CHAPTER I

GROUPS

1. Preliminaries

The basic framework in which modern mathematics is developed is *set theory*. We assume familiarity with the notation and basic concepts of that subject. Where relatively advanced set theoretic notions are needed, we will introduce them. For a thorough treatment of set theory as used in modern mathematics, see [Enderton]. Most books on Algebra (e.g. [Lang]) have a short summary at the beginning.

In principle, algebra is developed in a complete and rigorous manner from set theory. In fact, since it is done by people, the development is not complete and often contains minor flaws in logic or notation. In working problems, you should try to develop your skill in the *art* of mathematical exposition. Since you cannot say everything, you should learn what it is important to say and what it is important to leave out.

2. Group Theory

We shall be studying a variety of *algebraic structures* starting with groups. Algebraic structures are usually defined as sets with certain operations satisfying appropriate rules or axioms.

Given a set X, we use the term *binary operation* or *law of composition* for a function

$$* : X \times X \to X.$$

The result of applying the function $*$ to a pair (x, y) would in conventional functional notation be denoted

$$*(x, y)$$

but several other common notations exist. These are

Prefix:	$*xy$	No parentheses or commas used
Infix:	$x * y$	Most commonly used notation.
Postfix:	$xy*$	

The *name* of the function should in principle be unique in each case, but we commonly use the same symbols $(*, +, \dots)$ for different examples of the same structure or even for entirely different structures. In group theory, the most commonly used names for the operations are '+' and '' (the empty string.) In the latter case, prefix, infix, and postfix notation all result in the same notation for the result of the operation

$$(x, y) \mapsto xy$$

(i.e., juxtaposition.)

Sometimes exponential notation, as in x^y, is used to denote the result of a binary operation. There is also an alternate form of this, which you may not have seen, in which the exponent is put to the left of the base, as in ${}^y x$.

In order to keep track of the order in which repeated applications of the operation are performed, we must use parentheses. For example, (using juxtapositional notation for the operation) we cannot assume that

$$x(y(z(wx))) = ((xy)(z(wx))).$$

However, if the binary operation obeys the *associative law*

$$x(yz) = (xy)z \qquad \text{for all } x, y, z \in X$$

then it may be proved that any meaningful insertion of parentheses into a string of elements of X yields the same result, and so we may omit parentheses. If you have never seen this proved, you should try to prove it now. If you have any trouble, see one of the references (e.g., [Lang]). We denote the product $x_1 x_2 \cdots x_n$ by x^n if $x_i = x$ for all i. The usual laws of exponents hold.

An element e of X is called a left (right) *identity* if

$$ex = x \quad (xe = x) \qquad \text{for all } x \in X.$$

If e is both a left and right identity it is just called an identity or sometimes a two-sided identity.

An operation is called *commutative* if $xy = yx$ for all $x, y \in X$.

If X has an identity e (left, right, or both), and x is any element of X, then an element $y \in X$ is called a left inverse for x (relative to e) if $yx = e$. (You should be able to figure out what a right inverse would be.) An element which is both a left and right inverse for x is just called an inverse or sometimes a two-sided inverse.

A *group* consists of a set G and a binary operation satisfying the following rules:

1) The operation is associative.
2) There is an identity.
3) For each element of G there is an inverse.

It is possible to weaken these axioms and still have a logically equivalent set of axioms. For example, the proper combination of one sided identity and one sided inverse will work quite well. Also, it is not hard to see that there is exactly one identity in a group and that each element has exactly one inverse. If juxtapositional notation is used, we will generally denote the identity by 1 and the inverse of x by x^{-1}. If the operation is denoted by '+', then 0 denotes the identity and $-x$ denotes the inverse of x. See an introductory book on algebra (e.g. [Herstein] or [Saracino]) for such a discussion of these points.

If the binary group operation is commutative, we say the group is *abelian*. (That term is pretty much restricted to group theory; other structures with commutative operations are just called commutative.)

Examples.

1) Let M_n denote the set of $n \times n$ matrices with real entries, and let the law of composition be matrix multiplication. The identity matrix I is the identity element for matrix multiplication. It is shown in linear algebra courses that a matrix is left invertible if and only if it is right invertible, so in either case it has a two sided inverse which is unique. In addition an $n \times n$ matrix A is invertible if and only if $\det A \neq 0$. One also calls such matrices *non-singular*.

It is not too hard to see that the set of $n \times n$ invertible (i.e., non-singular) matrices is closed under multiplication. One easy way to see this is to use the product rule

$$\det(AB) = \det(A)\det(B).$$

Denote the set of non-singular $n \times n$ matrices by $GL(n)$. Then matrix multiplication provides a binary operation on this set under which it becomes a group. The inverse of a matrix A is the usual matrix inverse.

To get a bit ahead of ourselves, if k is any field, we may similarly define the group $Gl(n, k)$ of non-singular $n \times n$ matrices with entries in that field. The fields you are most likely to have encountered so far are the fields $\mathbf{R}$ and $\mathbf{C}$ of real and complex numbers respectively.

2) Let X be any set and let $E(X)$ denote the set of all functions $f : X \to X$. Let the binary operation be the composition of functions $f \circ g$ (where $f \circ g(x) = f(g(x))$.) Composition is associative, and the identity function Id_X is an identity, but generally a function $f : X \to X$ has neither a left inverse nor a right inverse. A function f which is onto, i.e, such that $X = f(X) = \{f(x)|x \in X\}$, always has a right inverse. Similarly, a function that is one-to-one, i.e., such that $f(x) = f(y) \Rightarrow x = y$, always has a left inverse. The subset $S(X)$ of $E(X)$ consisting of all functions which are both one-to-one and onto—such *functions are called bijections*—can be shown to be closed under composition. So it forms a group if the binary operation is composition of functions. The set $E(X)$ does not form a group because inverses may not exist. It is an example of an algebraic structure called a *monoid*, where we require only the associative law and existence of an identity.

If X is finite, the bijections are usually called permutations, and the group $S(X)$ is called the *symmetric group* on the set X. For the special case $X = \{1, 2, \ldots, n\}$, we use the notation $S_n = S(X)$ and call the group the symmetric group of degree n. In this case we also use a special notation to denote elements

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n). \end{pmatrix}$$

3) We denote the system of integers by $\mathbf{Z}$. It is a group under the operation $+$. Also, if n is a positive integer, the set

$$\mathbf{Z}/n\mathbf{Z} = \{0, 1, 2, \ldots, n-1\}$$

forms a group under the operation of addition modulo $n : x + y \mod n =$ the remainder of $x + y$ on division by n.

4) Let $\mathbf{S}$ be a collection of sets. (We have to be careful because if $\mathbf{S}$ is too large—e.g., the collection of all sets—we will run into well known logical paradoxes.) For each pair of sets X, Y in $\mathbf{S}$, let $\mathrm{Map}(X, Y)$ denote the set of functions $f : X \to Y$. Let C denote the union of all sets $\mathrm{Map}(X, Y)$ for X, Y in $\mathbf{S}$. Given $f, g \in C$, if the domain of g is the same as the codomain (also called range) of f, then the composition $g \circ f$ is defined and is also an element of C. If $f : X \to Y$, then the identity function $\mathrm{Id}_X : X \to X$ is a right identity for f, i.e., $f \circ \mathrm{Id}_X = f$. Similarly, Id_Y is a left identity for f. The algebraic structure C is clearly not a group. But it comes close to being a monoid except for the fact that composition is not a binary operation in the previous sense since it is only defined for *some* pairs (f, g). The algebraic structure C is an example of a structure called a *category*, which is very important in modern mathematics. We shall return to categories later.

We use the notation $|X|$ to denote the cardinality of the set X. If G is a group, then $|G|$ is called the *order* of G. For example,

$$|\mathbf{Z}/n\mathbf{Z}| = n.$$
$$|S_n| = n! \qquad \text{(Do you remember the proof?)}$$

Exercises.

1. Let $f : X \to X$.
   (a) Prove f is one-to-one if and only if there is a $g : X \to X$ such that $g \circ f = \mathrm{Id}_X$. What if f is onto?
   (b) Prove that if X is finite then f is one-to-one if and only if it is onto. Give an example of a one-to-one function on an infinite set which is not onto.

2. Show that the set of all $n \times n$ real matrices with determinant one forms a group under matrix multiplication.

3. Let $V = \mathbf{R}^3$ and set $C = \mathbf{R} \times V$. (So as a real vector space, C may be identified with $\mathbf{R}^4$.) Define a product on C by $(a, \mathbf{u})(b, \mathbf{v}) = (ab - \mathbf{u} \cdot \mathbf{v}, a\mathbf{v} + b\mathbf{u} + \mathbf{u} \times \mathbf{v})$. ($C$ is called the *quaternion algebra*. Define $N(a, \mathbf{u}) = a^2 + |\mathbf{u}|^2$.
   (a) Show that the product defined above is associative.
   (b) Show that $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbf{C}$.
   (c) Show that the set of nonzero elements of C is a group under multiplication. .

3. Subgroups and homomorphisms

Let G be a group. A **nonempty** subset H of G is called a *subgroup* if $x, y \in H \Rightarrow xy^{-1} \in H$. (Note that this implies $1 = xx^{-1} \in H$. Also, if $x \in H$, then it follows that $x^{-1} = 1x^{-1} \in H$. Hence, a subgroup is closed under products (since $(x^-)^{-1} = x$) and taking inverses. Conversely, one may show that a nonempty subset closed under products and inverses is a subgroup.) It is not too hard to see that if H is finite, then it is a subgroup provided it is just closed under taking products.

Let G and G' be groups. A function $f : G \to G'$ is called a *homomorphism* if $f(xy) = f(x)f(y)$ for all $x, y \in G$. If f is a homomorphism, then one can show that $f(1_G) = 1_{G'}$. Also, for each $x \in G$, we have $f(x^{-1}) = f(x)^{-1}$.

$\mathrm{Im}(f) = \{f(x) \mid x \in G\}$ is a subgroup of G'.

A homomorphism $f : G \to G'$ is surjective if $\mathrm{Im}(f) = G'$. It is *injective* if f is one-to-one. f is called an *isomorphism* if it is both surjective and injective (and in that case, the inverse function $f^{-1} : G' \to G$ is also an isomorphism.) Often the terms *epimorphism* and *monomorphism* are used for *homomorphisms* which are onto or one-to-one respectively.

If there is an isomorphism $f : G \to G'$ from one group G onto another G', we say the groups are isomorphic and we write $G \cong G'$.

Let G be a group. A homomorphism $f : G \to G$ is called an *endomorphism*. If $f : G \to G'$ is also an isomorphism, it is called an *automorphism*. Let $\mathrm{Aut}(G)$ denote the subset of $S(G)$ consisting of all automorphisms. If f, g are automorphisms, then

$$(f \circ g)(xy) = f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y)) = (f \circ g)(x)(f \circ g)(y).$$

Hence, $\mathrm{Aut}(G)$ is closed under composition. Similarly, one can show that it is closed under taking inverses. Hence, it is a subgroup of $S(G)$.

Let G be a group. One way to investigate the structure of G is to study homomorphisms $\phi : G \to S(X)$ into the permutation group on some set X. Such homomorphisms are often called *representations*. If X is also a group, it is even better to have a homomorphism $\phi : G \to \mathrm{Aut}(X)$. The advantage of using a representation of a group is that you can relate the group to a relatively more concrete structure which may have additional features which you can use.

There are always two representations which always exist for any group. The first shows that G can be represented as a subgroup of the symmetric group $S(G)$.

THEOREM (CAYLEY). *Let G be a group. $\rho : G \to S(G)$ defined by $\rho(g)(x) = gx$ is a monomorphism.*

PROOF.

$$\rho(gh)(x) = (gh)x = g(hx) = g(\rho(h)(x)) = \rho(g)(\rho(h)(x)) = \rho(g) \circ \rho(h)(x)$$

so $\rho(gh) = \rho(g) \circ \rho(h)$. Hence, ρ is a homomorphism.

Also, $\rho(g) = \rho(h) \Rightarrow gx = hx$ for all $x \in G$, including $x = 1_G$, so $g = h$. Hence, ρ is one-to-one. □

Note: It was once thought that this theorem greatly simplified the theory of abstract groups by reducing it to the theory of permutation groups which seemed much more concrete. In fact, it didn't really help that much, but extensions of this idea to be discussed later really are quite helpful.

The second representation of G employs $\mathrm{Aut}(G)$. Define $\alpha : G \to \mathrm{Aut}(G)$ by $\alpha(g)(x) = gxg^{-1}$. ($\alpha(g)$ is in fact an automorphism of G since $\alpha(g)(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1}$. It is called an *inner automorphism.*)

PROPOSITION. *$\alpha : G \to \mathrm{Aut}(G)$ is a homomorphism.*

PROOF. Left to the student.

Note that α won't generally be a monomorphism.

Some Notation and terminology. If $\phi : G \to S(X)$ is a representation of G in a permutation group, we sometimes use the shorthand notation

$$gx = \phi(g)(x) \qquad \text{for } g \in G \text{ and } x \in X. \tag{A}$$

The rule $\phi(gh) = \phi(g) \circ \phi(h)$ then becomes

$$(gh)x = g(hx) \qquad \text{for all } g, h \in G, x \in X.$$

In other words, we can think of ϕ as providing a binary operation $G \times X \to X$ which obeys the associative law stated above, and such that

$$1x = x \qquad \text{for all } x \in X$$

since $\phi(1) = \mathrm{Id}_X$, Also, given any such a binary operation, we can define a homomorphism $\phi : G \to S(X)$ by reading the formula (A) the other way.) In case X is itself a group, and $\phi : G \to \mathrm{Aut}(X)$ then we have something of a notational problem. If the group operation in X is denoted by some symbol like '+', then the fact that each $\phi(g)$ is an automorphism becomes

$$\phi(g)(x + y) = \phi(g)(x) + \phi(g)(y) \quad \text{or} \quad g(x + y) = gx + gy.$$

On the other hand, if the operation in X is denoted by juxtaposition, the corresponding formula becomes too confusing. Hence, in that case we introduce *pre-exponential* notation: ${}^g x = \phi(g)(x)$. (This is a variation of the more common exponential notation for conjugation $h^g = g^{-1}hg$ for $h, g \in G$.) The fact that $\phi(g)$ is an automorphism now reads

$${}^g(xy) = {}^g x\, {}^g y.$$

Whatever the notation, when we intend to suppress the name of the representation, we say that G *acts* on X.

Introduce the notation $H \leq G$ to mean H is a subgroup of G.

Suppose H and K are subgroups of the group G. Then the intersection $H \cap K$ is a subgroup. (Proof?) Moreover, the same is true for the intersection of any family of subgroups. It may even be an infinite family of subgroups. $H \cap K$ is in fact the *largest* subgroup of G which is contained in both H and K.

On the other hand, the union $H \cup K$ is not generally a subgroup of G.

Let $S \subseteq G$ be a subset of G. Denote by $\langle S \rangle$ the smallest subgroup of G which contains S. It is called the *subgroup generated by* S. It is not too hard to see that

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H.$$

Another way to describe $\langle S \rangle$ is as the set of all finite products

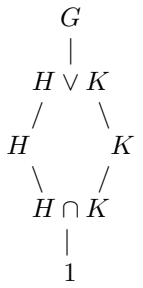
$$x_1 x_2 x_3 \cdots x_n$$

where each x_i is either an element of S or the inverse of such an element. The identity is obtained by using the empty product.

In particular, if $S = \{x\}$ consists of a single element, then $\langle x \rangle$ is called the *cyclic group generated by* x. It consists of all powers of x (assuming juxtapositional notation.)

If $x^n = 1$ for some positive integer n, we say x is a *torsion element*. In that case, the least positive n with that property is called the *order* of x and is denoted $o(x)$. If x is not a torsion element, we say its order is infinite.

Let H and K be subgroups of G. $\langle H \cup K \rangle$ is the smallest subgroup of G containing both H and K. It is called the subgroup generated by H and K and it is denoted $H \vee K$. Let $HK = \{hk | h \in H, k \in K\}$. HK is not generally a subgroup. $HK \subseteq \langle H \vee K \rangle$. We can summarize some of the above concepts in the diagram



Exercises.

1. Show that every subgroup of the additive group of integers $\mathbf{Z}$ is of the form $n\mathbf{Z}$ for some non-negative integer n.
2. If G is a group and H is a finite nonempty subset closed under products, show than H is a subgroup.
3. Show that if every element of a group G has order at most two, then G is abelian.
4. Show that every subgroup of a group of index two is normal.
5. Let C be a cyclic group of order n. Show that there is a unique subgroup of order d for each $d \mid n$. Show also that the subgroup of order d' is contained in the subgroup of order d'' if and only if $d' \mid d''$.
6. Determine under which conditions $H \cup K$ is a subgroup of G if H and K are subgroups of G.
7. Consider the quaternion algebra C defined the exercises for the previous section.

(a) Show that the set of all $\alpha \in C$ for which $N(\alpha) = 1$ is a subgroup of the group C^* of nonzero elements. Note that this set may be identified with the unit 3-sphere S^3 in $\mathbf{R}^4$.

(b) Let $\mathbf{i}, \mathbf{j}, \mathbf{k}$ be the usual orthonormal basis of unit vectors on the coordinate axes in $V = \mathbf{R}^3$. By abuse of notation, write also $\mathbf{i} = (0, \mathbf{i}), \mathbf{j} = (0, \mathbf{j}), \mathbf{k} = (0, \mathbf{k})$. Find the subgroup of C^* generated by $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$, and show it is of order eight.

4. Cosets, kernels, and the isomorphism theorems

Let G be a group and suppose $H \leq G$. Define

$$x \equiv y \quad \text{to mean} \quad x^{-1}y \in H.$$

It is easy to see that $\equiv$ is an equivalence relation. (See [Saracino] or [Herstein] for a review of equivalence relations.) Also,

$$x \equiv y \quad \text{if and only if} \quad x \in yH = \{yh \mid h \in H\}.$$

Thus, the sets yH are the equivalence classes of this relation. They are called *left cosets*. By the general theory of equivalence relations, we have

$$x \equiv y \quad \text{if and only if} \quad xH = yH.$$

Similarly, we can define another equivalence relation $\equiv'$ by reversing the order in the product, and the resulting equivalence classes Hx are called *right cosets*.

Multiplication by x is a bijection, so for any subset of G, S, Sx and xS have the same cardinality. Hence, all cosets of a subgroup have the same cardinality.

THEOREM (LAGRANGE). *If H is a subgroup of G, and $|G|$ is finite, then $|H|$ divides $|G|$.*

PROOF. The left cosets are disjoint, they have the same cardinality, and their union is G. □

We introduce the notation $(G : H)$ for the number of distinct cosets of the subgroup H in the group G. The mapping $x \mapsto x^{-1}$ takes left cosets into right cosets and vice versa. It provides a bijection of the set of left cosets with the set of right cosets, so $(G : H)$ might equally well have been defined in terms of right cosets. If $|G|$ is finite, then clearly $(G : H) = |G|/|H|$.

We denote the set of left cosets by G/H. Sometimes G/H is called the *homogeneous* space defined by H. We can generalize the construction in Cayley's theorem by defining $\rho : G \to S(G/H)$ by

$$\rho(g)(kH) = (gk)H \qquad \text{for } g \in G \text{ and } kH \in G/H.$$

As usual the corresponding group action of G on G/H is defined by $g(kH) = gkH$.

Everything we just said could be done with right cosets except that the function ρ would not be a homomorphism because it would *reverse* the order of the operations. Such a function is often called an anti-homomorphism.

Let H be a subgroup of the group G. For each $g \in G$, the set gHg^{-1} is again a subgroup (the image of H under the inner automorphism induced by g.) Such a subgroup is called a *conjugate* subgroup of H. A subgroup H of G is called *normal* if every conjugate of H is contained in H. (It follows easily in that case that every conjugate $gHg^{-1} = H$.)

We indicate H is normal in G by $H \lhd G$. If $H \lhd G$, then it is easy to see that $gH = Hg$ for all $g \in G$, i.e., the left cosets are identical with the right cosets.

Every subgroup of an abelian group is normal. (However, there are non-abelian groups—e.g., the quaternion group of order eight—with the same property.)

If $H \leq G$, then we define a binary operation on the set of cosets by $(xH)(yH) = (xy)H$. One must show that this operation is well defined in the sense that the result depends only on the cosets xH and yH and not on the particular representatives x and y. (That is left to the student.) Doing the appropriate calculations shows that G/H becomes a group in this case.

If $H \leq G$, then we define $\phi : G \to G/H$ by $\phi(g) = gH$. $\phi(gk) = (gk)H = (gH)(kH)$ (by definition) so $\phi(gk) = \phi(g)\phi(k)$ and ϕ is a homomorphism. It is clearly onto, and it is called the *canonical homomorphism* of the group onto its factor group.

An important example of a factor group is $\mathbf{Z}/n\mathbf{Z}$ where n is a positive integer. This group is cyclic of order n. Previously we used this same notation for the group consisting of the integers from 0 to $n-1$ with binary operation addition modulo n. These groups are clearly isomorphic, so we *abuse notation* by denoting them with the same symbols.

The situation described in the previous paragraph is a model for any homomorphism. Namely, let $f : G \to G'$ be a homomorphism. Define the *kernel* of f by

$$\operatorname{Ker} f = \{x \in G \mid f(x) = 1\}.$$

A simple calculation shows that if $h \in \operatorname{Ker} f$, then $ghg^{-1} \in \operatorname{Ker} f$ for each $g \in G$. It follows that kernels are normal subgroups. (The kernel of the canonical epimorphism $\phi : G \to G/H$—for a normal subgroup H—is just that subgroup H.)

Define $\tilde{f} : G/(\operatorname{Ker} f) \to \operatorname{Im} f$ by

$$\tilde{f}(g \operatorname{Ker} f) = f(g).$$

We have

$$\begin{aligned} g \equiv g' \Leftrightarrow g^{-1}g' \in \operatorname{Ker} f \Leftrightarrow f(g^{-1}g') = 1 \\ \Leftrightarrow f(g)^{-1}f(g') = 1 \Leftrightarrow f(g) = f(g'). \end{aligned}$$

Hence, it follows that the definition of $\tilde{f}$ makes sense. $\tilde{f}$ is easily seen to be a homomorphism, and it is certainly onto. Also,

$$\tilde{f}(g) = \tilde{f}(g') \Rightarrow f(g) = f(g') \Rightarrow f(g)^{-1}f(g') = 1.$$

The last statement implies that $f(g^{-1}g') = 1$, i.e., $g^{-1}g' \in \operatorname{Ker} f$ or g and g' are in the same coset of $\operatorname{Ker} f$. That means that $\tilde{f}$ is in fact an isomorphism. We have proved the following theorem.

THEOREM. (First Isomorphism Theorem) *Let $f : G \to G'$ be a homomorphism of groups. Then*

$$\tilde{f} : G/(\operatorname{Ker} f) \cong \operatorname{Im} f \leq G'.$$

Any homomorphism f may be decomposed into the composition of a surjection onto $\operatorname{Im} f$ followed by the injection of $\operatorname{Im} f$ into G'. The first isomorphism theorem gives us a concrete way to handle the surjection part of the decomposition.

If you examine the proof given above of the first isomorphism theorem, you will see that for each $g' \in \operatorname{Im} f \leq G'$, the set

$$f^{-1}(g') = \{g \in G \mid f(g) = g'\}$$

is a coset of $\operatorname{Ker} f$. It follows that f is injective if and only if $\operatorname{Ker} f = \{1\}$. This usually simplifies checking that a homomorphism is a monomorphism.

We can get the usual facts about the order of an element from the first isomorphism theorem. Namely, given $x \in G$, define $f : \mathbf{Z} \to G$ by $f(k) = x^k$. The law of exponents shows that this is a homomorphism. Its image is $\langle x \rangle$ the cyclic subgroup generated by x. By an exercise,, we know that $\operatorname{Ker} f$—which is a subgroup of $\mathbf{Z}$—is of the form $n\mathbf{Z}$ for some non-negative integer n. Suppose n is positive. Since $x^k = 1$ if and only if $k \in \operatorname{Ker} f = n\mathbf{Z}$, it follows that the least positive integer with this property, i.e., the order of x, is n. If $n = 0$, then the subgroup generated by x, $\langle x \rangle$, is infinite cyclic.

Notice that we have now classified all cyclic groups. Up to isomorphism they are just the groups $\mathbf{Z}$ or $\mathbf{Z}/n\mathbf{Z}$. (Of course, these facts can be derived quite easily without the first isomorphism theorem.)

Let $f : G \to G'$ be a homomorphism, and let $K = \ker f$. We want to analyze the relationship between subgroups of G and subgroups of G'. Let H be any subgroup of G; then $f(H)$ is a subgroup of G'. On the other hand, let H' be any subgroup of G'; then $f^{-1}(H') = \{g \in G \mid f(g) \in H'\}$ is easily seen to be a subgroup of G. We have

$$f(f^{-1}(H') = H' \cap \operatorname{Im} f$$

so that all subgroups with the same intersection with $\operatorname{Im} f$ pull back to the same subgroup of G. On the other hand, we have

$$f^{-1}(f(H)) = \langle H \cup K \rangle = H \vee K.$$

For, $g \in f^{-1}(f(H)) \iff f(g) = f(h)$ with $h \in H \iff f(g^{-1}h) = 1 \iff g^{-1}h \in K \iff g \in hK$ for some $h \in H$. However, since K is normal, we have $\langle H \cup K \rangle = H \vee K = HK$ where

$$HK = \{hk \mid h \in H, k \in K\}$$

since any $h_1k_1h_2k_2 \cdots h_nk_n$ can be put in the form hk by moving the h's past the k's by conjugating and using the normality of K. Hence, $g \in hK$ for some $h \in H$ if and only if $g \in HK$ as required. HK is in fact the largest subgroup of G with image in G' equal to $f(H)$. It follows from the above analysis that there is a one-to-one correspondence between subgroups H of G containing K and subgroups H' of $\operatorname{Im} f$: $H = f^{-1}(H')$ and $h' = f(H)$. In addition, we have the following result.

THEOREM. (Third Isomorphism Theorem.) *Let $f : G \to G'$ be a surjective homomorphism. Then, there is a one-to-one correspondence between subgroups of G containing K and subgroups of G' as described above, and moreover $H = f^{-1}(H')$ is normal if and only if $H' = f(H)$ is normal. Moreover, f induces an isomorphism $G/H \cong G'/H'$.*

PROOF. It is not hard to see that $f^{-1}(H')$ is normal in general whenever H' is normal in G', and similarly, $f(H)$ is normal in $f(G)$ whenever H is normal in G. To see that $G/H \cong G'/H'$ define $f^{\#} : G/H \to G'/H'$ by $f^{\#}(gH) = f(g)H'$. It is straightforward to show that $f^{\#}$ is a homomorphism and is onto and has trivial kernel. □

Next, let $H \leq G$, consider the restriction $f_1 : H \to G'$ of f to H, and let $K = \operatorname{Ker} f$. By the first isomorphism theorem, we have

$$H/\operatorname{Ker} f_1 \cong \operatorname{Im} f_1 = f(H).$$

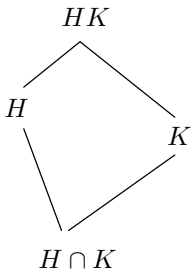
However, $\operatorname{Ker} f_1 = \{h \in H | f(h) = f_1(h) = 1\} = H \cap (\operatorname{Ker} f) = H \cap K$. Since $f(HK) = f(H)$, and since $(HK) \cap K = K$, applying the same result to HK yields $HK/K \cong f(H)$. Putting this together gives

THEOREM. (Second Isomorphism Theorem.) *Let $H \leq G$ and suppose $K \lhd G$. Then, the inclusion of H in HK yields an isomorphism*

$$H/H \cap K \cong HK/K.$$

PROOF. Apply the above reasoning to the canonical epimorphism $G \to G/K$.

The above situation is summarized in the diagram



Semi-direct products. Let G and H be groups and suppose $\rho : G \to \mathrm{Aut}(H)$ provides an action of G on H. We consider the set of all pairs (h, g) where $h \in H$ and $g \in G$, and we define a binary operation on this set by

$$(h_1, g_1)(h_2, g_2) = (h_1(g_1 h_2), g_1 g_2).$$

It is a good exercise in algebraic pencil-pushing to check that this operation satisfies the group axioms. The group defined in this way is called the semi-direct product and it is denoted $H \ltimes G$ or $G \rtimes H$.

The semi-direct product is an important construction in group theory. By far the most important case is that in which the homomorphism $\rho : G \to \mathrm{Aut}(H)$ has trivial image, i.e., $\rho(g) = id_H$ for all $g \in G$. In that case, the operation becomes

$$(h_1, g_1)(h_2, g_2) = (h_1 h_2, g_1 g_2),$$

the group is called the *direct product* and is denoted $H \times G$.

It is easy to see that $H \times G \cong G \times H$. Moreover, an associativity law

$$H_1 \times (H_2 \times H_3) \cong (H_1 \times H_2) \times H_3$$

holds. (Clearly, that may be generalized to any number of factors.)

Exercises.

1. Find up to isomorphism all groups of order 2, 3, 4, 5, 6, 7, 8, 9, and 10. (Hint: They are all either cyclic or isomorphic to a direct or semi-direct product of cyclic groups except for one group of order 8. You may use the fact that there is an element of order p for every prime p dividing the order of the group.)

2. Let $\mathbf{Q}$ denote the group of rational numbers with addition the binary operation. $\mathbf{Z}$ is a subgroup of $\mathbf{Q}$ so we may form the factor group $\mathbf{Q}/\mathbf{Z}$.

(a) Show that every element of $\mathbf{Q}/\mathbf{Z}$ is torsion.

(b) Show that for each positive integer n, $\mathbf{Q}/\mathbf{Z}$ has a unique subgroup of order n and that subgroup is cyclic.

3. Let $\xi : K \to \mathrm{Aut}(H)$ be a homomorphism, and put $G = K \rtimes H$. Define $p_K : G \to K$ by $p_K(h, k) = k$ and define $p_H : G \to H$ similarly. Show that p_K is an epimorphism. Determine conditions under which p_H is homomorphism.

4. Let G be a group and let $H \leq G$ with $(G : H)$ finite. Prove that H contains a normal subgroup of G of finite index. Do not assume G is finite.

5. Let H and K be subgroups of G with H normal in G. Suppose that $G = HK$ and $H \cap K = \{1\}$. Show that there is a homomorphism $\xi : K \to \mathrm{Aut}(H)$ and an isomorphism $G \cong K \rtimes H$.

6. Let P be a cyclic group of prime order p. Show that the automorphisms of P are in one-to-one correspondence with the integers i with $0 < i < p$ and $(i, p) = 1$. Show also that if α_i is the automorphism corresponding to i, then $\alpha_i \alpha_j = \alpha_{ij}$ where ij is read modulo p. What is the order of $\mathrm{Aut}(P)$? How does the above theory change if p is replaced by an arbitrary positive integer n?

7. Let H and K be subgroups of a group G such that $H \cap K = \{1\}$. Prove that if H and K are both normal then $hk = kh$ for all $h \in H$ and $k \in K$.

8. (a) Let H be cyclic of order 4 and let K be cyclic of order 3. Show that there is exactly one nontrivial homomorphism $\alpha : H \to \mathrm{Aut}(K)$.

(b) Let

$$H = \{1, u, v, w \mid u^2 = v^2 = w^2 = 1, uv = vu = w,\ uw = wu = v, vw = wv = u\}$$

be the Klein 4-group (isomorphic to a direct product of two cyclic groups of order 2.) Show that there are exactly three nontrivial homomorphisms $\alpha : H \to \mathrm{Aut}(K)$. Show that the semidirect products resulting from these three representations are all isomorphic

9. Assume G is a group and K is a subgroup such that every element t not in K satisfies $t^2 = 1$. Show that K is normal in G.

5. Free Groups

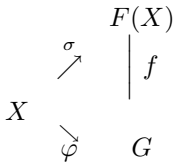
Let X be a set. Let $M(X)$ be the set of strings (or words)

$$w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_m}$$

with $\epsilon_1 = \pm 1$ and each $x_i \in X$. Usually we will omit the exponent if it is $+1$. Define an operation on $M(X)$ by concatenating strings. The operation is associative,and the empty string is an identity. Hence $M(X)$ is a monoid under this operation. It is not a group because there are no inverses. To make a group, we introduce an equivalence relation as follows. We say a string is obtained from another by *reduction* if the first string contains a substring of the form xx^{-1} or one of the form $x^{-1}x$ and the second string is obtained from the first by deleting that substring. We say that two words u and v are equivalent if there is a chain of intermediate words $u = w_0, w_1, \ldots w_n = v$ such that adjacent words are related in that one is a reduction of the other. It is clear that if u is equivalent to u' and v is equivalent to v', then uv is equivalent to $u'v'$. Hence, we may define a product on the set of equivalence classes by $[u][v] = [uv]$ (where $[u]$ denotes the equivalence class of u). This operation is also associative and the class of the empty word is an identity. If u is a word in $M(X)$, denote by u^{-1} the word with the factors written in the opposite order and with opposite exponents. Then $[u][u^{-1}] = [uu^{-1}] = [1]$. Hence, the set of equivalence classes forms a group which we denote by $F(X)$ and call the *free* group on the set X.

Define $\sigma : X \to F(X)$ by $\sigma(x) = x$ (i.e., the word with single entry x. The function σ has the following *universal mapping* property:

Given any function $\varphi : X \to G$ where G is a group, there is a unique homomorphism $f : F(X) \to G$ such that $\varphi = f \circ \sigma$.



For, it is clear that $\langle \sigma(G) \rangle = F(X)$ so that any two homomorphisms which agree on $\sigma(G)$ must be the same. On the other hand, it is also clear that we can extend φ to a function $M(X) \to G$ which preserves products and that equivalent words get carried into the same element by that extension.

PROPOSITION. *Every group is a homomorphic image of a free group.*

PROOF. Let X be any subset of G such that $G = \langle X \rangle$ (i.e., X is a subset of generators.) For example, X could be the set G itself although generally, you can take it to be much smaller. Let $\varphi : X \to G$ be the inclusion of X in G. The induced homomorphism $F : F(X) \to G$ is a surjection because its image clearly contains X, which by assumption generates. □

The above construction may be generalized as follows. Let X and X' be sets and form the free groups and inclusions $\sigma : X \to F(X)$, $\sigma' : X' \to F(X')$. Then for each set theoretic function $f : X \to X'$, there is a unique group homomorphism $F(f) : F(X) \to F(X')$ such that the diagram below "commutes."

$$\begin{array}{ccc} X & \xrightarrow{f} & X' \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma'} \\ F(X) & \xrightarrow[F(f)]{} & F(X') \end{array}$$

This fact follows by applying the previous result to the composition $\sigma' \circ f$.

The free group construction is an example of a *functor*. That is, to each set we associate a group and also to each mapping of sets we associate a group homomorphism. Moreover, it is clear that this association has natural properties. Thus, the identity function of the set X gets taken to the identity homomorphism of the group $F(X)$. Also, composition is preserved, i.e., $F(g \circ h) = F(g) \circ F(h)$ The notion of functor is extremely important in modern algebra. We shall see other examples later.

We may use the above ideas to describe groups in a convenient way. We have essentially done this already in the case of a finite cyclic group. To remind you, let $C = \langle c \rangle$, where $o(c) = n$ is finite. Let F be the free group on a single generator x. Clearly, $F \cong \mathbf{Z}$, and if we map F onto C by sending $x \mapsto c$, we simply obtain the homomorphism $\mathbf{Z} \to C$ discussed earlier. Using the new terminology, we see that the kernel is just the subgroup $R = \langle x^n \rangle$ of F. In other words, we have an isomorphism $F/R \cong C$. This is called a *presentation* of C. Sometimes we summarize this situation by writing $C = \langle c \mid c^n = 1 \rangle$.

More generally, suppose $G = \langle g_1, g_2, \ldots, g_n \rangle$. Let F be the free group on a set $\{x_1, x_2, \ldots, x_n\}$ and construct an epimorphism from F onto G by sending $x_i \mapsto g_i$. Let R be the kernel of this epimorphism. We call the isomorphism $F/R \cong G$ a presentation of G. The most interesting case is that in which we can find a reasonable set of generators for R as a subgroup of F. Each such generator is in the form of a word in the x_i which becomes 1 when g_i is substituted for x_i. In fact, we need not find a complete set of generators for R as a subgroup of F. For most purposes, it suffices to find a subset $\{r_1, r_2, \ldots, r_m\}$ of R with the property that R is the smallest *normal* subgroup of F contains that subset. (In fact, R is the subgroup generated by the elements r_i and all their conjugates by arbitrary elements of F.) The r_i are words in the generators x_i of F, and we can think of them as "monomials" in the x_i which may be "evaluated" by substituting g_i for

x_i. If we use the same symbol r_i for the word in R and the corresponding "expression" in terms of the g_i, then we may summarize the information about the presentation by writing

$$G = \langle g_1, g_2, \ldots, g_n \mid r_1 = 1, r_2 = 1, \ldots, r_m = 1 \rangle.$$

In attempting to determine groups of a given order (or with some specified structure) you will often come upon a presentation. For example, you may in one of the exercises have discovered that the non-abelian group of order 6 can be generated by two elements a and b satisfying the relations $a^3 = 1$, $b^2 = 1$, $ba = a^2b$ (or $bab^{-1}a^{-2} = 1$). Let F be the free group on generators A and B which we map onto a and b respectively thereby inducing an epimorphism of F onto G. Let R be the smallest normal subgroup of F containing the words in A and B corresponding to the relations written above. It is clear that R is contained in the kernel of the epimorphism of F onto G, but it is not at all clear that the kernel equals R. To establish that we need some further argument. One way to proceed would be as follows: Show that any epimorphic image of F/R (i.e., any group generated by two elements satisfying the given relations) has order at most 6. Since G in this case has order $= 6$, it will follow that $F/R \cong G$, i.e., we do indeed have a presentation of the given group.

The general case is similar. If you show that a group G is generated by elements satisfying certain relations, that suggests a possible presentation F/R for which you know to start only that G is an epimorphic image of F/R. To show in fact that $F/R \cong G$ requires further (often very difficult) arguments.

Given a presentation of a group, it is often necessary to determine if two words in the generators represent the same element in the original group. The *word problem* asked for a general algorithm to accomplish that. The word problem has been shown to be unsolvable, i.e., there is no such algorithm which will work for arbitrary groups, (but there are special algorithms which will work for specific classes of groups).

Exercises.

1. Show that the operation multiplication by juxtaposition on words is well defined on equivalence classes of words as described above. That is, show that if w_1 is equivalent to w_1' and w_2 is equivalent to w_2', then w_1w_2 is equivalent to $w_1'w_2'$.

2. (a) Show that the group with presentation

$$\langle a, b \mid a^4 = b^4 = 1, bab^{-1} = a^{-1} \rangle$$

has order 16.

(b) Show that the group with presentation

$$\langle a, b, c \mid a^{-1}ba = b^2, b^{-1}cb = c^2, c^{-1}ac = a^2 \rangle$$

is trivial. (This is hard!)

3. Let S be a set and define the *free monoid* $M(X)$ on X to be the set of all words of the form $x_1x_2 \ldots x_k$ where $x_1, \ldots, x_k \in X$. Denote the empty word by 1. Define multiplication in $M(X)$ by justapostion.

(a) Show that $M(X)$ is a monoid.

(b) Define the set theoretic map $i : X \to M(X)$ by $i(x) = x$ where the symbol on the left stands for a word of length 1 in $M(X)$. Formulate and prove a universal mapping property for i.