a sequence $0 \to M' \xrightarrow{\mu} M \xrightarrow{\epsilon} M'' \to 0$ of R-modules. Prove that this sequence is exact if and only if the sequence

$$0 \to \mathrm{Hom}_R(M'', I) \xrightarrow{\epsilon^*} \mathrm{Hom}_R(M, I) \xrightarrow{\mu^*} \mathrm{Hom}_R(M', I) \to 0$$

is exact for every injective R-module I.

8. Let M be an R-module. Prove that

$$\mathrm{Hom}_R(R, M) \cong_R M.$$

9. Prove that if $A_\alpha,\ \alpha \in \mathcal{A}$, is a family of abelian groups, then

$$\mathrm{Hom}_{\mathbb{Z}}(R, \prod_{\alpha\in\mathcal{A}} A_\alpha) \cong_R \prod_{\alpha\in\mathcal{A}} \mathrm{Hom}_{\mathbb{Z}}(R, A_\alpha).$$

10. Let M be a *right* R-module, and let A be an abelian group. Prove that the scalar multiplication $(r \cdot f)(m) = f(mr),\ r \in R,\ m \in M,\ f \in \mathrm{Hom}_{\mathbb{Z}}(M, A)$ gives $\mathrm{Hom}_{\mathbb{Z}}(M, A)$ the structure of a left R-module.

11. Prove that there is a natural isomorphism of abelian groups:

$$\mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R, A)) \cong \mathrm{Hom}_{\mathbb{Z}}(M, A),$$

where M is an R-module and A is an abelian group.

12. Let R be an integral domain in which every ideal is a *free* R-module. Prove that R is a *principal ideal domain.*

13. Let $\mathbb{F}$ be a field and let R be the ring

$$R \ = \ \left\{ \left[\begin{array}{cc} a & b \\ 0 & c \end{array} \right] \mid a, b, c \in \mathbb{F} \right\},$$

with left R-modules

$$M \ = \ \left\{ \left[\begin{array}{c} a \\ b \end{array} \right] \mid a, b \in \mathbb{F} \right\}$$

and

$$L \ = \ \left\{ \left[\begin{array}{c} a \\ 0 \end{array} \right] \mid a \in \mathbb{F} \right\}$$

as in *Exercises* 6 and 7 of *Section* 5.7.

(a) Prove that L is a projective R-module, but that M/L is not.

(b) If we set

$$I \ = \ \left\{ \left[\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right] \mid a, b \in \mathbb{F} \right\},$$

show that the ideal I is a projective R-module.

14. A ring for which every ideal is projective is called a *hereditary* ring. In *Section* 4.6 we saw that every every ideal of a Dedekind domain R is invertible. In turn, by *Theorem* 5.8.2 every invertible ideal is a projective R-module. Thus, Dedekind domains are hereditary. Prove that if $\mathbb{F}$ is a field, then the ring $\mathrm{M}_n(\mathbb{F})$ of $n \times n$ matrices over $\mathbb{F}$ is hereditary. The same is true for the ring of lower triangular $n \times n$ matrices over $\mathbb{F}$.

15. Let A be an abelian group and let $B \leq A$ be such that A/B is infinite cyclic. Prove that $A \cong A/B \times B$.

16. Let A be an abelian group and assume that $A = H \times Z_1 = K \times Z_2$ where Z_1 and Z_2 are infinite cyclic. Prove that $H \cong K$. (Hint: First $H/(H \cap K) \cong HK/K \leq A/K \cong Z_2$ so $H/(H \cap K)$ is either trivial or infinite cyclic. Similarly for $K/(H \cap K)$. Next $A/(H \cap K) \cong H/(H \cap K) \times Z_1$ and $A/(H \cap K) \cong K/(H \cap K) \times Z_2$ so $H/(H \cap K)$ and $K/(H \cap K)$ are either both trivial (in which case $H = K$) or both infinite cyclic. Thus, from *Exercise* 10 obtain $H \cong H/(H \cap K) \times H \cap K \cong K/(H \cap K) \times H \cap K \cong K$, done.)

17. Prove *Baer's Criterion:* Let I be an R-module and assume that for any left ideal $J \subseteq R$ and any R-module homomorphism $\alpha_J : J \to I$, α extends to an R-module homomorphis $\alpha : R \to I$. Show that I is injective. (Hint: Let $M' \subseteq M$ be R-modules and assume that there is an R-module homomorphism $\alpha : M' \to I$. Consider the poset of pairs (N, α_N), where $M' \subseteq N \subseteq M$ and where α_N extends α. Apply Zorn's Lemma to obtain a maximal element (N_0, α_0). If $N_0 \neq M$, let $m \in M - N_0$ and let $J = \{r \in R |\ rm \in N_0\}$; note that J is a left ideal of R. Now what?)

18. Let R be a Dedekind domain with fraction field $\mathbb{E}$. Recall that a *fractional ideal* is simply a finitely-generated R-submodule of $\mathbb{E}$. If $J \subseteq \mathbb{E}$ is a fractional ideal, prove that J is a projective R-module. (Hint: As for ordinary ideals, define $J^{-1} = \{\alpha \in \mathbb{E} |\ \alpha J \subseteq R\}$. Using *Lemma* 4.5.1 of *Section* 4.5, argue that $J^{-1}J = R$. Now argue exactly as in *Theorem* 5.8.2, (i) to prove that J is a projective R-module.)

19. Let R be a Dedekind domain with field of fractions $\mathbb{E}$. If $I, J \subseteq \mathbb{E}$ are fractional ideals, and if $0 \neq \phi \in \mathrm{Hom}_R(I, J)$, prove that ϕ is injective. (Hint: If $J_0 = \mathrm{im}\ \phi$, then argue that J_0 is a projective R-module.

Therefore, One obtains $I = \ker \phi \oplus J'$, where $J \cong_R J_0$. Why is such a decomposition a contradition?)

20. Let R be a Noetherian domain. Prove that R is a Dedekind domain if and only if every ideal of R is a projective R-module. (See *Exercise* 5 of *Section* 4.6.)

5.9 Semisimple Modules

Let R be a ring and let M be an R-module. We say that M is *semisimple* if given any submodule $N \subseteq M$, there exists a submodule $N' \subseteq M$ with $M = N \oplus N'$.

Example 1. Let V be an $\mathbb{F}$-vector space and let $T \in \mathrm{End}_{\mathbb{F}}(V)$ be a *semisimple* linear transformation. If V is given an $\mathbb{F}[x]$-module structure in the usual way, then it is clear that V is semisimple. (Recall that by *Exercise* 6 of *Section* 5.5, a linear transformation T is semisimple if and only if the minimal polynomial $m_T(x)$ is multiplicity-free in its prime factorization. We'll obtain the same result as a direct consequence of *Theorem* 5.9.5, below.)

Example 2. Let A be a finite abelian group of exponent e. Assume that the factorization of e into primes is multiplicity-free. Then A is a semisimple $\mathbb{Z}$-module. This can be seen in a number of ways, including using *Theorem* 5.9.5, below.

Example 3. Let $\mathbb{F}$ be a field and let R be the ring

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{F} \right\}.$$

R acts in the obvious way on the vector space M, where

$$M = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} \mid a, b \in \mathbb{F} \right\}.$$

If $M' \subseteq M$ is the submodule defined by setting

$$M' = \left\{ \begin{bmatrix} a \\ 0 \end{bmatrix} \mid a \in \mathbb{F} \right\},$$

then it is easy to verify that $M \neq M' \oplus M''$, for any submodule $M'' \subseteq M$. Thus M is not a semisimple R-module.

Example 4. Obviously, any irreducible module is semisimple.

LEMMA 5.9.1 *Submodules and homomorphic images of semisimple modules are semisimple.*

Recall that an R-module M is called *irreducible* if and only if it contains no nontrivial submodules.

LEMMA 5.9.2 *Any non-zero semisimple module contains a non-zero irreducible submodule.*

LEMMA 5.9.3 (SCHUR'S LEMMA) *Let R be a ring and let M be an R-module. If M is irreducible, then the ring $E := Hom_R(M, M)$ is a division ring. More generally, if $\phi : M \to N$ is an R-module homomorphism between irreducible R-modules M, N, then ϕ is either the 0-map or is an isomorphism.*

THEOREM 5.9.4 *The following conditions are equivalent for the R-module M.*

(i) M is semisimple.

(ii) $M = \sum_{i\in\mathcal{I}} M_i$, for some family $\{M_i |\ i \in \mathcal{I}\}$ of irreducible submodules of M.

(iii) $M = \oplus_{i\in\mathcal{I}} M_i$, for some family $\{M_i |\ i \in \mathcal{I}\}$ of irreducible submodules of M.

The astute reader will realize that the following important theorem is as much a theorem about *rings*, as about modules.

THEOREM 5.9.5 *The following are equivalent about the ring R.*

(1) Every R-module is injective.

(2) Every R-module is projective.

(3) Every R-module is semisimple.

(4) The left R-module R is a direct sum of a finite number of irreducible left ideals:

$$R \ = \ \bigoplus_{i=1}^{n} L_i.$$

Furthermore each $L_i = Re_i$, where $e_1, e_2, \ldots, e_n$ are orthogonal idempotents (i.e., $e_i e_j = 0$, whenever $i \neq j$) satisfying

$$\sum_{i=1}^{n} e_i \ = \ 1 \in R.$$

(5) $R = \oplus_{i=1}^{k} A_i$, *where* $A_1, A_2, \ldots, A_k$ *are the distinct minimal 2-sided ideals in* R, *and where*

$$A_i \cong M_{n_i}(\Delta_i),\ i = 1, 2 \ldots, k,$$

for suitable division rings $\Delta_i,\ i = 1, 2, \ldots, k$.

COROLLARY 5.9.5.1 *Let* R *be a ring satisfying any of the equivalent conditions above, and let* M *be an irreducible* R*-module. Then* $M \cong I$ *(as* R*-modules), for some minimal left ideal* $I \subseteq R$.

Let us illustrate examples of the kinds of rings indicated above.

Example 1. If $R = \mathbb{Z}/(n)$, where the prime factorization of n is multiplicity-free, then by the *Chinese Remainder Theorem*, R is isomorphic to the direct sum of fields of the form $\mathbb{Z}/(p)$.

Example 2. Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$, where $f(x)$ admits a multiplicity-free factorization. As above, the Chinese Remainder Theorem shows that $R = \mathbb{F}[x]/(f(x))$ is the direct sum of fields.

Example 3. Let $\mathbb{F}$ be a field, and let $R = M_n(\mathbb{F})$.

Note that if R is any of the rings above, then any R-module is semisimple. In particular, this gives a proof of *Exercise* 6 of *Section* 5.5,

Exercises

1. Let R be a ring and let e be an idempotent. Prove that the left R-module Re is a projective R-module.

2. Let R be a ring satisfying any one of the conditions of *Theorem* 5.9.5, and let M be an irreducible R-module. Prove that $M \cong L$, for some irreducible left ideal L of R. (Hint: Let $0 \neq m \in M$, and define $\phi : R \to M$ via $\phi(r) = rm \in M$. Conclude that $M \cong R/(\ker \phi)$. Now what?)

3. Let Δ be a division ring and let $R = M_n(\Delta)$. Prove that R is a *simple* ring in that it has no proper 2-sided ideals.

4. Let R be as in *Exercise* 3. Prove that all irreducible R-modules are isomorphic. (Indeed, any irreducible R-module is isomorphic with the module Δ^n of all $n \times 1$ column vectors with entries in Δ.)

5. Let $\mathbb{F}$ be a field and let R be the ring

$$R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{F} \right\}.$$

Define the R-modules

$$M_1 = \left\{ \begin{bmatrix} a \\ 0 \end{bmatrix} \mid a \in \mathbb{F} \right\}, \quad M_2 = \left\{ \begin{bmatrix} 0 \\ b \end{bmatrix} \mid b \in \mathbb{F} \right\}.$$

Prove that $M_1 \ncong M_2$. (Does this surprise you?) (Compare with *Exercise* 8, *Section* 1.2.)

6. Let R be a ring and assume that $R = \oplus_{i=1}^{n} I_i$, where $I_1, \ldots I_n$ are minimal left ideals of R. If M is an irreducible left R-module, prove that $M \cong I_j$ for some index j, $1 \leq j \leq n$.

7. Let R be a simple ring and let $C = Z(R)$, the center of R. Prove that C is a field.

8. Prove the converse of Schur's lemma in case the module M is completely reducible. (Note that the unconditional converse of Schur's lemma fails; see *Exercise* 7 of *Section* 5.7.)

5.10 Example: Group Algebras

In this short section we give an example of an important class of rings for which the conclusion of *Theorem* 5.9.5 holds. To this end, let G be a finite group, and let $\mathbb{F}$ be a field. Define the $\mathbb{F}$-*group ring* $\mathbb{F}G$, by setting

$$\mathbb{F}G \;=\; \{\text{functions } \alpha : G \to \mathbb{F}\}.$$

The operations are *pointwise* addition and *convolution* multiplication. Thus, if $\alpha, \beta \in \mathbb{F}G$, and if $g \in G$, then

(i) $(\alpha + \beta)(g) = \alpha(g) + \beta(g)$,

(ii) $(\alpha * \beta)(g) = \sum_{h \in G} \alpha(gh^{-1})\beta(h)$.

Note that we may identify $g \in G$ with the characteristic function in $\mathbb{F}G$ on the set $\{g\}$, viz.,

$$g(h) \;=\; \begin{cases} 1 & \text{if } h = g \\ 0 & \text{if } h \neq g. \end{cases}$$

Thus, we may write $\alpha \in \mathbb{F}G$ as $\alpha = \sum_{g \in G} \alpha(g)g$, and the convolution multiplication is simply the ordinary group multiplication, extended by linearity. As a result, we can think of elements of $\mathbb{F}G$ as $\mathbb{F}$-linear combinations of elements of G.

The ring $A := \mathbb{F}G$ is actually an $\mathbb{F}$-*algebra* in the sense that it is not only a ring, but is an $\mathbb{F}$-vector space whose scalar multiplication satisfies

$$\alpha(ab) \;=\; (\alpha a)b \;=\; a(\alpha b),$$

$\alpha \in \mathbb{F},\ a, b \in A$. Thus we often call $\mathbb{F}G$ the $\mathbb{F}$-*group algebra*.

Let G be a finite group, and let M be an $\mathbb{F}$-vector space. A *representation* of G on M is a homomorphism $\phi : G \to \mathrm{GL}_{\mathbb{F}}(M)$.[1] Note that this gives M the structure of an $\mathbb{F}G$-module via

$$\sum_{g \in G} \alpha_g g \cdot m \;:=\; \sum_{g \in G} \alpha_g \phi(g) m,$$

$m \in M$. Conversely, if M is an $\mathbb{F}G$-module, then we get a representation of G on M in the obvious way. Note that if $\dim M = n$, then choosing

[1] Of course, this makes perfectly good sense even if G is not finite.

a basis of M induces a homomorphism $G \to \mathrm{GL}_n(\mathbb{F})$. Conversely, such a homomorphism clearly defines a representation of G on M.

The main result of the section is this:

THEOREM 5.10.1 (MASCHKE'S THEOREM) *Let G be a finite group, and let $\mathbb{F}$ be a field whose characteristic doesn't divide $|G|$. Then any $\mathbb{F}G$-module is semisimple.*

Thus we see that if $\mathrm{char}\ \mathbb{F} \not| \ |G|$, then $\mathbb{F}G$ satisfies the conditions of *Theorem* 51.

In case the field $\mathbb{F}$ satisfies the condition of the above theorem and is *algebraically closed* we can make a very precise statement about the structure of $\mathbb{F}G$.

THEOREM 5.10.2 *Let G be a finite group and let $\mathbb{F}$ be an algebraically closed field of characteristic not dividing $|G|$. Then there exist integers $n_1, n_2, \ldots, n_t$ with $\mathbb{F}G \cong \oplus_{i=1}^{t} M_{n_i}(\mathbb{F})$.*

We mention in passing that even in the non-semisimple situation, i.e., when the characteristic of $\mathbb{F}$ divides the order of the group G, then it still turns out that finitely-generated modules over the group algebra $\mathbb{F}G$ are projective if and only if they are injective. (See, e.g., C. W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, *Wiley Interscience*, New York, 1962, *Theorem* (58.14).)

Exercises

1. Let $\mathbf{C}$ be the complex field, and let A be an abelian group. Prove that any irreducible $\mathbf{C}A$-module is one-dimensional.

2. Let A be a cyclic group of order 3, say $A = \langle t \rangle$, and let $\mathbb{F} = \mathbb{F}_2$, the field of 2 elements. Prove that the assignment

$$t \to \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \in \mathrm{M}_2(\mathbb{F})$$

   defines an irreducible representation of G.

3. Let G be a finite group, let $\mathbb{F}$ be a field and let $\zeta : G \to \mathbb{F}^\times$ be a homomorphism. Define $e = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} \zeta(g^{-1}) g \in \mathbb{F}G$.

(i) Prove that e is an idempotent.

(ii) Prove that if $A = \mathbb{F}G$, then $\dim_{\mathbb{F}} Ae = 1$. (Thus Ae is a minimal left ideal of $\mathbb{F}G$.)

4. Let G be a p-group, where p is a prime and let $\mathbb{F}$ be a field of characteristic p. Interpret and prove the following: *The only irreducible $\mathbb{F}G$-module is the trivial one.* (Hint: Let G act on the vector space M and let $z \in Z(G)$ have order p. Let $M_0 = \{m \in M |\ z(m) = m\}$, and argue that $0 \neq M_0 \subseteq M$. Next, show that M_0 is a sub-$\mathbb{F}G$-module and so if M is irreducible, $M_0 = M$. Thus z acts trivially on M; this makes M into a $\mathbb{F}(G/\langle z \rangle)$-module. Now apply induction.)

5. Let G be a finite group, and let $\mathbb{F}$ be a field of characteristic p, where $p||G|$. Prove that $A := \mathbb{F}G$ is not semisimple. (Hint: consider the element $a = \sum_{g \in G} g$, and show that $a^2 = 0$. Next, argue that the left ideal $I = \mathbb{F}Ga$ is one- dimensional and is equal to $\{\alpha a |\ \alpha \in \mathbb{F}\}$. If A is semisimple, then $A = I \oplus J$, for some left ideal $J \subseteq A$. Now write $1 \in A$ as $1 = \alpha a + \beta$, where $\beta \in J$. What's the problem?)

Chapter 6

Ring Structure Theory

6.1 The Jacobson Radical and Semisimple Artinian Rings

In *Theorem* 5.9.5 of *Section* 5.9, we saw that rings all of whose left modules were semisimple were essentially classified (as direct sums of matrix rings). In the present section we shall define an ideal which serves as an "obstruction" of the above condition.

Let R be a ring. Define the *Jacobson radical* of R by setting

$$\mathcal{J}(R) \;=\; \{r \in R |\; rM = 0 \text{ for every irreducible } R\text{-module } M\}.$$

It is clear that $\mathcal{J}(R)$ is a left ideal of R. To see that it is also a right ideal of R, let $x \in \mathcal{J}(R)$ and let $r \in R$. If M is an irreducible R-module, then $xrM \subseteq xM = 0$; since M was arbitrary, we conclude that $xr \in \mathcal{J}(R)$. Let is now denote by $\mathcal{J}'(R)$ the set of all elements of R that kill every irreducible *right* R-module. Thus $\mathcal{J}'(R)$ is also a 2-sided ideal of R. We'll see momentarily that $\mathcal{J}'(R) = \mathcal{J}(R)$.

Here's our main characterization of $\mathcal{J}(R)$.

THEOREM 6.1.1 *The following ideals in R are identical.*

(1) $\mathcal{J}(R)$.

(2) $\cap_{\mathcal{M}}\mathcal{M}$, where $\mathcal{M}$ ranges over all maximal left ideals of R.

(3) $\cup_I I$, where I ranges over all left ideals of R such that $1 + I$ consists entirely of units.

(4) $\{r \in R | 1 + arb$ *is a unit in* R *for all* $a, b \in R\}$.

(5) $\mathcal{J}'(R)$.

(6) $\cap_{\mathcal{M}} \mathcal{M}$, *where* $\mathcal{M}$ *ranges over all maximal right ideals of* R.

(7) $\cup_I I$, *where* I *ranges over all right ideals of* R *such that* $1 + I$ *consists entirely of units.*

An element $r \in R$ is said to be *nilpotent* if $r^n = 0$ for some positive integer n. An ideal $I \subseteq R$ is called *nil* if every element of I is nilpotent. Finally, an ideal $I \subseteq R$ is *nilpotent* if $I^n = 0$ for some positive integer n. Note that every nilpotent ideal is nil.

Example 1. Let $\mathbf{F}$ be a field and let

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbf{F} \right\}.$$

Now set

$$I = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in \mathbf{F} \right\}.$$

Note that I is nilpotent.

Example 2. Let p be a prime, let n be a positive integer, and let $R = \mathbf{Z}/(p^n)$. For any positive integer m, the ideal $p^m R$ is nilpotent, hence nil. (See *Exercise* 8, below.)

Example 3. Here is an example of an ideal I in a ring R such that I is nil but not nilpotent. Let $\mathbf{F}$ be a field, and set $R = \mathbf{F}[x_1, x_2, x_3, \ldots]$, a polynomial ring in an infinite number of indeterminates. Let $A \subseteq R$ be the ideal generated by $\{x_1^2, x_2^3, x_3^4, \ldots\}$, and set $\bar{R} = R/A$. If $r \in R$ let $\bar{r} \in \bar{R}$ denote the image of r in $\bar{R}$ under the canonical map $R \to \bar{R}$. If $\bar{I} \subseteq \bar{R}$ is the ideal $(\bar{x}_1, \bar{x}_2, \ldots)$, then one easily checks that $\bar{I}$ is nil. On the other hand, if n is a positive integer, note that $0 \neq \bar{x}_n^n \in \bar{I}$, and so $\bar{I}$ is not nilpotent.

PROPOSITION 6.1.2 *If* $I \subseteq R$ *is a nil left ideal, then* $I \subseteq \mathcal{J}(R)$.

COROLLARY 6.1.2.1 *If* $I \subseteq R$ *is a nilpotent left ideal, then* $I \subseteq \mathcal{J}(R)$.

LEMMA 6.1.3 *Let* R *be a ring and let* I *be a non-nilpotent minimal left ideal of* R. *Then* I *contains a non-zero idempotent.*

COROLLARY 6.1.3.1 *Let $I \subseteq R$ be as above. Then $R = I \oplus I'$, for some left ideal $I' \subseteq R$. More generally, if J is a left ideal of R, and if $I \subseteq J$ is a non-nilpotent minimal left ideal of R, then $J = I \oplus J'$, for some left ideal $J' \subseteq J$ of R.*

PROPOSITION 6.1.4 (NAKAYAMA'S LEMMA) *Let M be a finitely generated R-module. Then $\mathcal{J}(R)M = M$ if and only if $M = 0$.*

The ring R is called *left Artinian* if the left R-module R is an Artinian module. Similarly we can define what it means for R to be *right Artinian, left Noetherian* and *right Noetherian*.

We now have the following.

THEOREM 6.1.5 *Let R be a left Artinian ring. Then the Jacobson radical $\mathcal{J}(R)$ is a nilpotent ideal.*

A ring R is called *semisimple* if $\mathcal{J}(R) = 0$. Note that this is different from saying that the left R-*module* R is *semisimple*. For example the reader can easily check that $\mathbf{Z}$ is a semisimple *ring*, but is certainly not a semisimple *module*. Here's the relationship between the two concepts of semisimplicity:

THEOREM 6.1.6 *Let R be a left Artinian ring. Then the following are equivalent.*

(i) R is a semisimple **ring**.

*(ii) R is a semisimple left R-***module**.

COROLLARY 6.1.6.1 (WEDDERBURN'S THEOREM) *A semisimple left Artinian ring is a direct sum of matrix rings over division rings.*

COROLLARY 6.1.6.2 *A semisimple left Artinian ring is also right Artinian.*

Finally, we have the following mildly surprising result.

THEOREM 6.1.7 (HOPKIN'S THEOREM) *A left Artinian ring is left Noetherian.*

EXERCISES 6.1

1. Consider the infinite matrix ring $R = \mathrm{M}_\infty(\mathbb{F})$ over the field $\mathbb{F}$, which consists of matrices with countably many rows and columns, but such that each matrix has only finitely many non-zero elements in any given row or column. Show that in R, there are elements that are left (right) invertible, but not right (left) invertible. (Hint: Let A be the matrix having 1's on the super-diagonal, and 0's elsewhere. Let B be the matrix having 1's on the sub-diagonal and 0's elsewhere. Note that $AB = I$.)

2. Let R be a ring and assume that the element $a \in R$ has a unique left inverse. Prove that a is invertible, i.e., the left inverse of a is also the right inverse of a.

3. Let $a \in R$ and assume that a has more than one left inverse. Prove that in fact a has infinitely many left inverses (thus R is infinite). (Hint: If a has exactly n left inverses $b_1, b_2, \ldots, b_n$, set $d_i = b_1 + 1 - ab_i,\ i = 1, 2, \ldots, n$. Note that the elements d_i are pairwise distinct and are also left inverses for a. If $d_i = b_1$ for some i, obtain a contradiction.)

4. Let R be a ring such that for all $0 \neq a \in R$, $Ra = R$. Prove that R is a division ring.

5. Let R be a ring without zero divisors such that R has only finitely many left ideals. Prove that R is a division ring. (Hint: Assume that $0 \neq a \in R$ and $Ra \neq R$. Look at the sequence $Ra \supseteq Ra^2 \supseteq \cdots$.)

6. Let R be a ring and let L be the intersection of all non-zero left ideals in R. If $L^2 \neq 0$, then R is a division ring. (Hint: By *Lemma* 6.1.3, we have $L = Re$, where e is a non-zero idempotent of L. Next, if $xe \neq x$ for some $x \in R$, then $xe - x$ is in the left annihilator $\mathrm{Ann}_R(e) = \{r \in R \mid re = 0\}$ of e. Since $\mathrm{Ann}_R(e)$ is also a left ideal of R, we get $L \subseteq \mathrm{Ann}_R(e)$, which is a contradiction. Therefore $xe = x$ for all $x \in R$, so $L = R$. This implies that $Ra = R$ for all $0 \neq a \in R$; apply *Exercise* 4.)

7. Assume that the ring R has no non-zero nilpotent elements. Prove that every idempotent of R is contained in the center of R (i.e., commutes with every element of R).

8. Let n be a positive integer, and let $R = \mathbb{Z}/(n)$. Describe the nilpotent ideals in R.

9. If R is a ring, prove that $\mathcal{J}(R)$ contains no non-zero idempotents.

10. Let R be the ring of all continuous real-valued functions on the interval $[0, 1]$. Prove that $\mathcal{J}(R) = 0$.

11. Let R be a ring. Prove that $\mathcal{J}(R/\mathcal{J}(R)) = 0$.

12. Let R be a left Artinian ring, and let $I \subseteq R$ be a nil ideal. Prove that I is actually nilpotent.

13. Let $\mathbb{F}$ be a field, and let R be the ring

$$R = = \left\{ \begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ 0 & 0 & a_7 \end{bmatrix} \mid a_i \in \mathbb{F} \right\}.$$

    Compute $\mathcal{J}(R)$.

14. Let R be a left Artinian ring, and let $I \subseteq R$ be a non-nilpotent left ideal. Prove that I contains a non-zero idempotent.

15. Let R be an Artinian ring. Prove that the following conditions are equivalent.

    (a) R is local, i.e., it has a unique maximal ideal.

    (b) R contains no non-trivial (i.e. $\neq 1$) idempotents.

    (c) If N is the radical of R, then R/N is a division ring.

Chapter 7

Tensor Products

7.1 Tensor Product as an Abelian Group

Throught this chapter R will denote a ring with identity. All modules will be unital.

Let M be a right R-module, let N be a left R-module, and let A be an abelian group. By a *balanced* map, we mean a map

$$f : M \times N \longrightarrow A,$$

such that

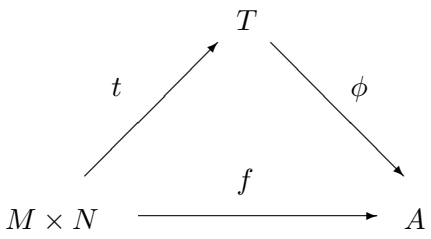
(i) $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$,

(ii) $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$,

(iii) $f(mr, n) = f(m, rn)$

where $m, m_1, m_2 \in M,\ n, n_1, n_2 \in N,\ r \in R$.

By a *tensor product* of M and N we mean an abelian group T, together with a balanced map $t : M \times N \to T$ such that given any abelian group A, and any balanced map $f : M \times N \to A$ there exists a unique abelian group homomorphism $\phi : T \to A$, making the diagram below commute



The following is the usual application of "abstract nonsense."

PROPOSITION 7.1.1 *The tensor product of the right R-module M and the left R-module N is unique up to abelian group isomorphism.*

This leaves the question of existence, which is also not very difficult. Indeed, given M and N as above, and let F be the free abelian group on the set $M \times N$. Let B be the subgroup of F generated by elements of the form

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n),$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2),$$

$$(mr, n) - (m, rn),$$

where $m, m_1, m_2 \in M,\ n, n_1, n_2 \in N,\ r \in R$. Write $M \otimes_R N = F/B$ and set $m \otimes n = (m, n) + B \in M \otimes_R N$. Therefore, in $M \otimes_R N$ we have the relations

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n,$$

$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2,$$

$$mr \otimes n = m \otimes rn,$$

$m, m_1, m_2 \in M,\ n, n_1, n_2 \in N,\ r \in R$. Furthermore, $M \otimes_R N$ is generated by all "simple tensors" $m \otimes n,\ m \in M, n \in N$.

Define the map $t : M \times N \to M \otimes_R N$ by setting $t(m, n) = m \otimes n,\ m \in M,\ n \in N$. Then, *by construction*, t is a balanced map. In fact

PROPOSITION 7.1.2 *The abelian group $M \otimes_R N$, together with the balanced map $t : M \times N \to M \otimes_R N$ is a tensor product of M and N.*

A couple of simple examples are in order here.

1. If N is a left R-module, then $R \otimes_R N \cong N$ as abelian groups. The proof simply amounts to showing that the map $t : R \times N \to N$ given by $t(r, n) = rn$ is balanced and is universal with respect to balanced maps into abelian groups. Invoke *Proposition* 1.

2. If A is any torsion abelian group and if D is any divisible abelian group, then $D \otimes_{\mathbb{Z}} A = 0$. If $a \in A$, let $0 \neq n \in \mathbb{Z}$ be such that $na = 0$. Then for any $d \in D$ there exists $d' \in D$ such that $d'n = d$. Therefore $d \otimes a = d'n \otimes a = d' \otimes na = d' \otimes 0 = 0$. Therefore every simple tensor in $D \otimes_{\mathbb{Z}} A$ is zero; thus $D \otimes_{\mathbb{Z}} A = 0$.

Next we wish to discuss the mapping or "functorial" properties of the tensor product.

PROPOSITION 7.1.3 *Let $f : M \to M'$ be a right R-module homomorphism and let $g : N \to N'$ be a left R-module homomorphism. Then there exists a unique abelian group homomorphism $f \otimes g : M \otimes_R N :\to M' \otimes_R N'$ such that for all $m \in M,\ n \in N,\ (f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.*

In particular, the following observation is the basis of all so-called "homological" properties of $\otimes$.

PROPOSITION 7.1.4

(i) Let $M' \xrightarrow{\mu} M \xrightarrow{\epsilon} M'' \to 0$ be an exact sequence of right R-modules, and let N be a left R-module. Then the sequence

$$M' \otimes_R N \xrightarrow{\mu \otimes 1_N} M \otimes_R N \xrightarrow{\epsilon \otimes 1_N} M'' \otimes_R N \to 0$$

is exact.

(ii) Let $N' \xrightarrow{\mu} N \xrightarrow{\epsilon} N'' \to 0$ be an exact sequence of left R-modules, and let M be a right R-module. Then

$$M \otimes_R N' \xrightarrow{1_M \otimes \mu} M \otimes_R N \xrightarrow{1_M \otimes \epsilon} M \otimes_R N'' \to 0$$

is exact.

We hasten to warn the reader that in *Proposition* 4 (i) above, even if $M' \xrightarrow{\mu} M$ is been injective, it need not follow that $M' \otimes_R N \xrightarrow{\mu \otimes 1_N} M \otimes_R N$ is

injective. (A similar comment holds for part (ii).) Put succinctly, the tensor product does not take short exact sequences to short exact sequences. In fact a large portion of "homological algebra" is devoted to the study of functors that do not preserve exactness. As an easy example, consider the short exact sequence of abelian groups (i.e. $\mathbb{Z}$-modules):

$$\mathbb{Z} \stackrel{\mu_2}{\to} \mathbb{Z} \to \mathbb{Z}/(2) \to 0,$$

where $\mu_2(a) = 2a$. If we tensor the above short exact sequence on the right by $\mathbb{Z}/(2)$, we get the sequence

$$\mathbb{Z}/(2) \stackrel{0}{\to} \mathbb{Z}/(2) \stackrel{\cong}{\to} \mathbb{Z}/(2).$$

Thus the exactness breaks down.

EXERCISES 7.1

1. Let M_1, M_2 be right R-modules and let N be a left R-module. Prove that
$$(M_1 \oplus M_2) \otimes_R N \cong M_1 \otimes_R N \oplus M_2 \otimes_R N.$$

2. Let N be a left R-module. Say that N is *flat* if for any injective homomorphism of right R-modules $M' \to M$, then the abelian group homomorphism $M' \otimes N \to M \otimes N$ is also injective. (The obvious analogous definition also applies to right R-modules.) Prove that if N is projective then N is flat.

3. Let A be an abelian group. If n is a positive integer, prove that
$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} A \cong A/nA.$$

4. Let m, n be positive integers and let $k = \text{g.c.d}(m, n)$. Prove that
$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z}.$$

7.2 Tensor Product as a Left S-Module

In the last section we started with a right R-module M and a left R-module N and constructed the abelian group $M \otimes_R N$. In this section, we shall discussion conditions that will enable $M \otimes_R N$ to carry a module structure. To this end let S, R be rings, and let M be an abelian group. We say that M is an (S, R)-*bimodule* if M is a left S-module and a right R-module and that for all $s \in S, m \in M, r \in R$ we have

$$(sm)r \;=\; s(mr).$$

Next assume that M is an (S, R)-bimodule and that N is a left R-module. As in the last section we have the abelian group $M \otimes_R N$. In order to give $M \otimes_R N$ the structure of a left S-module we need to construct a ring homomorphism

$$\phi : S \to \mathrm{End}_{\mathbb{Z}}(M \otimes_R N);$$

this allows for the definition of an S-scalar multiplication: $s{\cdot}a = \phi(s)(a),\ a \in M \otimes_R N$. For each $s \in S$ define $f_s : M \times N \to M \otimes_R N$ by setting $f_s(m, n) = sm \otimes n,\ s \in S, m \in M, n \in N$. Then f_s is easily checked to be a balanced map; by the universality of tensor product, there exists a unique abelian group homomorphism $\phi_s : M \otimes_R N \to M \otimes_R N$ satisfying $\phi_s(m \otimes n) = sm \otimes n$. Note that the above uniqueness implies that $\phi_{s_1+s_2} = \phi_{s_1} + \phi_{s_2}$ and that $\phi_{s_1 s_2} = (\phi_{s_1}) \cdot (\phi_{s_2})$. In turn, this immediately implies that the mapping $\phi : S \to \mathrm{End}_{\mathbb{Z}}(M \otimes_R N), \phi(s) = \phi_s$ is the desired ring homomorphism. In other words, we have succeeded in giving $M \otimes_R N$ the structure of a left S-module.

The relevant universal property giving rise to a module homomorphism is the following:

PROPOSITION 7.2.1 *let M be an (S, R)-bimodule, and let M be a left R-module. If K is a left S-module and if $f : M \times N \to K$ is a balanced map which also satisfies $f(sm, n) = s \cdot f(m, n), s \in S,\ m \in M,\ n \in N$, then the induced abelian group homomorphism $\phi : M \otimes_R N \to K$ is a left S-module homomorphism.*

Of particular importence is the following. Assume that R is a commutative ring. If M is a left R-module, then M can be regarded also as a right

R-module simply by declaring that $m \cdot r = r \cdot m, r \in R, m \in M$. (How does the commutativity of R comes into play?) Therefore, in this situation, if M, N are both left R-modules, we can form the left R-module $M \otimes_R N$. Probably the most canonical example in this situation is the construction of the vector space $V \otimes_{\mathbb{F}} W$, where V, W are both $\mathbb{F}$-vector spaces. Also, in this specific situation, we can say more:

PROPOSITION 7.2.2 *Let V and W be $\mathbb{F}$-vector spaces with bases $\{v_1, \ldots, v_n\}$, $\{w_1, \ldots, w_m\}$, respectively. Then $V \otimes_{\mathbb{F}} W$ has basis $\{v_i \otimes w_j |\ 1 \leq i \leq n, 1 \leq j \leq m\}$. In particular,*

$$\dim V \otimes_{\mathbb{F}} W \ = \ \dim V \cdot \dim W.$$

The obvious analogue of the above is also true in the infinite-dimensional case; see *Exercise* 2, below.

EXERCISES 7.2

1. Let R be a ring and let M be a left R-module. Prove that $R \otimes_R M \cong M$ *as left R-modules.*
2. V and W be $\mathbb{F}$-vector spaces with bases $\{v_\alpha |\ \alpha \in \mathcal{A}\}$, $\{w_\beta |\ \beta \in \mathcal{B}\}$. Then $V \otimes_{\mathbb{F}} W$ has basis $\{v_\alpha \otimes w_\beta |\ \alpha \in \mathcal{A}, \beta \in \mathcal{B}\}$.
3. Let W be an $\mathbb{F}$-vector space and let $T : V_1 \to V_2$ be an injective linear transformation of $\mathbb{F}$-vector spaces. Prove that the sequence $1 \otimes T : W \otimes V_1 \to W \otimes V_2$ is injective.
4. Let $T : V \to V$ be a linear transformation of the finite-dimensional $\mathbb{F}$-vector space V. If $\mathbb{K} \supseteq \mathbb{F}$ is a field extension, prove that $m_{T,\mathbb{F}}(x) = m_{1 \otimes T, \mathbb{K}}(x)$. (Hint: Apply *Exercise* 3, above.)
5. Let $\mathbb{F}$ be a field and let $A \in \mathrm{M}_n$, $B \in \mathrm{M}_m$ be square matrices. Define the *Kronecker* (or *tensor*) product $A \otimes B$ as follows. If $A = [a_{ij}]$, $B = [b_{kl}]$, then $A \otimes B$ is the block matrix $[D_{pq}]$, where each D_{pq} is the $m \times m$ matrix $D_{pq} = a_{pq}B$. Thus, for instance, if

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \quad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

then

$$A \otimes B \;=\; \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}.$$

Now Let V, W be $\mathbb{F}$-vector spaces with ordered bases $\mathcal{A} = (v_1, v_2, \ldots, v_n)$, $\mathcal{B} = (w_1, w_2, \ldots, w_m)$, respectively. Let $T : V \to V,\ S : W \to W$ be linear transformations with matrix representations $T_{\mathcal{A}} = A,\ S_{\mathcal{B}} = B$. Assume that $\mathcal{A} \otimes \mathcal{B}$ is the ordered basis of $V \otimes_{\mathbb{F}} W$ given by $\mathcal{A} \otimes \mathcal{B} = (v_1 \otimes w_1, v_1 \otimes w_2, \ldots, v_1 \otimes w_m; v_2 \otimes w_1, \ldots, v_2 \otimes w_m; \ldots, v_n \otimes w_m)$. Show that the matrix representation of $T \otimes S$ relative to $\mathcal{A} \otimes \mathcal{B}$ is given by $(T \otimes S)_{\mathcal{A}\otimes\mathcal{B}} = A \otimes B$.

6. Let V be a two-dimensional vector space over the field $\mathbb{F}$, and let $T, S : V \to V$ be linear transformations. Assume that $m_T(x) = (x-a)^2,\ m_S(x) = (x-b)^2$. (Therefore T and S can be represented by Jordan blocks, $J_2(a),\ J_2(b)$, respectively.) Compute the invariant factors of $T \otimes S : V \otimes V \to V \otimes V$. (See *Exercise* 5 of *Section* 5.4).

7. Let M be a left R-module, and let $I \subseteq R$ be a 2-sided ideal in R. Prove that, as left R-modules,

$$R/I \otimes_R M \cong M/IM.$$

8. Let R be a commutative ring and let M_1, M_2, M_3 be R-modules. Prove that there is an isomorphism of R-modules:

$$(M_1 \otimes_R M_2) \otimes_R M_3 \;\cong\; M_1 \otimes_R (M_2 \otimes_R M_3).$$

9. Let R be a commutative ring and let $M_1, M_2, \ldots, M_k$ be R-modules. Assume that there is an R-multilinear map

$$f : M_1 \times M_2 \times \ldots \times M_k \longrightarrow N$$

into the R-module N. Prove that there is a unique R-module homomorphism

$$\phi : M_1 \otimes_R M_2 \otimes_R \ldots \otimes_R M_k \longrightarrow N$$

satisfying $\phi(m_1 \otimes m_2 \otimes \ldots \otimes m_k) = f(m_1, m_2, \ldots, m_k)$, where all $m_i \in M_i,\ i = 1, \ldots k$.

10. Let G be a finite group and let H be a subgroup of G. Let $\mathbb{F}$ be a field, and let $\mathbb{F}G, \mathbb{F}H$ be the $\mathbb{F}$-group algebras, as in *Section* 5.10. If V is a finite-dimensional $\mathbb{F}H$-module, prove that

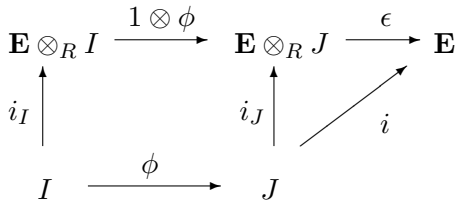
$$\dim \mathbb{F}G \otimes_{\mathbb{F}H} V \ = \ [G : H] \cdot \dim V.$$

11. Let A be an abelian group. Prove that a ring structure on A is equivalent to an abelian group homomorphism $\mu : A \otimes_{\mathbb{Z}} A \to A$, together with an element $e \in A$ such that $\mu(e \otimes a) = \mu(a \otimes e) = a$, for all $a \in A$, and such that

$$\begin{array}{ccc} A \otimes_{\mathbb{Z}} A \otimes_{\mathbb{Z}} A & \xrightarrow{1 \otimes \mu} & A \otimes_{\mathbb{Z}} A \\ \downarrow{\scriptstyle \mu \otimes 1} & & \downarrow{\scriptstyle \mu} \\ A \otimes_{\mathbb{Z}} A & \xrightarrow{\mu} & A \end{array}$$

commutes. (The above diagram, of course, stipulates that multiplication is associative.)

12. Let R be a Dedekind domain with fraction field $\mathbf{E}$, and let $I, J \subseteq \mathbf{E}$ be fractional ideals. If $I \cong_R J$, prove that $[I] = [J] \in \mathcal{C}_R$ (the ideal class group of R). (The converse is easier, see *Exercise* 4, of *Section* 5.1. Hint: Consider the commutative diagram below:



where $i_I,\ i_J$ are injections, given by $i_I(a) = 1 \otimes a,\ i_J(b) = 1 \otimes b,\ a \in I, b \in J,\ \epsilon : \mathbf{E} \otimes J \to \mathbf{E}$ is given by $\epsilon(\lambda \otimes b) = \lambda b$, and where $i : J \hookrightarrow \mathbf{E}$. Note also that $1 \otimes \phi : \mathbf{E} \otimes_R I \to \mathbf{E} \otimes J$ is a $\mathbf{E}$-linear transformation.

Next, if $0 \neq a_0 \in I$, note that for all $a \in I$, we have $1 \otimes a = a(a_0^{-1} \otimes a_0)$. Indeed, $a(a_0^{-1} \otimes a_0) = aa_0^{-1}(1 \otimes a) = a_0^{-1}(a \otimes a_0) = a_0^{-1}(1 \otimes aa_0) =$

$a_0^{-1}(a_0 \otimes a) = a_0^{-1}a_0(1 \otimes a) = 1 \otimes a$. Thus, if we set $\alpha_0 = \epsilon(1 \otimes \phi)(a_0^{-1} \otimes a_0)$ we have $\phi(a) = \alpha) \cdot a \in \mathbf{E}$. In other words, $\phi : I \to J$ is given by left multiplication by α_0, i.e., $J = \alpha_0 I$ and the result follows.)

7.3 Tensor Product as an Algebra

Throughout this section R denotes a commutative ring. Thus we need not distinguish between left or right R-modules. The R-module A is called an R-algebra if it has a ring structure that satisfies $(ra_1)a_2 = a_1(ra_2),\ r \in R,\ a_1, a_2 \in A$. If A, B are R-algebras, we shall give a natural R-algebra structure on the tensor product $A \otimes_R B$. Recall from *Section* 2 that $A \otimes_R B$ is already an R-module with scalar multiplication satisfying

$$r(a \otimes b) \ = \ ra \otimes b \ = \ a \otimes rb,$$

$a \in A,\ b \in B,\ r \in R$.

To obtain an R-algebra structure on $A \otimes_R B$, we shall apply *Exercise* 9 of the previous section. Indeed, we map

$$f : A \times B \times A \times B \longrightarrow A \otimes_R B,$$

by setting $f(a_1, b_1, a_2, b_2) = a_1a_2 \otimes b_1b_2,\ a_1, a_2 \in A,\ b_1, b_2 \in B$. Then f is clearly multilinear; this gives a mapping

$$\Delta : (A \otimes_R B) \otimes_R (A \otimes_R B) \longrightarrow A \otimes_R B.$$

Thus we define the multiplication on $A \otimes_R B$ by setting $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2,\ a_1, a_2 \in A,\ b_1, b_2 \in B$. One now has the targeted result:

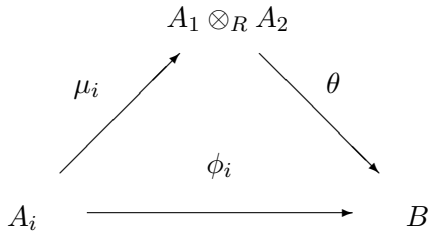
PROPOSITION 7.3.1 *Let A, B be R-algebras. Then there is an R-algebra structure on $A \otimes_R B$ such that $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$.*

EXERCISES 7.3

1. Let $\mathbb{F}$ be a field, and let A be a finite-dimensional $\mathbb{F}$-algebra that is also an integral domain. Prove that A is a field, algebraic over $\mathbb{F}$. (Of course, this is simply a restatement of *Exercise* 9 of *Section* 2.1.)

2. Let A_1, A_2 be commutative R-algebras. Prove that $A_1 \otimes_R A_2$ satisfies a universal condition reminiscient of that for direct sums of R-modules. Namely, there exist R-algebra homomorphisms $\mu_i : A_i \to A_1 \otimes_R A_2,\ i = 1, 2$ satisfying the following. If B is any commutative R-algebra such that there exist R-algebra homomorphisms $\phi_i : A_i \to B$,

there there exists a unique R-algebra homomorphism $\theta : A_1 \otimes_R A_2 \to B$ such that each diagram



commutes.

3. Prove that $R[x] \otimes_R R[y] \cong R[x, y]$ as R-algebras.

4. Let G_1, G_2 be finite groups with $\mathbb{F}$-group algebras as in *Section* 5.10. Prove that $\mathbb{F}[G_1 \times G_2] \cong \mathbb{F}G_1 \otimes_{\mathbb{F}} \mathbb{F}G_2$.

5. Let A be an algebra over the commutative ring R. We say that A is a *graded* R-algebra if A admits a direct sum decomposition $A = \bigoplus_{r=0}^{\infty} A_r$, where $A_r \cdot A_s \subseteq A_{r+s}$ for all $r, s \geq 0$. (We shall discuss graded algebras in somewhat more detail in the next section.) We say that the graded R-algebra A is *graded-commutative* (or just commutative !) if whenever $a_r \in A_r,\ a_s \in A_s$ we have $a_r a_s = (-1)^{rs} a_s a_r$.

   Now let $A = \bigoplus_{r=0}^{\infty} A_r,\ B = \bigoplus_{s=0}^{\infty} B_s$ be graded-commutative R-algebras. Prove that there is a graded-commutative algebra structure on $A \otimes_R B$ satisfying

$$(a_r \otimes b_s) \cdot (a_p \otimes b_q) = (-1)^{sp}(a_r a_p \otimes b_s b_q),$$

   $a_r \in A_r,\ a_p \in A_p,\ b_s \in B_s,\ b_q \in B_q$. This is usually the intended meaning of "tensor product" in the category of graded-commutative R-algebras.

7.4 Tensor, Symmetric and Exterior Algebra of a Vector Space

Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. We define a sequence $T^r(V)$ of $\mathbb{F}$-vector spaces by setting $T^0(V) = \mathbb{F}$, $T^1(V) = V$, and in general,

$$T^r(V) \;=\; \bigotimes_{i=1}^{r} V \;=\; V \otimes_{\mathbb{F}} \otimes \cdots \otimes_{\mathbb{F}} V \text{ (r factors)}.$$

Note that "$\otimes$" gives a natural "multiplication:"

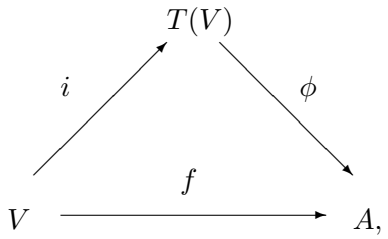
$$\otimes : T^r(V) \times T^s(V) \longrightarrow T^{r+s}(V),$$

where $(\alpha, \beta) \mapsto \alpha \otimes \beta$. As a result, if we set

$$T(V) \;=\; \bigoplus_{r=0}^{\infty} T^r(V),$$

we have a natural $\mathbb{F}$-algebra structure on $T(V)$, with multiplication given by $\otimes$. The algebra $T(V)$ so determined is called the *tensor algebra* of V.

If we denote by $i : V \to T(V)$ the composition $V = T^1(V) \hookrightarrow T(V)$, then we have the following universal mapping property. If A is any $\mathbb{F}$-algebra, and if $f : V \to A$ is any linear transformation, then there exists a unique $\mathbb{F}$-algebra homomorphism $\phi : T(V) \to A$ that extends f. In other words, we have the commutative triangle below:



where $i : V \to T(V)$ is the inclusion map.

In order to facilitate discussions of the *symmetric* and *exterior* algebras of the vector space V, we pause to make a few more comments concerning

the tensor algebra $T(V)$ of V. First of all if A is any $\mathbb{F}$-algebra admitting a direct sum decomposition $A = \bigoplus_{i=0}^{\infty} A_r$ such that for all indices r, s we have $A_r A_s \subseteq A_{r+s}$, then we call A a *graded algebra*. Elements of A_i are called *homogeneous elements* of *degree* r. Therefore, it is clear that the tensor algebra $T(V)$ is a graded algebra.

Next, if A is a graded algebra and if $I \subseteq A$ is a 2-sided ideal in A, we say that I is a *homogeneous* ideal (sometimes called a *graded* ideal) , if $I = \bigoplus_{r=0}^{\infty} A_r \cap I$.

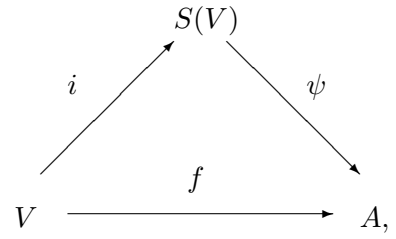
The following is pretty routine:

PROPOSITION 7.4.1 *Let A be a graded algebra and let I be a 2-sided ideal generated by homogeneous elements. Then I is a homogeneous ideal. In this case $A/I = \bigoplus_{r=0}^{\infty} A_r/(A_r \cap I)$ is a graded algebra.*

With the above in place, we now define the *symmetric algebra* of the vector space V as the quotient algebra $S(V) = T(V)/I$, where I is the homogeneous ideal generated by tensors of the form $v \otimes w - w \otimes v,\ v, w \in V$. By *Proposition* 7.4.1, $S(V) = \bigoplus S^r(V)$ is a graded algebra, where $S^r(V) = T^r(V)/(T^r(V) \cap I)$.

Multiplication in $S(V)$ is usually denoted by juxtaposition; in particular, if $v, w \in V \subseteq S(V)$, then vw is the product of v and w. Equivalently vw is just the coset: $vw = v \otimes w + I$, and $vw = wv\ v, w \in V$. As a result, if $\{v_1, v_2, \ldots, v_n\}$ is a basis of V, then $S^r(V)$ is spanned by elements of the form $v_1^{e_1} v_2^{e_2} \cdots v_n^{e_n}$, where $e_1 + e_2 + \cdots + e_n = r$. In fact, these elements form a basis of $S^r(V)$; see *Proposition* 7.4.2, below.

Note that there is a very natural isomorphism $i : V \xrightarrow{\cong} S^1(V) \hookrightarrow S(V)$. The symmetric algebra $S(V)$ then enjoys the following universal property. If A is any commutative $\mathbb{F}$-algebra, and if $f : V \to A$ is any linear transformation, then there exists a unique $\mathbb{F}$-algebra homomorphism $\psi : S(V) \to A$ that extends f. In other words, we have the commutative triangle below:

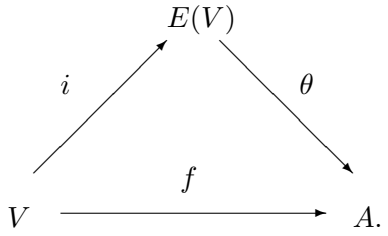


Actually the symmetric algebra is a pretty familiar object:

PROPOSITION 7.4.2 *Let V have $\mathbb{F}$-dimension n, and set $A = \mathbb{F}[x_1, x_2, \ldots, x_n]$, where $x_1, x_2, \ldots x_n$ are indeterminates over $\mathbb{F}$. Then $S(V) \cong A$.*

Finally, we turn to the so-called *exterior algebra* of the vector space V. This time we start with the homogeneous ideal $J \subseteq T(V)$ of $T(V)$ generated by homogeneous elements $v \otimes v,\ v \in V$. By *Proposition* 7.4.1, if we set $E(V) = T(V)/J$, $\bigwedge^r(V) = T^r(V)/(T^r(V) \cap J)$, then then $E(V) = \bigoplus_{r=0}^{\infty} \bigwedge^r(V)$ is a graded algebra (sometimes denoted $\bigwedge V$).

Again, we have a natural inclusion $i : V \hookrightarrow E(V)$, and $E(V)$ has the predictable universal mapping property: If If A is any $\mathbb{F}$-algebra, and if $f : V \to A$ is any linear transformation satisfying $f(v)^2 = 0$ for all $v \in V$, then there exists a unique $\mathbb{F}$-algebra homomorphism $\theta : E(V) \to A$ that extends f. In other words, we have the commutative triangle below:



If we regard V as a subspace of $E(V)$ via the map i above, and if $v, w \in V$, we denote the product of v and w by $v \wedge w$; again, this is just the coset $v \wedge w = v \otimes w + J$. Therefore, it is clear that $v \wedge v = 0$, and if $v, w \in V$ we have $(v+w) \wedge (v+w) = 0$, which implies that $v \wedge w = -w \wedge v$. In particular, if $\dim V = n$ and if $v_1, v_2, \ldots v_r \in V$, where $r > n$, then $v_1 \wedge v_2 \wedge \cdots \wedge v_r = 0$. Therefore, $r > n$ implies that $\bigwedge^r(V) = 0$ for all $m > n$.

PROPOSITION 7.4.3 *Assume that V is finite dimensional and that $\mathcal{A} = \{v_1, \ldots, v_n\}$ is a basis of V. Let $R = \{i_1, \ldots, i_r\}$, where $1 \leq i_1 < \cdots < i_r \leq n$, set $N = \{1, 2, \ldots, n\}$, and set $v_R = v_{i_1} \wedge \cdots \wedge v_{i_r}$. Then $\{v_R |\ R \subseteq \mathcal{A}\}$ spans $E(V)$ as a vector space. In particular dim $E(V) \leq 2^n$.*

In fact, in the above proposition, we get equality: $\dim E(V) = 2^n$. To prove this, it suffices to prove that $\dim \bigwedge^r V = \binom{n}{r}$. The method of doing

this is interesting in its own right; we sketch the argument here. First of all, let $f_1, f_2, \ldots, f_r \in V^*$ (the $\mathbb{F}$-dual of V), and define

$$F \;=\; F_{(f_1,f_2,\ldots,f_r)} : V \times V \times \cdots \times V \longrightarrow \mathbb{F}$$

by setting $F(w_1, w_2, \ldots, w_r) = f_1(w_1)f_2(w_2)\cdots f_r(w_r)$. It is routine to check that F is multilinear; thus there exists a unique linear map

$$\phi \;=\; \phi_{(f_1,f_2,\ldots,f_r)} : V \otimes V \otimes \cdots \otimes V \longrightarrow \mathbb{F}$$

satisfying $\phi(w_1 \otimes w_2 \ldots \otimes w_r) = f_1(w_1)f_2(w_2)\cdots f_r(w_r)$.

Now let $\{v_1, v_2, \ldots, v_n\}$ be the above basis of V, and let $f_1, f_2, \ldots, f_n$ be the dual functionals, i.e., satisfying $f_i(v_j) = \delta_{ij}$. Let $R = \{i_1, \ldots, i_r\}$, where $1 \leq i_1 < \cdots < i_r \leq n$, and define the linear map

$$\phi_R \;=\; \sum_{\sigma \in S_r} sgn(\sigma)\phi_{(f_{i_\sigma(1)}, f_{i_\sigma(2)}, \cdots f_{i_\sigma(r)})} : V \otimes V \otimes \cdots \otimes V \longrightarrow \mathbb{F}.$$

It is easy to check that ϕ_R factors through $\bigwedge^r V$, giving a linear map

$$f_K : \bigwedge^r V \longrightarrow \mathbb{F},$$

satisfying

$$f_R(w_1 \wedge \cdots \wedge w_r) = \sum_{\sigma \in S_r} sgn(\sigma) f_{i_\sigma(1)}(w_1) f_{i_\sigma(2)}(w_2) \cdots f_{i_\sigma(r)}(w_r).$$

From the above, it follows immediately that $f_R(v_{R'}) = \delta_{RR'}$, which implies that the set $\{v_R|\ |R| = r\}$ is a linearly independent subset of $\bigwedge^r V$. This proves what we wanted, viz.,

THEOREM 7.4.4 *The exterior algebra $E(V)$ of the n-dimensional vector space V has dimension 2^n.*

EXERCISES 7.4

1. Assume that the $\mathbb{F}$-vector space V has dimension n. For each $r \geq 0$, compute the $\mathbb{F}$-dimension of $S^r(V)$.

2. Let V and W be $\mathbb{F}$-vector spaces. An n-linear map $f : V \times V \times \cdots \times V \to W$ is called *alternating* if for any $v \in V$, we have

$$f(\ldots, v, \ldots, v, \ldots) = 0.$$

Prove that in this case there exists an $\mathbb{F}$-linear map $\hat{f} : \bigwedge^n V \to W$ such that

$$f(v_1, v_2, \ldots, v_n) = \hat{f}(v_1 \wedge v_2 \wedge \cdots \wedge v_n).$$

In particular, how can the *determinant* be interpreted as a linear functional on $\bigwedge^n V$?

3. Let $T : V \to V$ be a linear transformation, and let r be a non-negative integer. Show that there exists a unique linear transformation $\bigwedge^r T : \bigwedge^r V \to \bigwedge^r V$ satisfying $\bigwedge^r T(v_1 \wedge v_2 \wedge \cdots \wedge v_r) = T(v_1) \wedge T(v_2) \wedge \cdots \wedge T(v_r)$, where $v_1, v_2, \ldots, v_r \in V$.

4. Let $T : V \to V$ be a linear transformation, and assume that $\dim V = n$. Show that $\bigwedge^n T = \det T \cdot 1_{\bigwedge^n V} : \bigwedge^n V \to \bigwedge^n V$.

5. Let G be a group represented on the $\mathbb{F}$-vector space V (see *page* 148). Show that the mapping $G \to \mathrm{GL}_{\mathbb{F}}(\bigwedge^r V)$ given by $g \mapsto \bigwedge^r g$ defines a group representation on $\bigwedge^r V,\ r \geq 0$.

6. Let V be a vector space and let $v \in V$. Define the linear map $\cdot \wedge v : \bigwedge^r V \to \bigwedge^{r+1} V$ by $\omega \mapsto \omega \wedge v$. If $\dim V = n$, compute the dimension of the kernel of $\cdot \wedge v$.

7. Let V be n-dimensional over the field $\mathbb{F}$, and having basis $\{v_1, v_2, \ldots, v_n\}$. For each integer r, $0 \leq r \leq n$, set $E_r(V) = \bigwedge^r V$, and define the linear transformation $\partial_r : E_r(V) \to E_{r-1}(V),\ 1 \leq r \leq n$ on basis elements by setting

$$\partial_r(v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_r}) = \sum_{j=1}^{r} (-1)^{j-1} v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge \widehat{v_{i_j}} \wedge \cdots \wedge v_{i_r},$$

where $\widehat{(\cdot)}$ means *delete the factor* $(\cdot)$. The mapping $\partial_0 : E_1(V) = V \to E_0(V) = \mathbb{F}$ is the mapping determined by $\partial_0(v_i) = 1$, $i = 1, 2, \ldots, n$.

(a) Show that if $r \geq 1$, then $\partial_{r-1}\partial_r = 0 : E_r(V) \to E_{r-2}(V)$.

(b) Define a mapping $h_r : E_r(V) \to E_{r+1}(V)$, $0 \leq r \leq n-1$ by setting $h_r(\eta) = v_1 \wedge \eta$, where $\eta \in E_r(V)$. Show that if $1 \leq r \leq n-1$, then $\partial_{r+1} h_r + h_{r-1}\partial_r = 1_{E_r(V)}$, and that $h_{n-1}\partial_n = 1_{E_n(V)}$, $\partial_1 h_0 = 1_{E_0(V)}$.

(c) Conclude that the sequence

$$0 \to E_n(V) \stackrel{\partial_n}{\to} E_{n-1} \stackrel{\partial_{n-1}}{\to} E_{n-2} \to \cdots \stackrel{\partial_2}{\to} E_1(V) \stackrel{\partial_1}{\to} E_0(V) \to 0$$

is exact.

8. Let V be an $\mathbb{F}$-vector space, and, as in the above exercise, set $E_r(V) = \bigwedge^r V$, $r \geq 0$. An $\mathbb{F}$-linear mapping $\delta : E(V) \to E(V)$ is called an *antiderivation* if for all $\omega \in E_r(V)$, $\eta \in E_s(V)$ we have

$$\delta(\omega \wedge \eta) \;=\; \delta(\omega) \wedge \eta + (-1)^r \omega \wedge \delta(\eta).$$

Now let $f : V \to \mathbb{F}$ be a linear functional, and show that f can be extended uniquely to an antiderivation $\delta : E(V) \to E(V)$ satisfying $\delta(v) = f(v) \cdot \mathbf{1}$, where $\mathbf{1}$ is the multiplicative identity in $E(V)$. In addition, show that f satisfies

(a) $\delta : E_r \to E_{r-1}$, $r \geq 1$, $\delta : E_0(V) \to \{0\}$.

(b) $\delta^2 = 0 : E(V) \to E(V)$.

9. (The *Clifford Algebra*) Let V be and $\mathbb{F}$-vector space and let $Q : V \to \mathbb{F}$ be a function. We call Q a *quadratic form* if Q satisfies

(a) $Q(\alpha v) = \alpha^2 Q(v)$, for all $\alpha \in \mathbb{F}$, $v \in V$, and

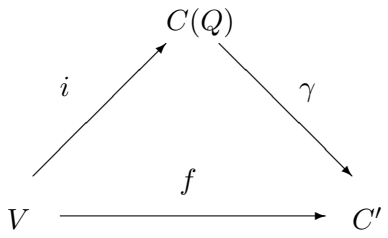
(b) the mapping $V \times V \to \mathbb{F}$ given by

$$(v, w) \mapsto Q(v + w) - Q(v) - Q(w)$$

defines a bilinear form on V.

Given the quadratic form Q on V, we define a new algebra, $C(Q)$, the *Clifford algebra*, as follows. Inside the tensor algebra $T(V)$ define the ideal I to be generated by elements of the form $v \otimes v - Q(v) \cdot \mathbf{1}$, $v \in V$. (Note that I is *not* a homogeneous ideal of $T(V)$.) The Clifford algebra is the quotient algebra $C(Q) = T(V)/I$. Show that $C(Q)$ satisfies the following universal criterion. Assume that C' is an $\mathbb{F}$-algebra and that

there exists a linear mapping $f : V \to C'$ such that for all $v \in V$, $(f(v))^2 = Q(v) \cdot \mathbf{1}'$, where $\mathbf{1}'$ is the multiplicative identity of C'. Prove that there exists a unique $\mathbb{F}$-algebra homomorphism $\gamma : C(Q) \to C'$ making the following triangle commute:



(In the above diagram, $i : V \to C(Q)$ is just the natural homomorphism $v \mapsto v + I$.)

10. Let V be an n-dimensional $\mathbb{F}$-vector space. If $d \leq n$, define the (n, d)-*Grassmann space*, $\mathcal{G}_d(V)$ as the set of all d-dimensional subspaces of V. In particular, if $d = 1$, the set $\mathcal{G}_1(V)$ is more frequently called the *projective space on* V, and is denoted by $\mathbf{P}(V)$. We define a mapping

$$\phi : \mathcal{G}_d(V) \longrightarrow \mathbf{P}(\textstyle\bigwedge^d V),$$

as follows. If $U \in \mathcal{G}_d(V)$, let $\{u_1, \ldots, u_d\}$ be a basis of U, and let $\phi(U)$ be the 1-space in $\mathbf{P}(\bigwedge^d V)$ spanned by $u_1 \wedge \cdots \wedge u_d$. Prove that $\phi : \mathcal{G}_d(V) \to \mathbf{P}(\bigwedge^d V)$ is a well-defined injection of $\mathcal{G}_d(V)$ into $\mathbf{P}(\bigwedge^d V)$. (This mapping is called the *Plücker embedding* .)

11. Let V be an n-dimensional over the finite field $\mathbb{F}_q$. Show that the Plücker embedding $\phi : \mathcal{G}_{n-1}(V) \longrightarrow \mathbf{P}(\bigwedge^{n-1} V)$ is surjective. This implies that every element of $z \in \bigwedge^{n-1} V$ can be written as a "decomposable element" of the form $z = v_1 \wedge v_2 \wedge \cdots \wedge v_{n-1}$ for suitable vectors $v_1, v_2, \ldots, v_{n-1} \in V$. (Actually this result is true independently of the field $\mathbb{F}$; see, e.g., M. Marcus, *Finite Dimensional Linear Algebra, part II*, Pure and Applied Mathematics, Marcel Dekker, Inc., New York, 1975, *page* 7. An alternative approach, suggested to me by Ernie Shult, is sketched in the exercise below.)

12. Let $G = \mathrm{GL}(V)$ acting naturally on the n-dimensional vector space V.

(a) Show that the recipe $g(f) = \det g \cdot f \circ g^{-1},\ g \in G,\ f \in V^*$ defines a representation of G on V^*, the dual space of V.

(b) Show that in the above action, G acts transitively on the non-zero vectors of V^*.

(c) Fix any isomorphism $\bigwedge^n V \cong \mathbb{F}$; show that the map $\bigwedge^{n-1} V \to V^*$ given by $\omega \mapsto \omega \wedge \cdot$ is a G-equivarient isomorphism. (See *page* 7.)

(d) Since G clearly acts on the set of decomposable vectors in $\bigwedge^{n-1} V$, conclude that every vector is decomposable.

13. Let V, W be $\mathbb{F}$-vector spaces. Prove that there is an isomorphism

$$\bigoplus_{i+j=r} \bigwedge^i V \oplus \bigwedge^j W \longrightarrow \bigwedge^r (V \oplus W).$$

14. Let V be an $\mathbb{F}$-vector space, where $\operatorname{char} \mathbb{F} \neq 2$. Define the linear transformation $S : V \otimes V \to V \otimes V$ by setting $S(v \otimes w) = w \otimes v$.

(a) Prove that S has minimal polynomial $m_S(x) = (x-1)(x+1)$.

(b) If $V_1 = \ker(S - I),\ V_{-1} = \ker(S + I)$, conclude that $V \otimes V = V_1 \oplus V_{-1}$.

(c) Prove that $V_1 \cong S^2(V),\ V_{-1} \cong \bigwedge^2(V)$.

(d) If $T : V \to V$ is any linear transformation, prove that V_1 and V_{-1} are $T \otimes T$-invariant subspaces of $V \otimes V$.

15. Let V an n-dimensional $\mathbb{F}$-vector space.

(a) Prove that $E(V)$ is graded-commutative in the sense of *Exercise* 5 of *Section* 7.3.

(b) If L is a one-dimensional $\mathbb{F}$-vector space, prove that as graded-commutative algebras,

$$E(V) \cong E(L) \otimes E(L) \otimes \cdots \otimes E(L) \quad (n \text{ factors}).$$

7.5 The Adjointness Relationship

Although we have not formally developed any *category theory* in these notes, we shall, in this section, use some of the elementary language. Let R be a ring and let ${}_R\mathbf{Mod}$, $\mathbf{Ab}$ denote the categories of left R-modules and abelian groups, respectively. Thus, if M is a fixed right R-module, then we have a *functor*

$$M \otimes_R - :_R \mathbf{Mod} \longrightarrow \mathbf{Ab}.$$

In an entirely similar way, for any fixed left R-module N, there is a functor $- \otimes_R N : \mathbf{Mod}_R \to \mathbf{Ab}$, where $\mathbf{Mod}_R$ is the category of right R-modules. Next we consider a functor $\mathbf{Ab} \to_R \mathbf{Mod}$, alluded to in *Section* 8 of *Chapter* 5. Indeed, if M is a fixed right R-module, we may define

$$\mathrm{Hom}_{\mathbb{Z}}(M, -) : \mathbf{Ab} \to_R \mathbf{Mod}.$$

Indeed, note that if A is an abelian group, then by *Exercise* 10 of *Section* 5.8, $\mathrm{Hom}_{\mathbb{Z}}(M, A)$ is a left R-module via $(r \cdot f)(m) = f(mr)$. For the fixed right R-module M, the functors $M \otimes_R -$ and $\mathrm{Hom}_{\mathbb{Z}}(M, -)$ satisfy the following important adjointness relationship.

THEOREM 7.5.1 (**Adjointness Relationship**) *If M is a right R-module, N is a left R-module, and if A is an abelian group, there is a natural equivalence of sets:*

$$Hom_{\mathbb{Z}} M \otimes_R N, A) \cong_{\mathbf{Set}} Hom_R(N, Hom_{\mathbb{Z}}(M, A)).$$

Indeed, in the above, the relevant mappings are as follows:

$$f \mapsto (n \mapsto (m \mapsto f(m \otimes n))), \quad g \mapsto (m \otimes n \mapsto g(n)(m)),$$

where $f \in \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, A)$, $g \in \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M, A))$.

In general if $\mathcal{C}, \mathcal{D}$ are categories, and if $F : \mathcal{C} \to \mathcal{D}$, $G : \mathcal{D} \to \mathcal{C}$ are functors, we say that F is *left adjoint* to G (and that G is *right adjoint* to F) if there is a natural equivalence of sets

$$\mathrm{Hom}_{\mathcal{D}}(F(X), Y) \cong_{\mathbf{Set}} \mathrm{Hom}_{\mathcal{C}}(X, F(Y)),$$

where X is an object of $\mathcal{C}$ and Y is an object of $\mathcal{D}$. Thus, we see that the functor $M \otimes_R -$ is left adjoint to the functor $\mathrm{Hom}_{\mathbb{Z}}(M, -)$.

One of the more important consequences of the above is in *Exercise* 1 below.

EXERCISES 7.5

1. Using the above adjointness relationship, interpret and prove the following: $M \otimes_R -$ preserves epimorphisms, and $\mathrm{Hom}_Z(M, -)$ preserves monomorphisms.

2. Let $\mathcal{C}$ be a category and let $\mu : A \to B$ be a morphism. We say that μ is a *monomorphism* if whenever A' is an object with morphisms $f : A' \to A,\ g : A' \to A$ such that $\mu \circ f = \mu \circ g : A' \to B$, then $f = g : A' \to A$. In other words, monomorphisms are those morphisms that have "left inverses." Similarly, epimorphisms are those morphisms that have right inverses. Now assume that $\mathcal{C}, \mathcal{D}$ are categories, and that $F : \mathcal{C} \to \mathcal{D},\ G : \mathcal{D} \to \mathcal{C}$ are functors, with F *left adjoint* to G. Prove that F preserves epimorphisms and that G preserves monomorphisms.

3. Let $i : \mathbb{Z} \hookrightarrow \mathbf{Q}$ be the inclusion homomorphism. Prove that in the category of rings, i is an epimorphism. Thus an epimorphism need not be surjective.

4. Let V, W be $\mathbb{F}$-vector spaces and let V^* be the $\mathbb{F}$-dual of V. Prove that there is a vector space isomorphism $V^* \otimes_{\mathbb{F}} W \cong \mathrm{Hom}_{\mathbb{F}}(V, W)$.

5. Let G be a group. Exactly as in *Section* 5.10, we may define the *integral group ring* $\mathbb{Z}G$; (these are $\mathbb{Z}$-linear combinations of group elements in G). correspondingly, given a ring R we may form its *group of units* $U(R)$. Thus we have functors

$$\mathbb{Z} : \mathbf{Groups} \longrightarrow \mathbf{Rings},\ U : \mathbf{Rings} \longrightarrow \mathbf{Groups}.$$

   Prove that $\mathbb{Z}$ is left adjoint to U.

6. Below are some further examples of adjoint functors. In each case you are to prove that F is left adjoint to G.

   (a)

$$\mathbf{Groups} \xrightarrow{F} \mathbf{Abelian\ Groups} \overset{G}{\hookrightarrow} \mathbf{Groups};$$

   F is the commutator quotient map.

(b)
$$\textbf{Sets} \xrightarrow{F} \textbf{Groups} \xrightarrow{G} \textbf{Sets},$$
where $F(X)$ = free group on X and $G(H)$ is the underlying set of the group H.

(c)
$$\textbf{Integral Domains} \xrightarrow{F} \textit{Fields} \overset{G}{\hookrightarrow} \textbf{Integral Domains};$$
$F(D)$ is the field of fractions of D. (Note: for this example we consider the morphisms of the category **Integral Domains** to be restricted only to injective homomorphisms.)

(d)
$$\mathbb{K} - \textit{Vector Spaces} \xrightarrow{F} \mathbb{K} - \textit{Algebras} \xrightarrow{G} \mathbb{K} - \textit{Vector Spaces};$$
$F(V) = T(V)$, the tensor algebra of V and $G(A)$ is simply the underlying vector space structure of A.

(e)
$$\textbf{Abelian Groups} \xrightarrow{F} \textbf{Torsion Free Abelian Groups} \overset{G}{\hookrightarrow} \textbf{Abelian Groups};$$
$F(A) = A/T(A)$, where $T(A)$ is the torsion subgroup of A.

(f)
$$\textbf{Left R} - \textbf{modules} \xrightarrow{F} \textbf{Abelian Groups} \xrightarrow{G} \textbf{Left R} - \textbf{modules};$$
F is the forgetful functor, $G = \mathrm{Hom}_{\mathbb{Z}}(R, -)$.

(g) If G is a group, denote by GSet the category of all sets X acted on by G. If X_1, X_2 are objects in GSet then the morphisms from X_1 to X_2 are the mappings in $\mathrm{Hom}_G(X_1, X_2)$. Then an adjoint functor pair is given by
$$G\text{Set} \xrightarrow{F} H\text{Set} \xrightarrow{G} G\text{Set}$$
$F(X) = \mathrm{Res}^G_H(X)$, $G(Y) = \mathrm{Ind}^G_H(Y)$. (Compare with *Exercise* 18 on page 11.)

Appendix A

Zorn's Lemma and some Applications

Zorn's Lemma is a basic axiom of set theory; during our course in Higher Algebra, we have had a number of occasions to use Zorn's Lemma. Below, I've tried to indicate exactly where we have made use of this important axiom.

The setting for Zorn's Lemma is a *partially ordered set*, which I now define. If S is a set, and $\leq$ is a relation on S such that

(i) $s \leq s$ for all $s \in S$,

(ii) if $s_1 \leq s_2$ and $s_2 \leq s_1$, then $s_1 = s_2$,

(iii) if $s_1 \leq s_2$ and $s_2 \leq s_3$, then $s_1 \leq s_3$,

then $(S, \leq)$ is called a *partially ordered set*. If $(S, \leq)$ is a partially ordered set such that whenever $s_1, s_2 \in S$ we have $s_1 \leq s_2$ or $s_2 \leq s_1$, we call $(S, \leq)$ a *totally ordered set*. If $(S, \leq)$ is a partially ordered set and if C is a totally ordered subset of S, then C is called a *chain*. An *upper bound* for a chain $C \subseteq S$ is an element $s \in S$ such that $c \leq s$ for all $c \in C$. A *maximal element* in the partially ordered set $(S, \leq)$ is an element $m \in S$ such that if $s \in S$ with $m \leq s$, then $m = s$.

We are now ready to state **Zorn's Lemma**:

Let $(S, \leq)$ be a partially ordered set in which every chain in S has an upper bound. Then S has a maximal element.

We turn now to a few standard applications.

1. **Basis of a Vector Space.** Let V be a (possibly infinite dimensional) vector space over the field $\mathbf{F}$. We shall prove that V contains a *basis*, i.e., a linearly independent set which spans V. To prove this, let S be the set of all linearly independent subsets of V, partially ordered by inclusion $\subseteq$. Then $(S, \subseteq)$ is a partially ordered set. Let C be a chain in S; to prove that C has an upper bound, we construct the set

$$\mathcal{B} \;=\; \bigcup_{\mathcal{A}\in C} \mathcal{A}.$$

We can easily prove that $\mathcal{B}$ is linearly independent, which will show that $\mathcal{B}$ is an upper bound for C. Indeed, suppose that $b_1, b_2, \ldots, b_r \in \mathcal{B}$ such that there is a linear dependence relation of the form

$$\sum_{i=1}^{r} \alpha_i b_i \;=\; 0,$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbf{F}$. Since C is a chain we see that for some $\mathcal{A} \in C$ we have $b_1, b_2, \ldots, b_r \in \mathcal{A}$, which, of course, violates the fact that $\mathcal{A}$ is a linearly independent subset of V. Thus, we can apply Zorn's Lemma to infer that there exists a maximal element $\mathcal{M}$ of S. We claim that $\mathcal{M}$ is a basis of V. To prove this, we need only show that $\mathcal{M}$ spans V. But if there is a vector $v \in V - \text{span }(\mathcal{M})$, then $\mathcal{M} \cup \{v\}$ is a linearly independent subset of V (i.e. is an element of S), which violates the maximality of $\mathcal{M}$.

2. **Maximal Ideals in Rings.** Let R be a ring with identity 1. We can apply Zorn's Lemma to prove that R contains a proper maximal ideal M, as follows. Let $S = \{\text{proper ideals } I \subseteq R\}$, partially ordered by inclusion. If C is a chain in S, form the set

$$J \;=\; \bigcup_{I\in C} I.$$

Then it is easy to check that $x, y \in J$ implies that $x + y \in J$, and that if $x \in J,\ r \in R$, then $rx, xr \in J$. Thus J is an ideal of R. Furthermore, it is a proper ideal, for otherwise we would have $1 \in J$, and so $1 \in I$, for some $I \in C$, contrary to the assumption that I is a proper ideal of R. By Zorn's Lemma, we conclude that S has a maximal element M. It is then clear that M is a maximal proper ideal of R.

3. **Proof of** *Proposition* **2.2.8** Let S be the set of ordered pairs $(\mathbf{F}_\alpha, \psi_\alpha)$ such that $\mathbf{F}_1 \subseteq \mathbf{F}_\alpha$ and such that

$$\begin{array}{ccc} \mathbf{F}_\alpha & \xrightarrow{\psi_\alpha} & \mathbf{K}_2 \\ \uparrow & & \uparrow \\ \mathbf{F}_1 & \xrightarrow{\psi} & \mathbf{F}_2 \end{array}$$

commutes. Partially order S by $(\mathbf{F}_\alpha, \psi_\alpha) \leq (\mathbf{F}_\beta, \psi_\beta)$ if and only if $\mathbf{F}_\alpha \subseteq \mathbf{F}_\beta$ and $\psi_\beta | \mathbf{F}_\alpha = \psi_\alpha$. Chains have upper bounds and so by Zorn's Lemma there is a maximal element $(\bar{\mathbf{F}}_1, \bar{\psi})$. If $\bar{\mathbf{F}} \neq \mathbf{K}_1$, then there exists $f_1(x) \in \mathcal{F}_1$ such that $f_1(x)$ doesn't split in $\bar{\mathbf{F}}_1$. Thus if $\bar{\mathbf{K}}_1$ is the splitting field over $\bar{\mathbf{F}}_1$ of $f_1(x)$, then apply *Proposition* 2.2.7 to get

$$\begin{array}{ccc} \bar{\mathbf{K}}_1 & \longrightarrow & \bar{\mathbf{K}}_2 \\ \uparrow & & \uparrow \\ \bar{\mathbf{F}}_1 & \xrightarrow{\bar{\psi}} & \bar{\psi}(\bar{\mathbf{F}}_1), \end{array}$$

where $\bar{\mathbf{K}}_2$ is the splitting field for $\hat{\psi}(f_1(x))$ over $\bar{\mathbf{F}}_1$. This, of course, is a contradiction to maximality.

4. **Existence of an Algebraic Closure of a Given Field.**

Lemma. *If* $\mathbf{F}$ *is a field, then there exists an extension field* $\mathbf{F}_1$ *such that every polynomial in* $\mathbf{F}[x]$ *has a root in* $\mathbf{F}_1$.

Proof. For each irreducible $f = f(x) \in \mathbf{F}[x]$ let X_f be a corresponding indeterminate, and set $\mathcal{X} = \{X_f |\ f = f(x) \in \mathbf{F}[x] \text{ is irreducible }\}$. We shall work in the gigantic polynomial ring $\mathbf{F}[\mathcal{X}] = \mathbf{F}[\ldots, X_f, \ldots]$. Let $I \subseteq \mathbf{F}[\mathcal{X}]$ be the ideal generated by the polynomials $f(X_f)$, where $f = f(x)$ ranges over the set of irreducible polynomials in $\mathbf{F}[x]$. I claim that $I \neq \mathbf{F}[\mathcal{X}]$. For otherwise, there would exist polynomials $f_1(x), \ldots f_r(x) \in \mathbf{F}[x]$, and polynomials $g_1, \ldots g_r \in \mathbf{F}[\mathcal{X}]$ such that

$$1 \ = \ g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + \cdots + g_r f_r(X_{f_r}).$$

Let $\mathbf{K}$ be an extension field of $\mathbf{F}$ such that each $f_i(x)$ has a root $\alpha_i \in \mathbf{K}$, $i = 1, 2, \ldots, r$. Let $E : \mathbf{F}[\mathcal{X}] \to \mathbf{K}[\mathcal{X}]$ be the evaluation map that sends each X_{f_i} to α_i, $i = 1, 2, \ldots, r$, and maps all remaining X_h's to themselves, where $h = h(x) \notin \{f_1(x), f_2(x), \ldots, f_r(x)\}$. If we apply E to the above equation, we get $1 = 0$, a clear contradiction.

Next, form the quotient ring $\mathbf{F}[\mathcal{X}]/I$, which by the above, is not the 0-ring. By Zorn's Lemma, there is a maximal ideal $\bar{M} \subseteq \mathbf{F}[\mathcal{X}]/I$; if $\pi : \mathbf{F}[\mathcal{X}] \to \mathbf{F}[\mathcal{X}]/I$ is the quotient map, then $M := \pi^{-1}(\bar{M})$ is a maximal ideal of $\mathbf{F}[\mathcal{X}]$. Thus we have a field $\mathbf{F}_1 := \mathbf{F}[\mathcal{X}]/M$ and an injection $\mathbf{F} \to \mathbf{F}_1$. (As usual, we can regard $\mathbf{F}$ as a subfield of $\mathbf{F}_1$.) Since each $f(X_f) \in M$, we see that if $\gamma_f = X_f + M \in \mathbf{F}_1$, then γ_f is a root of $f(x)$ in $\mathbf{F}_1$. This proves the lemma.

Proof of the Existence of Algebraic Closure. Let $\mathbf{F} = \mathbf{F}_0$ be the field whose algebraic closure we are to construct. By the above Lemma, we may generate a sequence

$$\mathbf{F}_0 \subseteq \mathbf{F}_1 \subseteq \mathbf{F}_2 \subseteq \cdots,$$

where every polynomial in $\mathbf{F}_i[x]$ has a root in $\mathbf{F}_{i+1}$. Thus we may form the field

$$\mathbf{E} \;=\; \bigcup_{i \geq 0} \mathbf{F}_i;$$

clearly every polynomial $f(x) \in \mathbf{F}[x]$ has a root in $\mathbf{E}$. Thus if $\bar{\mathbf{F}}$ is the subfield of $\mathbf{E}$ generated by the roots of all of the polynomials $f(x) \in \mathbf{F}[x]$, then clearly $\bar{\mathbf{F}}$ is an algebraic closure of $\mathbf{F}$.

5. **Free Modules over a Principal Ideal Domain.**

Here we shall prove *Proposition* 5.3.11:

Proposition . *Let M be a free module over the principal ideal domain R. If N is a submodule of M, then N is free, and rank$(N) \leq$ rank(M).*

Proof. We may certainly assume that $N \neq 0$; let $\mathcal{B}$ be a basis for M. For any subset $\mathcal{C} \subseteq \mathcal{B}$, set $M_{\mathcal{C}} = R < \mathcal{C} >$, and set $N_{\mathcal{C}} = N \cap M_{\mathcal{C}}$.

Consider the set S of all triples $(\mathcal{C}', \mathcal{C}, f)$, where

(i) $\mathcal{C}' \subseteq \mathcal{C} \subseteq \mathcal{B}$,

(ii) $N_{\mathcal{C}}$ is a free R-module,

(iii) $f : \mathcal{C}' \to N_{\mathcal{C}}$ is a function such that $f(\mathcal{C})$ is a basis of $N_{\mathcal{C}}$.

Since $(\emptyset, \emptyset, \emptyset) \in S$, we see that $S \neq \emptyset$. Now partially order S by

$$(\mathcal{C}', \mathcal{C}, f) \leq (\mathcal{D}', \mathcal{D}, g) \Leftrightarrow \mathcal{C}' \subseteq \mathcal{D}',\ \mathcal{C} \subseteq \mathcal{D} \text{ and } g|_{\mathcal{C}'} = f.$$

It is easy to prove that chains have upper bounds and so Zorn's lemma guarantees a maximal element $(\mathcal{A}', \mathcal{A}, h) \in S$. By the above, we'll be done as soon as we show that $\mathcal{A} = \mathcal{B}$.

So assume that there is some $b \in \mathcal{B} - \mathcal{A}$ and set $\mathcal{D} = \mathcal{A} \cup \{b\}$. If $N_{\mathcal{D}} = N_{\mathcal{A}}$, then clearly $(\mathcal{A}', \mathcal{A}, h) < (\mathcal{A}', \mathcal{D}, h)$. Thus we may assume that $N_{\mathcal{D}}$ properly contains $N_{\mathcal{A}}$. Let $I \subseteq R$ be defined by setting

$$I \ = \ \{r \in R |\ y + rb \in N, \text{for some } y \in M_{\mathcal{A}}\};$$

since $N_{\mathcal{D}}$ properly contains $N_{\mathcal{A}}$, we have $I \neq 0$. Clearly I is an ideal of R. Thus $I = (s)$ for some $s \in R$. We have $w := x + sb \in N$ for some $x \in M_{\mathcal{A}}$. Set $\mathcal{D}' = \mathcal{A}' \cup \{b\}$ and extend $h' : \mathcal{D}' \to N_{\mathcal{D}}$ by setting $h'(b) = w$. We shall show that $(\mathcal{D}', \mathcal{D}, h') \in S$.

We first show that $h'(\mathcal{D}')$ spans $N_{\mathcal{D}}$. If $z \in N_{\mathcal{D}}$ then $z = y + rb$ for some $r \in R, y \in M_{\mathcal{A}}$. Also $r = r's$ for some $r' \in R$ and so $z = y + r'sb = y + r'(w - x) = (y - r's) + r'w$; also $z - r'w = y - r'x \in N \cap M_{\mathcal{A}} = N_{\mathcal{A}}$. Therefore $N_{\mathcal{D}}$ is spanned by $h'(\mathcal{D}')$. Next, if $h'(\mathcal{D}')$ is R-linearly dependent, then $\{w\} \cup h'(\mathcal{A}') = \{w\} \cup h(\mathcal{A}')$ is R-linearly dependent. Since $h(\mathcal{A}')$ is R-linearly independent, we infer that $rw \in R < h(\mathcal{A}') > \cap N = N_{\mathcal{A}}$ and so $rsb \in M_{\mathcal{A}}$ which contradicts the fact that $\mathcal{A} \cup \{b\}$ is R-linearly independent. The result follows.

As we mentioned in class, the only place we really used the above proposition is in the proof of *proposition* 9, that is, in showing that finitely generated torsion-free modules over the *p.i.d.* are free. Therefore, all we really need is the above theorem in the case that M is *finitely generated*. The proof in this case is quite simple, as indicated below.

First, a lemma. Note that we essentially proved this in class when we proved *proposition* 10.

Lemma. *If F is a free module over the ring R (not necessarily a* p.i.d.*), and if $\epsilon : M \to F$ is an epimorphism of R-modules, then $M \cong \ker(\epsilon) \oplus F$*

Proof. Let $\mathcal{B}$ be a basis of F, and for each $b \in \mathcal{B}$ choose an element $b' \in \epsilon^{-1}(b)$. Now map $\mathcal{B} \to M$ by $b \mapsto b'$ thereby obtining a homorphism

$\sigma : F \to M$ which satisfies $\epsilon \circ \sigma = 1_F$. Note that $F \cong \sigma\epsilon(M)$; thus it suffices to show that $M = \ker(\epsilon) \oplus \sigma\epsilon(M)$. This is easy; recall how we did it in class.

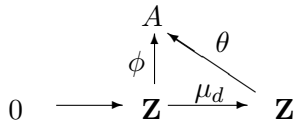
Theorem. *Let M be a finitely generated free module over the principal ideal domain R. If N is a submodule of M, then N is free, and rank$(N) \leq$ rank(M).*

Proof. We use induction on the rank of M. If the rank is 1, then, of course, $M \cong R$, in which case any submodule is just an ideal of R. Since R is a *p.i.d.*, nonzero ideals are free, rank 1 submodules of R, so we're done. Thus, assume that the rank of M is greater than 1. Let $\{m_1, m_2, \ldots, m_k\}$ be a basis of M, and let $\epsilon : M \to R$ be the homomorphism determined by $\epsilon(m_1) = \ldots = \epsilon(m_{k-1}) = 0, \epsilon(m_k) = 1$. Note that $\ker(\epsilon) = R < m_1, \ldots, m_{k-1} >$, which is a free R-module of rank $k-1$. Let $N \subseteq M$ be the given submodule of M; note that $\ker(\epsilon : N \to R)$ is a submodule of the free module $R < m_1, \ldots, m_{k-1} >$. By induction, we have that $\ker(\epsilon : N \to R)$ is a free R-module of rank less than or equal to $k-1$. Since $\epsilon(N) \subseteq R$ is free, we apply the above lemma to infer that $N \cong \ker(\epsilon : N \to R) \oplus \epsilon(N)$, and so N is a free R-module of rank at most k.

6. **The Equivalence of Divisible and Injective Abelian Groups.**

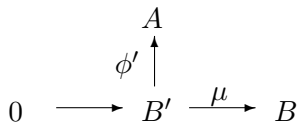
Theorem. *Let A be an abelian group. Then A is injective if and only if it is divisible.*

Proof. We shall first show that if A is injective, then it is divisible. Let $a \in A$ and let $d \in \mathbf{Z}$. Consider the diagram



where $\phi(1) = a$. Let $b = \theta(1)$. Then $db = d\theta(1) = \theta(d) = \theta\mu_d(1) = \theta(1) = a$, done.

Conversely, let A be divisible and consider the diagram



(exact).

We may as well regard $B' \subseteq B$ via μ. Let $\mathcal{P} = \{(B'', \phi'')\}$ such that $B' \subseteq B'' \subseteq B$ and $\phi'' : B'' \to A$ with $\phi''|_{B'} = \phi'$. Partially order by $(B'', \phi'') \leq (C'', \theta'')$ if and only if $B'' \leq C''$ and $\theta''|B'' = \phi''$. As $(B', \phi') \in \mathcal{P}$, we see that $\mathcal{P}$ is nonempty. Clearly every chain in $\mathcal{P}$ has an upper bound and so by Zorn's Lemma, there exists a maximal element $(B'_0, \phi'_0) \in \mathcal{P}$. We shall show that $B'_0 = B$. If not, then there exists $b \in B - B'_0$; let m be the order of the element $b + B'_0 \in B/B'_0$. Set $\tilde{B}'_0 = B'_0 + < b >$.

Case 1: $m = \infty$. Then $< b > \cap B'_0 = 0$ and so $\tilde{B}'_0 = B'_0 \oplus < b >$, and $< b >$ is free. Then we can define $\phi :< b > \to A$ arbitrarily and define $\tilde{\phi}'_0 : B'_0 \oplus < b > \to A$ by the universal property of $\oplus$.

Case 2: $m < \infty$. Now $mb \in B'_0$ and $\phi'_0(mb) \in A$. Find $a \in A$ with $ma = \phi'_0(mb)$ and define $\tilde{\phi}'_0 : \tilde{B}'_0 \to A$ by setting $\tilde{\phi}'_0(b'_0 + nb) = \phi'_0(b'_0) + na$. One easily shows that $\tilde{\phi}'_0$ is a well-defined homomorphism which extends ϕ'_0, so we are done.

7. Applications to Semisimple Modules

Lemma. *A semisimple module has an irreducible submodule.*

Proof. Let M be semisimple, and let $0 \neq m \in M$. Let $\mathcal{P} = \{\text{submodules } N \subseteq M |\ m \notin N\}$. An easy application of Zorn's lemma shows that $\mathcal{P}$ has a maximal element M_0. Since M is semisimple, there is a submodule $M' \subseteq M$ such that $M = M_0 \oplus M'$; we shall show that M' is irreducible. If not then M' decomposes as $M' = M'_1 \oplus M'_2$ where $M'_1, M'_2 \neq 0$. But then, by maximality of M_0, we have $m \in M_0 \oplus M'_1,\ M_0 \oplus M'_2$ and so $m \in M_0 \oplus M'_1 \cap M_0 \oplus M'_2 = M_0$, a contradiction.

Theorem. *The following conditions are equivalent for the R-module M.*

(i) M is semisimple.

(ii) $M = \sum_{i \in \mathcal{I}} M_i$, for some family $\{M_i |\ i \in \mathcal{I}\}$ of irreducible submodules of M.

(iii) $M = \oplus_{i \in \mathcal{I}} M_i$, for some family $\{M_i |\ i \in \mathcal{I}\}$ of irreducible submodules of M.

Proof. (i)⇒(ii): Let $\{M_\alpha |\ \alpha \in \mathcal{A}\}$ be the set of all irreducible submodules of M. We'll show that $M = \sum_{\alpha \in \mathcal{A}} M_\alpha$. If not, then $M = \sum_{\alpha \in \mathcal{A}} M_\alpha \oplus N$ for

some submodule N. Apply the above lemma to conclude that N contains a nonzero irreducible submodule of N, a clear contradiction.

(ii)$\Rightarrow$ (iii): As above, let $\{M_\alpha |\ \alpha \in \mathcal{A}\}$ be the set of all irreducible submodules of M; by hypothesis, $M = \sum M_\alpha$. Let $\mathcal{P} = \{\mathcal{B} \subseteq \mathcal{A} |\ \sum_{\beta\in\mathcal{B}} M_\beta = \bigoplus_{\beta\in\mathcal{B}} M_\beta\}$ and partially order $\mathcal{P}$ by inclusion. Apply Zorn to get a maximal element $\mathcal{B}_0 \subseteq \mathcal{A}$. Thus $\sum_{\beta\in\mathcal{B}_0} M_\beta = \bigoplus_{\beta\in\mathcal{B}_0} M_\beta$. If $\sum_{\beta\in\mathcal{B}_0} M_\beta \neq M$, then from $\sum_{\alpha\in\mathcal{A}} M_\alpha = M$ there must exist an irreducible submodule $M_\alpha \not\subseteq \sum_{\beta\in\mathcal{B}_0} M_\beta$. But then $M_\alpha \cap \sum_{\beta\in\mathcal{B}_0} M_\beta = \emptyset$, i.e., $M_\alpha + \sum_{\beta\in\mathcal{B}_0} M_\beta = M_\alpha \oplus \sum_{\beta\in\mathcal{B}_0} M_\beta$, contrary to the maximality of $\mathcal{B}_0$.

(iii)$\Rightarrow$(i): Assume that $\{M_\alpha |\ \alpha \in \mathcal{A}\}$ is the set of irreducibles in M; thus $M = \sum_{\alpha\in\mathcal{A}} M_\alpha$. Let $N \subseteq M$, and use Zorn's lemma to obtain a set $\mathcal{C} \subseteq \mathcal{A}$ which is maximal with respect to $N \cap \sum_{\alpha\in\mathcal{C}} M_\alpha = 0$. If $M \neq N + \sum_{\alpha\in\mathcal{C}} M_\alpha$, then there exists $\gamma \in \mathcal{A}$ such that $M_\gamma \not\subseteq N + \sum_{\alpha\in\mathcal{C}} M_\alpha$. But then $M_\gamma \cap (N + \sum_{\alpha\in\mathcal{C}} M_\alpha) = 0$, and so $N \cap (M_\gamma + \sum_{\alpha\in\mathcal{C}} M_\alpha) = 0$, contrary to the maximality of $\mathcal{C}$.

Index

k-transitively, 26
p-group, 6

a.c.c., 130
action
    imprimitive, 25
    permutation, 7
    primitive, 25
acts on, 5
adjoint
    left, 174
    right, 174
algebra, 147, 164
algebraic, 43
algebraic closure, 49
algebraic integer, 92
algebraic integer domain, 93
algebraic number, 44
algebraically closed, 49
algorithm, 85
alternating, 170
alternating bilinear form, 34
alternating group, 23
ascending chain condition, 130
associates, 77
atomic domain, 83
automorphism, 8

balanced, 155
basis, 112
bilinear form
    alternating, 34
bimodule, 159
Butterfly Lemma, 107

category theory, 174
Cauchy's Theorem, 2
characteristic, 22, 29, 43
characteristic polynomial, 125
characteristic subgroup, 29
Chinese Remainder Theorem, 74
closed, 52
closure, 52
cofree R-module, 138
comaximal ideals, 74
commutative
    graded algebra, 165
commutator, 29, 31
commutator subgroup, 29
companion matrix, 125
complete flag, 16
composite, 46
composition series, 30, 131
compositum, 46
conjugacy class, 5
content of a polynomial, 79
convolution, 147
coordinate mappinga, 110
cycle, 23
cycle type, 24
cycles
    disjoint, 23

cyclic R-module, 117
cyclic group, 2
cyclotomic polynomial, 67

d.c.c, 130
Dedekind Domain, 97
Dedekind Independence Lemma, 51
degree
    of an element, 44, 167
    of an extension, 43, 44
degree of an extension, 43
descending chain condition, 130
determinantal rank, 121
differential, 114
dihedral group, 4
direct sum, 109
discrete valuation ring, 105
discriminant, 63
disjoint cycles, 23
divides, 77
divisible abelian group, 137
division algorithm, 85
division ring, 134
double transitivity, 9

elementary components, 118
elementary divisors, 117
equivariant mapping, 7
Euclidean domain, 85
exact, 32, 89
exponent, 117
extension, 43
    Galois, 52
    purely inseparable, 56
    separable, 56
    simple, 44, 71
extension degree, 43
exterior algebra, 168

F-algebra, 147
field extension, 43
finitely generated, 82
    submodule, 89
fixed point set, 5
fixed points, 5
flag, 16
    type, 16
fractional ideal, 101
    principal fractional ideal, 101
Frattini subgroup, 35
free
    group, 37
    module, 111
free R-module, 140
free product, 41
Frobenius automorphism, 58
Fundamental Theorem of Algebra, 63
Fundamental Theorem of Algebraic Number Theory, 99
Fundamental Theorem of Galois Theory, 52

Galois extension, 52
Galois group, 51
Gaussian integers, 76
general linear group, 15
generalized quaternion group, 21
generator
    of a group, 2
generators and relations, 38
graded
    algebra, 167
    ideal, 167
graded algebra, 165
graded-commutative, 165
Grassmann space, 172
greatest common divisor, 77, 78
group action, 5

faithful, 5
group algebra, 147
group of units, 77, 175
group ring, 147

Heisenberg Group, 34
Hilbert Basis Theorem, 82
homogeneous
elements, 167
homogeneous ideal, 167
homomorphism
module, 89
Hopkin's Theorem, 152

ideal class group, 101
idempotent, 144
idempotents
orthogonal, 144
imprimitivity, 25
imprivitively, 25
Inclusion-Exclusion Principle, 60
inner automorphism, 19
integral domain, 73
integral group ring, 175
integrally closed, 93
internal direct sum, 89, 91, 110
invariant basis number, 113
invariant basis number (IBN), 113
invariant factors, 118
invertible ideal, 102, 137
involution, 4
irreducible, 77, 131
R-module, 131
R-module, 144

Jacobson radical, 150
Jordan canonical form, 126, 127
Jordan-Hölder Theorem, 30

kernel of the action, 5
Kronecker product, 160
Krull topology, 62

Lagrange's Theorem, 1
Langrange's Theorem, 1
least common multiple, 77, 78
left adjoint, 174
left Artinian, 152
left Noetherian, 152
local ring, 133
localization, 103
lower central series, 31

maximal ideal, 73
minimal polynomial, 44
of a linear transformation, 124
minor, 121
modular law, 90, 107
module, 88
module homomorphism, 89
monomorphism, 175

Nakayama's Lemma, 152
nil ideal, 151
nilpotent
element, 151
group, 31
ideal, 151
nilpotent element, 76
Noether Isomorphism Theorem, 107
Noetherian
module, 90
ring, 82
Noetherian module, 130
norm map, 59
normal closure, 38
normal series, 30

orbit, 5

Orbit-Stabilizer Reciprocity Theorem, 5
order, 2, 116
    infinite, 2
outer automorphism, 19
overring, 103

p-part, 13
perfect, 57
permutation isomorphic, 7
Plücker embedding, 172
pointwise, 147
polynomial
    separable, 56
Primary Decomposition Theorem, 127
primary ideal, 75
prime
    element, 77
    ideal, 73
primitive, 25
primitive element, 71
Primitive Element Theorem, 71
primitive polynomial, 79
principal ideal, 73
principal ideal domain, 82
prinicpal fractional ideal, 101
projection mappings, 110
projective, 136
projective general linear group, 15
projective space, 16, 172
projective special linear group, 15
purely inseparable, 56
    element, 56

quadratic integer domains, 93
quasi-dihedral group, 20
quaternion group, 21
    generalized, 21

rank, 112
rational canonical form, 125
regular normal subgroup, 27
relations, 38
relations matrix, 120
relatively prime ideals, 74
representation, 147
residual quotient, 75
right adjoint, 174
right Artinian, 152
right Noetherian, 152
root tower, 70

Schreier Refinement Theorem, 131
Second Isomorphism Theorem, 107
semi-direct product, 18
    external, 18
    internal, 18
semidihedral group, 20
semisimple, 128
    linear transformation, 134
    R-module, 143
    ring, 152
separable, 56, 71
    element, 56
    extension, 56, 71
    polynomial, 56
separable element, 71
short exact sequence, 89
    splitting, 113
    splitting of, 91
simple, 131
simple R-module, 131
simple field extension, 44
simple radical extension, 70
simple ring, 145
Smith equivalent, 120
solvable, 30
    group, 30

solvable by radicals, 70
special linear group, 15
split short exact sequence, 113
splits, 91
splitting field, 44, 48
stabilizer, 5
stable, 52
subgroup
    characteristic, 22, 29
submultiplicative algorithm, 85
subnormal series, 30
Sylow subgroup, 13
symmetric algebra, 167
symmetric group, 3
system of imprimitivity, 25
    non-trivial, 25
    trivial, 25

tensor algebra, 166
tensor product, 155
Third Isomorphism Theorem, 107
torsion element, 116
torsion submodule, 116
torsion-free, 116
totally discontinuous, 62
transitive, 7
transposition, 23

u.f.d., 77
unique factorization domain, 77
unit, 77

valuation ring, 104

word problem, 39

Zassenhaus Lemma, 107
zero-divisor, 73