Chapter 2

Groups

Groups are the central objects of algebra. In later chapters we will define rings and modules and see that they are special cases of groups. Also ring homomorphisms and module homomorphisms are special cases of group homomorphisms. Even though the definition of group is simple, it leads to a rich and amazing theory. Everything presented here is standard, except that the product of groups is given in the additive notation. This is the notation used in later chapters for the products of rings and modules. This chapter and the next two chapters are restricted to the most basic topics. The approach is to do quickly the fundamentals of groups, rings, and matrices, and to push forward to the chapter on linear algebra. This chapter is, by far and above, the most difficult chapter in the book, because group operations may be written as addition or multiplication, and also the concept of coset is confusing at first.

Definition Suppose G is a non-void set and $\phi : G \times G \to G$ is a function. ϕ is called a *binary operation*, and we will write $\phi(a, b) = a \cdot b$ or $\phi(a, b) = a+b$. Consider the following properties.

1) If $a, b, c \in G$ then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.	If $a, b, c \in G$ then $a + (b + c) = (a + b) + c$.
2) $\exists\ e = e_G \in G$ such that if $a \in G$ $e \cdot a = a \cdot e = a$.	$\exists\ \underline{0}=\underline{0}_G \in G$ such that if $a \in G$ $\underline{0}+a = a+\underline{0}= a$.
3) If $a \in G$, $\exists b \in G$ with $a \cdot b = b \cdot a = e$ (b is written as $b = a^{-1}$).	If $a \in G, \exists b \in G$ with $a + b = b + a = \underline{0}$ (b is written as $b = -a$).
4) If $a, b \in G$, then $a \cdot b = b \cdot a$.	If $a, b \in G$, then $a + b = b + a$.

Definition If properties 1), 2), and 3) hold, (G, ϕ) is said to be a *group*. If we write $\phi(a, b) = a \cdot b$, we say it is a *multiplicative* group. If we write $\phi(a, b) = a + b$,

we say it is an *additive* group. If in addition, property 4) holds, we say the group is *abelian* or *commutative*.

Theorem Let (G, ϕ) be a multiplicative group.

(i) Suppose $a, c, \bar{c} \in G$. Then $a \cdot c = a \cdot \bar{c} \Rightarrow c = \bar{c}$.
Also $c \cdot a = \bar{c} \cdot a \Rightarrow c = \bar{c}$.
In other words, if $f : G \to G$ is defined by $f(c) = a \cdot c$, then f is injective. Also f is bijective with f^{-1} given by $f^{-1}(c) = a^{-1} \cdot c$.

(ii) e is unique, i.e., if $\bar{e} \in G$ satisfies 2), then $e = \bar{e}$. In fact, if $a, b \in G$ then $(a \cdot b = a) \Rightarrow (b = e)$ and $(a \cdot b = b) \Rightarrow (a = e)$. Recall that b is an identity in G provided it is a right and left identity for any a in G. However group structure is so rigid that if $\exists\ a \in G$ such that b is a right identity for a, then $b = e$. Of course, this is just a special case of the cancellation law in (i).

(iii) Every right inverse is an inverse, i.e., if $a \cdot b = e$ then $b = a^{-1}$. Also if $b \cdot a = e$ then $b = a^{-1}$. Thus inverses are unique.

(iv) If $a \in G$, then $(a^{-1})^{-1} = a$.

(v) The multiplication $a_1 \cdot a_2 \cdot a_3 = a_1 \cdot (a_2 \cdot a_3) = (a_1 \cdot a_2) \cdot a_3$ is well defined. In general, $a_1 \cdot a_2 \cdots a_n$ is well defined.

(vi) If $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ Also $(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_1^{-1}$.

(vii) Suppose $a \in G$. Let $a^0 = e$ and if $n > 0$, $a^n = a \cdots a$ (n times) and $a^{-n} = a^{-1} \cdots a^{-1}$ (n times). If $n_1, n_2, ..., n_t \in \mathbf{Z}$ then $a^{n_1} \cdot a^{n_2} \cdots a^{n_t} = a^{n_1 + \cdots + n_t}$. Also $(a^n)^m = a^{nm}$. Finally, if G is abelian and $a, b \in G$, then $(a \cdot b)^n = a^n \cdot b^n$.

Exercise. Write out the above theorem where G is an additive group. Note that part (vii) states that G has a scalar multiplication over $\mathbf{Z}$. This means that if a is in G and n is an integer, there is defined an element an in G. This is so basic, that we state it explicitly.

Theorem. Suppose G is an additive group. If $a \in G$, let $a0 = \underline{0}$ and if $n > 0$, let $an = (a + \cdots + a)$ where the sum is n times, and $a(-n) = (-a) + (-a) \cdots + (-a)$,

which we write as $(-a - a \cdot \cdot - a)$. Then the following properties hold in general, except the first requires that G be abelian.

$$\begin{array}{lcl} (a+b)n & = & an+bn \\ a(n+m) & = & an+am \\ a(nm) & = & (an)m \\ a1 & = & a \end{array}$$

Note that the plus sign is used ambiguously — sometimes for addition in G and sometimes for addition in $\mathbf{Z}$. In the language used in Chapter 5, this theorem states that any additive abelian group is a $\mathbf{Z}$-module. (See page 71.)

Exercise Suppose G is a non-void set with a binary operation $\phi(a,b) = a \cdot b$ which satisfies 1), 2) and [3′) If $a \in G$, $\exists b \in G$ with $a \cdot b = e$]. Show (G, ϕ) is a group, i.e., show $b \cdot a = e$. In other words, the group axioms are stronger than necessary. If every element has a right inverse, then every element has a two sided inverse.

Exercise Suppose G is the set of all functions from $\mathbf{Z}$ to $\mathbf{Z}$ with multiplication defined by composition, i.e., $f \cdot g = f \circ g$. Note that G satisfies 1) and 2) but not 3), and thus G is not a group. Show that f has a right inverse in G iff f is surjective, and f has a left inverse in G iff f is injective (see page 10). Also show that the set of all bijections from $\mathbf{Z}$ to $\mathbf{Z}$ is a group under composition.

Examples $G = \mathbf{R}$, $G = \mathbf{Q}$, or $G = \mathbf{Z}$ with $\phi(a,b) = a + b$ is an additive abelian group.

Examples $G = \mathbf{R} - 0$ or $G = \mathbf{Q} - 0$ with $\phi(a,b) = ab$ is a multiplicative abelian group.
$G = \mathbf{Z} - 0$ with $\phi(a,b) = ab$ is not a group.
$G = \mathbf{R}^+ = \{r \in \mathbf{R} : r > 0\}$ with $\phi(a,b) = ab$ is a multiplicative abelian group.

Subgroups

Theorem Suppose G is a multiplicative group and $H \subset G$ is a non-void subset satisfying

1) if $a, b \in H$ then $a \cdot b \in H$
and 2) if $a \in H$ then $a^{-1} \in H$.

Then $e \in H$ and H is a group under multiplication. H is called a *subgroup* of G.

Proof Since H is non-void, $\exists a \in H$. By 2), $a^{-1} \in H$ and so by 1), $e \in H$. The associative law is immediate and so H is a group.

Example G is a subgroup of G and e is a subgroup of G. These are called the *improper* subgroups of G.

Example If $G = \mathbf{Z}$ under addition, and $n \in \mathbf{Z}$, then $H = n\mathbf{Z}$ is a subgroup of $\mathbf{Z}$. By a theorem in the section on the integers in Chapter 1, every subgroup of $\mathbf{Z}$ is of this form (see page 15). This is a key property of the integers.

Exercises Suppose G is a multiplicative group.

1) Let H be the *center* of G, i.e., $H = \{h \in G : g \cdot h = h \cdot g \text{ for all } g \in G\}$. Show H is a subgroup of G.

2) Suppose H_1 and H_2 are subgroups of G. Show $H_1 \cap H_2$ is a subgroup of G.

3) Suppose H_1 and H_2 are subgroups of G, with neither H_1 nor H_2 contained in the other. Show $H_1 \cup H_2$ is not a subgroup of G.

4) Suppose T is an index set and for each $t \in T$, H_t is a subgroup of G. Show $\bigcap_{t \in T} H_t$ is a subgroup of G.

5) Furthermore, if $\{H_t\}$ is a monotonic collection, then $\bigcup_{t \in T} H_t$ is a subgroup of G.

6) Suppose $G = \{\text{all functions } f : [0,1] \to \mathbf{R}\}$. Define an addition on G by $(f+g)(t) = f(t) + g(t)$ for all $t \in [0,1]$. This makes G into an abelian group. Let K be the subset of G composed of all differentiable functions. Let H be the subset of G composed of all continuous functions. What theorems in calculus show that H and K are subgroups of G? What theorem shows that K is a subset (and thus subgroup) of H?

Order Suppose G is a multiplicative group. If G has an infinite number of

elements, we say that $o(G)$, the *order* of G, is infinite. If G has n elements, then $o(G) = n$. Suppose $a \in G$ and $H = \{a^i : i \in \mathbf{Z}\}$. H is an abelian subgroup of G called the *subgroup generated by* a. We define the *order of the element* a to be the order of H, i.e., the order of the subgroup generated by a. Let $f : \mathbf{Z} \to H$ be the surjective function defined by $f(m) = a^m$. Note that $f(k + l) = f(k) \cdot f(l)$ where the addition is in $\mathbf{Z}$ and the multiplication is in the group H. We come now to the first real theorem in group theory. It says that the element a has finite order iff f is not injective, and in this case, the order of a is the smallest positive integer n with $a^n = e$.

Theorem Suppose a is an element of a multiplicative group G, and $H = \{a^i : i \in \mathbf{Z}\}$. If $\exists$ distinct integers i and j with $a^i = a^j$, then a has some finite order n. In this case H has n distinct elements, $H = \{a^0, a^1, \ldots, a^{n-1}\}$, and $a^m = e$ iff $n|m$. In particular, the order of a is the smallest positive integer n with $a^n = e$, and $f^{-1}(e) = n\mathbf{Z}$.

Proof Suppose $j < i$ and $a^i = a^j$. Then $a^{i-j} = e$ and thus $\exists$ a smallest positive integer n with $a^n = e$. This implies that the elements of $\{a^0, a^1, ..., a^{n-1}\}$ are distinct, and we must show they are all of H. If $m \in \mathbf{Z}$, the Euclidean algorithm states that $\exists$ integers q and r with $0 \leq r < n$ and $m = nq + r$. Thus $a^m = a^{nq} \cdot a^r = a^r$, and so $H = \{a^0, a^1, ..., a^{n-1}\}$, and $a^m = e$ iff $n|m$. Later in this chapter we will see that f is a homomorphism from an additive group to a multiplicative group and that, in additive notation, H is isomorphic to $\mathbf{Z}$ or $\mathbf{Z}_n$.

Exercise Write out this theorem for G an additive group. To begin, suppose a is an element of an additive group G, and $H = \{ai : i \in \mathbf{Z}\}$.

Exercise Show that if G is a finite group of even order, then G has an odd number of elements of order 2. Note that e is the only element of order 1.

Definition A group G is *cyclic* if $\exists$ an element of G which generates G.

Theorem If G is cyclic and H is a subgroup of G, then H is cyclic.

Proof Suppose $G = \{a^i : i \in \mathbf{Z}\}$ is a cyclic group and H is a subgroup of G. If $H = e$, then H is cyclic, so suppose $H \neq e$. Now there is a smallest positive integer m with $a^m \in H$. If t is an integer with $a^t \in H$, then by the Euclidean algorithm, m divides t, and thus a^m generates H. Note that in the case G has finite order n, i.e., $G = \{a^0, a^1, \ldots, a^{n-1}\}$, then $a^n = e \in H$, and thus the positive integer m divides n. In either case, we have a clear picture of the subgroups of G. Also note that this theorem was proved on page 15 for the additive group $\mathbf{Z}$.

Cosets Suppose H is a subgroup of a group G. It will be shown below that H partitions G into right cosets. It also partitions G into left cosets, and in general these partitions are distinct.

Theorem If H is a subgroup of a multiplicative group G, then $a \sim b$ defined by $a \sim b$ iff $a \cdot b^{-1} \in H$ is an equivalence relation. If $a \in G$, $cl(a) = \{b \in G : a \sim b\} = \{h \cdot a : h \in H\} = Ha$. Note that $a \cdot b^{-1} \in H$ iff $b \cdot a^{-1} \in H$.

If H is a subgroup of an additive group G, then $a \sim b$ defined by $a \sim b$ iff $(a - b) \in H$ is an equivalence relation. If $a \in G$, $cl(a) = \{b \in G : a \sim b\} = \{h + a : h \in H\} = H + a$. Note that $(a - b) \in H$ iff $(b - a) \in H$.

Definition These equivalence classes are called *right cosets*. If the relation is defined by $a \sim b$ iff $b^{-1} \cdot a \in H$, then the equivalence classes are $cl(a) = aH$ and they are called *left cosets*. H is a left and right coset. If G is abelian, there is no distinction between right and left cosets. Note that $b^{-1} \cdot a \in H$ iff $a^{-1} \cdot b \in H$.

In the theorem above, H is used to define an equivalence relation on G, and thus a partition of G. We now do the same thing a different way. We define the right cosets directly and show they form a partition of G. You might find this easier.

Theorem Suppose H is a subgroup of a multiplicative group G. If $a \in G$, define the right coset containing a to be $Ha = \{h \cdot a : h \in H\}$. Then the following hold.

1) $Ha = H$ iff $a \in H$.
2) If $b \in Ha$, then $Hb = Ha$, i.e., if $h \in H$, then $H(h \cdot a) = (Hh)a = Ha$.
3) If $Hc \cap Ha \neq \emptyset$, then $Hc = Ha$.
4) The right cosets form a partition of G, i.e., each a in G belongs to one and only one right coset.
5) Elements a and b belong to the same right coset iff $a \cdot b^{-1} \in H$ iff $b \cdot a^{-1} \in H$.

Proof There is no better way to develop facility with cosets than to prove this theorem. Also write this theorem for G an additive group.

Theorem Suppose H is a subgroup of a multiplicative group G.

1) Any two right cosets have the same number of elements. That is, if $a, b \in G$, $f : Ha \to Hb$ defined by $f(h \cdot a) = h \cdot b$ is a bijection. Also any two left cosets have the same number of elements. Since H is a right and left coset, any two cosets have the same number of elements.

2) G has the same number of right cosets as left cosets. The function F defined by $F(Ha) = a^{-1}H$ is a bijection from the collection of right cosets to the left cosets. The number of right (or left) cosets is called the *index* of H in G.

3) If G is finite, $o(H)$ (index of H) $= o(G)$ and so $o(H) \mid o(G)$. In other words, $o(G)/o(H) =$ the number of right cosets = the number of left cosets.

4) If G is finite, and $a \in G$, then $o(a) \mid o(G)$. (Proof: The order of a is the order of the subgroup generated by a, and by 3) this divides the order of G.)

5) If G has prime order, then G is cyclic, and any element (except e) is a generator. (Proof: Suppose $o(G) = p$ and $a \in G$, $a \neq e$. Then $o(a) \mid p$ and thus $o(a) = p$.)

6) If $o(G) = n$ and $a \in G$, then $a^n = e$. (Proof: $a^{o(a)} = e$ and $n = o(a)\,(o(G)/o(a))$.)

Exercises

i) Suppose G is a cyclic group of order 4, $G = \{e, a, a^2, a^3\}$ with $a^4 = e$. Find the order of each element of G. Find all the subgroups of G.

ii) Suppose G is the additive group $\mathbf{Z}$ and $H = 3\mathbf{Z}$. Find the cosets of H.

iii) Think of a circle as the interval $[0, 1]$ with end points identified. Suppose $G = \mathbf{R}$ under addition and $H = \mathbf{Z}$. Show that the collection of all the cosets of H can be thought of as a circle.

iv) Let $G = \mathbf{R}^2$ under addition, and H be the subgroup defined by $H = \{(a, 2a) : a \in \mathbf{R}\}$. Find the cosets of H. (See the last exercise on p 5.)

Normal Subgroups

We would like to make a group out of the collection of cosets of a subgroup H. In

general, there is no natural way to do that. However, it is easy to do in case H is a normal subgroup, which is described below.

Theorem If H is a subgroup of G, then the following are equivalent.

1) If $a \in G$, then $aHa^{-1} = H$
2) If $a \in G$, then $aHa^{-1} \subset H$
3) If $a \in G$, then $aH = Ha$
4) Every right coset is a left coset, i.e., if $a \in G$, $\exists\ b \in G$ with $Ha = bH$.

Proof 1) $\Rightarrow$ 2) is obvious. Suppose 2) is true and show 3). We have $(aHa^{-1})a \subset Ha$ so $aH \subset Ha$. Also $a(a^{-1}Ha) \subset aH$ so $Ha \subset aH$. Thus $aH = Ha$.
3) $\Rightarrow$ 4) is obvious. Suppose 4) is true and show 3). $Ha = bH$ contains a, so $bH = aH$ because a coset is an equivalence class. Thus $aH = Ha$.
Finally, suppose 3) is true and show 1). Multiply $aH = Ha$ on the right by a^{-1}.

Definition If H satisfies any of the four conditions above, then H is said to be a *normal* subgroup of G. (This concept goes back to Evariste Galois in 1831.)

Note For any group G, G and e are normal subgroups. If G is an abelian group, then every subgroup of G is normal.

Exercise Show that if H is a subgroup of G with index 2, then H is normal.

Exercise Show the intersection of a collection of normal subgroups of G is a normal subgroup of G. Show the union of a monotonic collection of normal subgroups of G is a normal subgroup of G.

Exercise Let $A \subset \mathbf{R}^2$ be the square with vertices $(-1,1), (1,1), (1,-1)$, and $(-1,-1)$, and G be the collection of all "isometries" of A onto itself. These are bijections of A onto itself which preserve distance and angles, i.e., which preserve dot product. Show that with multiplication defined as composition, G is a multiplicative group. Show that G has four rotations, two reflections about the axes, and two reflections about the diagonals, for a total of eight elements. Show the collection of rotations is a cyclic subgroup of order four which is a normal subgroup of G. Show that the reflection about the x-axis together with the identity form a cyclic subgroup of order two which is not a normal subgroup of G. Find the four right cosets of this subgroup. Finally, find the four left cosets of this subgroup.

Quotient Groups Suppose N is a normal subgroup of G, and C and D are cosets. We wish to define a coset E which is the product of C and D. If $c \in C$ and $d \in D$, define E to be the coset containing $c \cdot d$, i.e., $E = N(c \cdot d)$. The coset E does not depend upon the choice of c and d. This is made precise in the next theorem, which is quite easy.

Theorem Suppose G is a multiplicative group, N is a normal subgroup, and G/N is the collection of all cosets. Then $(Na) \cdot (Nb) = N(a \cdot b)$ is a well defined multiplication (binary operation) on G/N, and with this multiplication, G/N is a group. Its identity is N and $(Na)^{-1} = (Na^{-1})$. Furthermore, if G is finite, $o(G/N) = o(G)/o(N)$.

Proof Multiplication of elements in G/N is multiplication of subsets in G. $(Na) \cdot (Nb) = N(aN)b = N(Na)b = N(a \cdot b)$. Once multiplication is well defined, the group axioms are immediate.

Exercise Write out the above theorem for G an additive group. In the additive abelian group $\mathbf{R}/\mathbf{Z}$, determine those elements of finite order.

Example Suppose $G = \mathbf{Z}$ under $+$, $n > 1$, and $N = n\mathbf{Z}$. $\mathbf{Z}_n$, the *group of integers mod n* is defined by $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$. If a is an integer, the coset $a + n\mathbf{Z}$ is denoted by $[a]$. Note that $[a] + [b] = [a + b]$, $-[a] = [-a]$, and $[a] = [a + nl]$ for any integer l. Any additive abelian group has a scalar multiplication over $\mathbf{Z}$, and in this case it is just $[a]m = [am]$. Note that $[a] = [r]$ where r is the remainder of a divided by n, and thus the distinct elements of $\mathbf{Z}_n$ are $[0], [1], ..., [n-1]$. Also $\mathbf{Z}_n$ is cyclic because each of $[1]$ and $[-1] = [n-1]$ is a generator. We already know that if p is a prime, any non-zero element of $\mathbf{Z}_p$ is a generator, because $\mathbf{Z}_p$ has p elements.

Theorem If $n > 1$ and a is any integer, then $[a]$ is a generator of $\mathbf{Z}_n$ iff $(a, n) = 1$.

Proof The element $[a]$ is a generator iff the subgroup generated by $[a]$ contains $[1]$ iff $\exists$ an integer k such that $[a]k = [1]$ iff $\exists$ integers k and l such that $ak + nl = 1$.

Exercise Show that a positive integer is divisible by 3 iff the sum of its digits is divisible by 3. Note that $[10] = [1]$ in $\mathbf{Z}_3$. (See the fifth exercise on page 18.)

Homomorphisms

Homomorphisms are functions between groups that commute with the group operations. It follows that they honor identities and inverses. In this section we list

the basic properties. Properties 11), 12), and 13) show the connections between coset groups and homomorphisms, and should be considered as the cornerstones of abstract algebra. As always, the student should rewrite the material in additive notation.

Definition If G and $\bar{G}$ are multiplicative groups, a function $f : G \to \bar{G}$ is a *homomorphism* if, for all $a, b \in G$, $f(a \cdot b) = f(a) \cdot f(b)$. On the left side, the group operation is in G, while on the right side it is in $\bar{G}$. The *kernel* of f is defined by $\ker(f) = f^{-1}(\bar{e}) = \{a \in G : f(a) = \bar{e}\}$. In other words, the kernel is the set of solutions to the equation $f(x) = \bar{e}$. (If $\bar{G}$ is an additive group, $\ker(f) = f^{-1}(\underline{0})$.)

Examples The constant map $f : G \to \bar{G}$ defined by $f(a) = \bar{e}$ is a homomorphism. If H is a subgroup of G, the inclusion $i : H \to G$ is a homomorphism. The function $f : \mathbf{Z} \to \mathbf{Z}$ defined by $f(t) = 2t$ is a homomorphism of additive groups, while the function defined by $f(t) = t + 2$ is not a homomorphism. The function $h : \mathbf{Z} \to \mathbf{R} - 0$ defined by $h(t) = 2^t$ is a homomorphism from an additive group to a multiplicative group.

We now catalog the basic properties of homomorphisms. These will be helpful later on in the study of ring homomorphisms and module homomorphisms.

Theorem Suppose G and $\bar{G}$ are groups and $f : G \to \bar{G}$ is a homomorphism.

1) $f(e) = \bar{e}$.

2) $f(a^{-1}) = f(a)^{-1}$. The first inverse is in G, and the second is in $\bar{G}$.

3) f is injective $\Leftrightarrow$ $\ker(f) = e$.

4) If H is a subgroup of G, $f(H)$ is a subgroup of $\bar{G}$. In particular, image(f) is a subgroup of $\bar{G}$.

5) If $\bar{H}$ is a subgroup of $\bar{G}$, $f^{-1}(\bar{H})$ is a subgroup of G. Furthermore, if $\bar{H}$ is normal in $\bar{G}$, then $f^{-1}(\bar{H})$ is normal in G.

6) The kernel of f is a normal subgroup of G.

7) If $\bar{g} \in \bar{G}$, $f^{-1}(\bar{g})$ is void or is a coset of $\ker(f)$, i.e., if $f(g) = \bar{g}$ then $f^{-1}(\bar{g}) = Ng$ where $N = \ker(f)$. In other words, if the equation $f(x) = \bar{g}$ has a

solution, then the set of all solutions is a coset of $N = \ker(f)$. This is a key fact which is used routinely in topics such as systems of equations and linear differential equations.

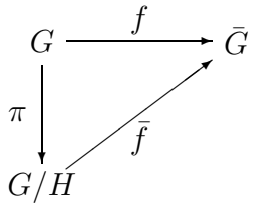
8) The composition of homomorphisms is a homomorphism, i.e., if $h : \bar{G} \to \bar{\bar{G}}$ is a homomorphism, then $h \circ f : G \to \bar{\bar{G}}$ is a homomorphism.

9) If $f : G \to \bar{G}$ is a bijection, then the function $f^{-1} : \bar{G} \to G$ is a homomorphism. In this case, f is called an *isomorphism*, and we write $G \approx \bar{G}$. In the case $G = \bar{G}$, f is also called an *automorphism*.

10) Isomorphisms preserve all algebraic properties. For example, if f is an isomorphism and $H \subset G$ is a subset, then H is a subgroup of G iff $f(H)$ is a subgroup of $\bar{G}$, H is normal in G iff $f(H)$ is normal in $\bar{G}$, G is cyclic iff $\bar{G}$ is cyclic, etc. Of course, this is somewhat of a cop-out, because an algebraic property is one that, by definition, is preserved under isomorphisms.

11) Suppose H is a normal subgroup of G. Then $\pi : G \to G/H$ defined by $\pi(a) = Ha$ is a surjective homomorphism with kernel H. Furthermore, if $f : G \to \bar{G}$ is a surjective homomorphism with kernel H, then $G/H \approx \bar{G}$ (see below).

12) Suppose H is a normal subgroup of G. If $H \subset \ker(f)$, then $\bar{f} : G/H \to \bar{G}$ defined by $\bar{f}(Ha) = f(a)$ is a well-defined homomorphism making the following diagram commute.



Thus defining a homomorphism on a quotient group is the same as defining a homomorphism on the numerator which sends the denominator to $\bar{e}$. The image of $\bar{f}$ is the image of f and the kernel of $\bar{f}$ is $\ker(f)/H$. Thus if $H = \ker(f)$, $\bar{f}$ is injective, and thus $G/H \approx \text{image}(f)$.

13) Given any group homomorphism f, $\text{domain}(f)/\ker(f) \approx \text{image}(f)$. This is the fundamental connection between quotient groups and homomorphisms.

14) Suppose K is a group. Then K is an infinite cycle group iff K is isomorphic to the integers under addition, i.e., $K \approx \mathbf{Z}$. K is a cyclic group of order n iff $K \approx \mathbf{Z}_n$.

Proof of 14) Suppose $\bar{G} = K$ is generated by some element a. Then $f : \mathbf{Z} \to K$ defined by $f(m) = a^m$ is a homomorphism from an additive group to a multiplicative group. If $o(a)$ is infinite, f is an isomorphism. If $o(a) = n$, $\ker(f) = n\mathbf{Z}$ and $\bar{f} : \mathbf{Z}_n \to K$ is an isomorphism.

Exercise If a is an element of a group G, there is always a homomorphism from $\mathbf{Z}$ to G which sends 1 to a. When is there a homomorphism from $\mathbf{Z}_n$ to G which sends $[1]$ to a? What are the homomorphisms from $\mathbf{Z}_2$ to $\mathbf{Z}_6$? What are the homomorphisms from $\mathbf{Z}_4$ to $\mathbf{Z}_8$?

Exercise Suppose G is a group and g is an element of G, $g \neq e$.

1) Under what conditions on g is there a homomorphism $f : \mathbf{Z}_7 \to G$ with $f([1]) = g$?

2) Under what conditions on g is there a homomorphism $f : \mathbf{Z}_{15} \to G$ with $f([1]) = g$?

3) Under what conditions on G is there an injective homomorphism $f : \mathbf{Z}_{15} \to G$?

4) Under what conditions on G is there a surjective homomorphism $f : \mathbf{Z}_{15} \to G$?

Exercise We know every finite group of prime order is cyclic and thus abelian. Show that every group of order four is abelian.

Exercise Let $G = \{h : [0,1] \to \mathbf{R} : h \text{ has an infinite number of derivatives}\}$. Then G is a group under addition. Define $f : G \to G$ by $f(h) = \frac{dh}{dt} = h'$. Show f is a homomorphism and find its kernel and image. Let $g : [0,1] \to \mathbf{R}$ be defined by $g(t) = t^3 - 3t + 4$. Find $f^{-1}(g)$ and show it is a coset of $\ker(f)$.

Exercise Let G be as above and $g \in G$. Define $f : G \to G$ by $f(h) = h'' + 5h' + 6t^2h$. Then f is a group homomorphism and the differential equation $h'' + 5h' + 6t^2h = g$ has a solution iff g lies in the image of f. Now suppose this equation has a solution and $S \subset G$ is the set of all solutions. For which subgroup H of G is S an H-coset?

Exercise Suppose G is a multiplicative group and $a \in G$. Define $f : G \to G$ to be conjugation by a, i.e., $f(g) = a^{-1} \cdot g \cdot a$. Show that f is a homomorphism. Also show f is an automorphism and find its inverse.

Permutations

Suppose X is a (non-void) set. A bijection $f : X \to X$ is called a *permutation* on X, and the collection of all these permutations is denoted by $S = S(X)$. In this setting, variables are written on the left, i.e., $f = (x)f$. Therefore the composition $f \circ g$ means "f followed by g". $S(X)$ forms a multiplicative group under composition.

Exercise Show that if there is a bijection between X and Y, there is an isomorphism between $S(X)$ and $S(Y)$. Thus if each of X and Y has n elements, $S(X) \approx S(Y)$, and these groups are called the *symmetric* groups on n elements. They are all denoted by the one symbol S_n.

Exercise Show that $o(S_n) = n!$. Let $X = \{1, 2, ..., n\}$, $S_n = S(X)$, and $H = \{f \in S_n : (n)f = n\}$. Show H is a subgroup of S_n which is isomorphic to S_{n-1}. Let g be any permutation on X with $(n)g = 1$. Find $g^{-1}Hg$.

The next theorem shows that the symmetric groups are incredibly rich and complex.

Theorem (Cayley's Theorem) Suppose G is a multiplicative group with n elements and S_n is the group of all permutations on the set G. Then G is isomorphic to a subgroup of S_n.

Proof Let $h : G \to S_n$ be the function which sends a to the bijection $h_a : G \to G$ defined by $(g)h_a = g \cdot a$. The proof follows from the following observations.

1) For each given a, h_a is a bijection from G to G.
2) h is a homomorphism, i.e., $h_{a \cdot b} = h_a \circ h_b$.
3) h is injective and thus G is isomorphic to image $(h) \subset S_n$.

The Symmetric Groups Now let $n \geq 2$ and let S_n be the group of all permutations on $\{1, 2, ..., n\}$. The following definition shows that each element of S_n may

be represented by a matrix.

Definition Suppose $1 < k \leq n$, $\{a_1, a_2, ..., a_k\}$ is a collection of distinct integers with $1 \leq a_i \leq n$, and $\{b_1, b_2, ..., b_k\}$ is the same collection in some different order. Then the matrix $\begin{pmatrix} a_1 & a_2 \dots a_k \\ b_1 & b_2 \dots b_k \end{pmatrix}$ represents $f \in S_n$ defined by $(a_i)f = b_i$ for $1 \leq i \leq k$, and $(a)f = a$ for all other a. The composition of two permutations is computed by applying the matrix on the left first and the matrix on the right second.

There is a special type of permutation called a *cycle*. For these we have a special notation.

Definition $\begin{pmatrix} a_1 & a_2 \dots a_{k-1} a_k \\ a_2 & a_3 \dots a_k \quad a_1 \end{pmatrix}$ is called a k-cycle, and is denoted by $(a_1, a_2, ..., a_k)$. A 2-cycle is called a *transposition*. The cycles $(a_1, ..., a_k)$ and $(c_1, ..., c_\ell)$ are *disjoint* provided $a_i \neq c_j$ for all $1 \leq i \leq k$ and $1 \leq j \leq \ell$.

Listed here are eight basic properties of permutations. They are all easy except 4), which takes a little work. Properties 9) and 10) are listed solely for reference.

Theorem

1) Disjoint cycles commute. (This is obvious.)

2) Every nonidentity permutation can be written uniquely (except for order) as the product of disjoint cycles. (This is easy.)

3) Every permutation can be written (non-uniquely) as the product of transpositions. (Proof: $I = (1,2)(1,2)$ and $(a_1, ..., a_k) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_k)$.)

4) The parity of the number of these transpositions is unique. This means that if f is the product of p transpositions and also of q transpositions, then p is even iff q is even. In this case, f is said to be an *even* permutation. In the other case, f is an *odd* permutation.

5) A k-cycle is even (odd) iff k is odd (even). For example $(1,2,3) = (1,2)(1,3)$ is an even permutation.

6) Suppose $f, g \in S_n$. If one of f and g is even and the other is odd, then $g \circ f$ is

odd. If f and g are both even or both odd, then $g \circ f$ is even. (Obvious.)

7) The map $h : S_n \to \mathbf{Z}_2$ defined by $h(\text{even}) = [0]$ and $h(\text{odd}) = [1]$ is a homomorphism from a multiplicative group to an additive group. Its kernel (the subgroup of even permutations) is denoted by A_n and is called the *alternating* group. Thus A_n is a normal subgroup of index 2, and $S_n/A_n \approx \mathbf{Z}_2$.

8) If a, b, c and d are distinct integers in $\{1, 2, \ldots, n\}$, then $(a, b)(b, c) = (a, c, b)$ and $(a, b)(c, d) = (a, c, d)(a, c, b)$. Since $I = (1, 2, 3)^3$, it follows that for $n \geq 3$, every even permutation is the product of 3-cycles.

The following parts are not included in this course. They are presented here merely for reference.

9) For any $n \neq 4$, A_n is simple, i.e., has no proper normal subgroups.

10) S_n can be generated by two elements. In fact, $\{(1, 2), (1, 2, ..., n)\}$ generates S_n. (Of course there are subgroups of S_n which cannot be generated by two elements).

Proof of 4) It suffices to prove if the product of t transpositions is the identity I on $\{1, 2, \ldots, n\}$, then t is even. Suppose this is false and I is written as t transpositions, where t is the smallest odd integer this is possible. Since t is odd, it is at least 3. Suppose for convenience the first transposition is (a, n). We will rewrite I as a product of transpositions $\sigma_1\sigma_2 \cdots \sigma_t$ where $(n)\sigma_i = (n)$ for $1 \leq i < t$ and $(n)\sigma_t \neq n$, which will be a contradiction. This can be done by inductively "pushing n to the right" using the equations below. If a, b, and c are distinct integers in $\{1, 2, \ldots, n-1\}$, then $(a, n)(a, n) = I$, $(a, n)(b, n) = (a, b)(a, n)$, $(a, n)(a, c) = (a, c)(c, n)$, and $(a, n)(b, c) = (b, c)(a, n)$. Note that $(a, n)(a, n)$ cannot occur here because it would result in a shorter odd product. (Now you may solve the tile puzzle on page viii.)

Exercise

1) Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 4 & 3 & 1 & 7 & 2 \end{pmatrix}$ as the product of disjoint cycles.
Write (1,5,6,7)(2,3,4)(3,7,1) as the product of disjoint cycles.
Write (3,7,1)(1,5,6,7)(2,3,4) as the product of disjoint cycles.
Which of these permutations are odd and which are even?

2) Suppose $(a_1, \ldots, a_k)$ and $(c_1, \ldots, c_\ell)$ are disjoint cycles. What is the order of their product?

3) Suppose $\sigma \in S_n$. Show that $\sigma^{-1}(1,2,3)\sigma = ((1)\sigma, (2)\sigma, (3)\sigma)$. This shows that conjugation by σ is just a type of relabeling. Also let $\tau = (4,5,6)$ and find $\tau^{-1}(1,2,3,4,5)\tau$.

4) Show that $H = \{\sigma \in S_6 : (6)\sigma = 6\}$ is a subgroup of S_6 and find its right cosets and its left cosets.

5) Let $A \subset \mathbf{R}^2$ be the square with vertices $(-1,1), (1,1), (1,-1)$, and $(-1,-1)$, and G be the collection of all isometries of A onto itself. We know from a previous exercise that G is a group with eight elements. It follows from Cayley's theorem that G is isomorphic to a subgroup of S_8. Show that G is isomorphic to a subgroup of S_4.

6) If G is a multiplicative group, define a new multiplication on the set G by $a \circ b = b \cdot a$. In other words, the new multiplication is the old multiplication in the opposite order. This defines a new group denoted by G^{op}, the opposite group. Show that it has the same identity and the same inverses as G, and that $f : G \to G^{op}$ defined by $f(a) = a^{-1}$ is a group isomorphism. Now consider the special case $G = S_n$. The convention used in this section is that an element of S_n is a permutation on $\{1, 2, \ldots, n\}$ with the variable written on the left. Show that an element of S_n^{op} is a permutation on $\{1, 2, \ldots, n\}$ with the variable written on the right. (Of course, either S_n or S_n^{op} may be called the symmetric group, depending on personal preference or context.)

Product of Groups

The product of groups is usually presented for multiplicative groups. It is presented here for additive groups because this is the form that occurs in later chapters. As an exercise, this section should be rewritten using multiplicative notation. The two theorems below are transparent and easy, but quite useful. For simplicity we first consider the product of two groups, although the case of infinite products is only slightly more difficult. For background, read first the two theorems on page 11.

Theorem Suppose G_1 and G_2 are additive groups. Define an addition on $G_1 \times G_2$ by $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$. This operation makes $G_1 \times G_2$ into a group. Its "zero" is $(\underline{0}_1, \underline{0}_2)$ and $-(a_1, a_2) = (-a_1, -a_2)$. The projections $\pi_1 : G_1 \times G_2 \to G_1$

and $\pi_2 : G_1 \times G_2 \to G_2$ are group homomorphisms. Suppose G is an additive group. We know there is a bijection from {functions $f : G \to G_1 \times G_2$} to {ordered pairs of functions (f_1, f_2) where $f_1 : G \to G_1$ and $f_2 : G \to G_2$}. Under this bijection, f is a group homomorphism iff each of f_1 and f_2 is a group homomorphism.

Proof It is transparent that the product of groups is a group, so let's prove the last part. Suppose G, G_1, and G_2 are groups and $f = (f_1, f_2)$ is a function from G to $G_1 \times G_2$. Now $f(a+b) = (f_1(a+b), f_2(a+b))$ and $f(a) + f(b) = (f_1(a), f_2(a)) + (f_1(b), f_2(b)) = (f_1(a) + f_1(b), f_2(a) + f_2(b))$. An examination of these two equations shows that f is a group homomorphism iff each of f_1 and f_2 is a group homomorphism.

Exercise Suppose G_1 and G_2 are groups. Show that $G_1 \times G_2$ and $G_2 \times G_1$ are isomorphic.

Exercise If $o(a_1) = m$ and $o(a_2) = n$, find the order of (a_1, a_2) in $G_1 \times G_2$.

Exercise Show that if G is any group of order 4, G is isomorphic to $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. Show $\mathbf{Z}_4$ is not isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$. Show $\mathbf{Z}_{12}$ is isomorphic to $\mathbf{Z}_4 \times \mathbf{Z}_3$. Finally, show that $\mathbf{Z}_{mn}$ is isomorphic to $\mathbf{Z}_m \times \mathbf{Z}_n$ iff $(m, n) = 1$.

Exercise Suppose G_1 and G_2 are groups and $i_1 : G_1 \to G_1 \times G_2$ is defined by $i_1(g_1) = (g_1, \underline{0}_2)$. Show i_1 is an injective group homomorphism and its image is a normal subgroup of $G_1 \times G_2$. Usually G_1 is identified with its image under i_1, so G_1 may be considered to be a normal subgroup of $G_1 \times G_2$. Let $\pi_2 : G_1 \times G_2 \to G_2$ be the projection map defined in the Background chapter. Show π_2 is a surjective homomorphism with kernel G_1. Therefore $(G_1 \times G_2)/G_1 \approx G_2$ as you would expect.

Exercise Let $\mathbf{R}$ be the reals under addition. Show that the addition in the product $\mathbf{R} \times \mathbf{R}$ is just the usual addition in analytic geometry.

Exercise Suppose $n > 2$. Is S_n isomorphic to $A_n \times G$ where G is a multiplicative group of order 2 ?

One nice thing about the product of groups is that it works fine for any finite number, or even any infinite number. The next theorem is stated in full generality.

Theorem Suppose T is an index set, and for any $t \in T$, G_t is an additive group. Define an addition on $\prod_{t\in T} G_t = \prod G_t$ by $\{a_t\} + \{b_t\} = \{a_t + b_t\}$. This operation makes the product into a group. Its "zero" is $\{\underline{0}_t\}$ and $-\{a_t\} = \{-a_t\}$. Each projection $\pi_s : \prod G_t \to G_s$ is a group homomorphism. Suppose G is an additive group. Under the natural bijection from $\{\text{functions } f : G \to \prod G_t\}$ to $\{\text{sequences of functions } \{f_t\}_{t\in T} \text{ where } f_t : G \to G_t\}$, f is a group homomorphism iff each f_t is a group homomorphism. Finally, the scalar multiplication on $\prod G_t$ by integers is given coordinatewise, i.e., $\{a_t\}n = \{a_t n\}$.

Proof The addition on $\prod G_t$ is coordinatewise.

Exercise Suppose s is an element of T and $\pi_s : \prod G_t \to G_s$ is the projection map defined in the Background chapter. Show π_s is a surjective homomorphism and find its kernel.

Exercise Suppose s is an element of T and $i_s : G_s \to \prod G_t$ is defined by $i_s(a) = \{a_t\}$ where $a_t = \underline{0}$ if $t \neq s$ and $a_s = a$. Show i_s is an injective homomorphism and its image is a normal subgroup of $\prod G_t$. Thus each G_s may be considered to be a normal subgroup of $\prod G_t$.

Exercise Let $f : \mathbf{Z} \to \mathbf{Z}_{30} \times \mathbf{Z}_{100}$ be the homomorphism defined by $f(m) = ([4m], [3m])$. Find the kernel of f. Find the order of $([4], [3])$ in $\mathbf{Z}_{30} \times \mathbf{Z}_{100}$.

Exercise Let $f : \mathbf{Z} \to \mathbf{Z}_{90} \times \mathbf{Z}_{70} \times \mathbf{Z}_{42}$ be the group homomorphism defined by $f(m) = ([m], [m], [m])$. Find the kernel of f and show that f is not surjective. Let $g : \mathbf{Z} \to \mathbf{Z}_{45} \times \mathbf{Z}_{35} \times \mathbf{Z}_{21}$ be defined by $g(m) = ([m], [m], [m])$. Find the kernel of g and determine if g is surjective. Note that the gcd of $\{45, 35, 21\}$ is 1. Now let $h : \mathbf{Z} \to \mathbf{Z}_8 \times \mathbf{Z}_9 \times \mathbf{Z}_{35}$ be defined by $h(m) = ([m], [m], [m])$. Find the kernel of h and show that h is surjective. Finally suppose each of $b, c,$ and d is greater than 1 and $f : \mathbf{Z} \to \mathbf{Z}_b \times \mathbf{Z}_c \times \mathbf{Z}_d$ is defined by $f(m) = ([m], [m], [m])$. Find necessary and sufficient conditions for f to be surjective (see the first exercise on page 18).

Exercise Suppose T is a non-void set, G is an additive group, and G^T is the collection of all functions $f : T \to G$ with addition defined by $(f+g)(t) = f(t)+g(t)$. Show G^T is a group. For each $t \in T$, let $G_t = G$. Note that G^T is just another way of writing $\prod_{t\in T} G_t$. Also note that if $T = [0, 1]$ and $G = \mathbf{R}$, the addition defined on G^T is just the usual addition of functions used in calculus. (For the ring and module versions, see exercises on pages 44 and 69.)