Chapter 1

Group Fundamentals

1.1 Groups and Subgroups

1.1.1 Definition

A *group* is a nonempty set G on which there is defined a binary operation $(a, b) \to ab$ satisfying the following properties.

***Closure*:** If a and b belong to G, then ab is also in G;

***Associativity*:** $a(bc) = (ab)c$ for all $a, b, c \in G$;

***Identity*:** There is an element $1 \in G$ such that $a1 = 1a = a$ for all a in G;

***Inverse*:** If a is in G, then there is an element a^{-1} in G such that $aa^{-1} = a^{-1}a = 1$.

A group G is *abelian* if the binary operation is commutative, i.e., $ab = ba$ for all a, b in G. In this case the binary operation is often written additively ($(a, b) \to a + b$), with the identity written as 0 rather than 1.

There are some very familiar examples of abelian groups under addition, namely the integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numers $\mathbb{C}$, and the integers $\mathbb{Z}_m$ modulo m. Nonabelian groups will begin to appear in the next section.

The associative law generalizes to products of any finite number of elements, for example, $(ab)(cde) = a(bcd)e$. A formal proof can be given by induction. If two people A and B form $a_1 \cdots a_n$ in different ways, the last multiplication performed by A might look like $(a_1 \cdots a_i)(a_{i+1} \cdots a_n)$, and the last multiplication by B might be $(a_1 \cdots a_j)(a_{j+1} \cdots a_n)$. But if (without loss of generality) $i < j$, then (induction hypothesis)

$$(a_1 \cdots a_j) = (a_1 \cdots a_i)(a_{i+1} \cdots a_j)$$

and

$$(a_{i+1} \cdots a_n) = (a_{i+1} \cdots a_j)(a_{j+1} \cdots a_n).$$

By the $n = 3$ case, i.e., the associative law as stated in the definition of a group, the products computed by A and B are the same.

The identity is unique ($1' = 1'1 = 1$), as is the inverse of any given element (if b and b' are inverses of a, then $b = 1b = (b'a)b = b'(ab) = b'1 = b'$). Exactly the same argument shows that if b is a right inverse, and b' a left inverse, of a, then $b = b'$.

1.1.2 Definitions and Comments

A *subgroup* H of a group G is a nonempty subset of G that forms a group under the binary operation of G. Equivalently, H is a nonempty subset of G such that if a and b belong to H, so does ab^{-1}. (Note that $1 = aa^{-1} \in H$; also, $ab = a((b^{-1})^{-1}) \in H$.)

If A is any subset of a group G, the *subgroup generated by* A is the smallest subgroup containing A, often denoted by $\langle A \rangle$. Formally, $\langle A \rangle$ is the intersection of all subgroups containing A. More explicitly, $\langle A \rangle$ consists of all finite products $a_1 \cdots a_n$, $n = 1, 2, \dots$, where for each i, either a_i or a_i^{-1} belongs to A. To see this, note that all such products belong to any subgroup containing A, and the collection of all such products forms a subgroup. In checking that the inverse of an element of $\langle A \rangle$ also belongs to $\langle A \rangle$, we use the fact that

$$(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$$

which is verified directly: $(a_1 \cdots a_n)(a_n^{-1} \cdots a_1^{-1}) = 1$.

1.1.3 Definitions and Comments

The groups G_1 and G_2 are said to be *isomorphic* if there is a bijection $f \colon G_1 \to G_2$ that preserves the group operation, in other words, $f(ab) = f(a)f(b)$. Isomorphic groups are essentially the same; they differ only notationally. Here is a simple example. A group G is *cyclic* if G is generated by a single element: $G = \langle a \rangle$. A finite cyclic group generated by a is necessarily abelian, and can be written as $\{1, a, a^2, \dots, a^{n-1}\}$ where $a^n = 1$, or in additive notation, $\{0, a, 2a, \dots, (n-1)a\}$, with $na = 0$. Thus a finite cyclic group with n elements is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n. Similarly, if G is an infinite cyclic group generated by a, then G must be abelian and can be written as $\{1, a^{\pm 1}, a^{\pm 2}, \dots\}$, or in additive notation as $\{0, \pm a, \pm 2a, \dots\}$. In this case, G is isomorphic to the additive group $\mathbb{Z}$ of all integers.

The *order* of an element a in a group G (denoted $|a|$) is the least positive integer n such that $a^n = 1$; if no such integer exists, the order of a is infinite. Thus if $|a| = n$, then the cyclic subgroup $\langle a \rangle$ generated by a has exactly n elements, and $a^k = 1$ iff k is a multiple of n. (Concrete examples are more illuminating than formal proofs here. Start with 0 in the integers modulo 4, and continually add 1; the result is $0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, \dots$.)

The *order of the group* G, denoted by $|G|$, is simply the number of elements in G.

1.1.4 Proposition

If G is a finite cyclic group of order n, then G has exactly one (necessarily cyclic) subgroup of order n/d for each positive divisor d of n, and G has no other subgroups. If G is an infinite cyclic group, the (necessarily cyclic) subgroups of G are of the form $\{1, b^{\pm 1}, b^{\pm 2}, \dots\}$, where b is an arbitrary element of G, or, in additive notation, $\{0, \pm b, \pm 2b, \dots\}$.

Proof. Again, an informal argument is helpful. Suppose that H is a subgroup of $\mathbb{Z}_{20}$ (the integers with addition modulo 20). If the smallest positive integer in H is 6 (a non-divisor of 20) then H contains $6, 12, 18, 4$ (oops, a contradiction, 6 is supposed to be the smallest positive integer). On the other hand, if the smallest positive integer in H is 4, then $H = \{4,8,12,16,0\}$. Similarly, if the smallest positive integer in a subgroup H of the additive group of integers $\mathbb{Z}$ is 5, then $H = \{0, \pm 5, \pm 10, \pm 15, \pm 20, \dots\}$. ♣

If $G = \{1, a, \dots, a^{n-1}\}$ is a cyclic group of order n, when will an element a^r also have order n? To discover the answer, let's work in $\mathbb{Z}_{12}$. Does 8 have order 12? We compute $8, 16, 24\ (= 0)$, so the order of 8 is 3. But if we try 7, we get $7, 14, 21, \dots, 77, 84 = 7 \times 12$, so 7 does have order 12. The point is that the least common multiple of 7 and 12 is simply the product, while the lcm of 8 and 12 is smaller than the product. Equivalently, the greatest common divisor of 7 and 12 is 1, while the gcd of 8 and 12 is $4 > 1$. We have the following result.

1.1.5 Proposition

If G is a cyclic group of order n generated by a, the following conditions are equivalent:

(a) $|a^r| = n$.

(b) r and n are relatively prime.

(c) r is a *unit* mod n, in other words, r has an *inverse* mod n (an integer s such that $rs \equiv 1 \bmod n$).

Furthermore, the set U_n of units mod n forms a group under multiplication. The order of this group is $\varphi(n)$ = the number of positive integers less than or equal to n that are relatively prime to n; φ is the familiar *Euler φ function*.

Proof. The equivalence of (a) and (b) follows from the discussion before the statement of the proposition, and the equivalence of (b) and (c) is handled by a similar argument. For example, since there are 12 distinct multiples of 7 mod 12, one of them must be 1; specifically, $7 \times 7 \equiv 1 \bmod 12$. But since 8×3 is 0 mod 12, no multiple of 8 can be 1 mod 12. (If $8x \equiv 1$, multiply by 3 to reach a contradiction.) Finally, U_n is a group under multiplication because the product of two integers relatively prime to n is also relatively prime to n. ♣

Problems For Section 1.1

1. A *semigroup* is a nonempty set with a binary operation satisfying closure and associativity (we drop the identity and inverse properties from the definition of a group). A *monoid* is a semigroup with identity (so that only the inverse property is dropped). Give an example of a monoid that is not a group, and an example of a semigroup that is not a monoid.
2. In $\mathbb{Z}_6$, the group of integers modulo 6, find the order of each element.
3. List all subgroups of $\mathbb{Z}_6$.

4. Let S be the set of all n by n matrices with real entries. Does S form a group under matrix addition?
5. Let S^* be the set of all nonzero n by n matrices with real entries. Does S^* form a group under matrix multiplication?
6. If H is a subgroup of the integers $\mathbb{Z}$ and $H \neq \{0\}$, what does H look like?
7. Give an example of an infinite group that has a nontrivial finite subgroup (trivial means consisting of the identity alone).
8. Let a and b belong to the group G. If $ab = ba$ and $|a| = m$, $|b| = n$, where m and n are relatively prime, show that $|ab| = mn$ and that $\langle a\rangle \cap \langle b\rangle = \{1\}$.
9. If G is a finite abelian group, show that G has an element g such that $|g|$ is the least common multiple of $\{|a|\colon a \in G\}$.
10. Show that a group G cannot be the union of two proper subgroups, in other words, if $G = H \cup K$ where H and K are subgroups of G, then $H = G$ or $K = G$. Equivalently, if H and K are subgroups of a group G, then $H \cup K$ cannot be a subgroup unless $H \subseteq K$ or $K \subseteq H$.
11. In an arbitrary group, let a have finite order n, and let k be a positive integer. If (n, k) is the greatest common divisor of n and k, and $[n, k]$ the least common multiple, show that the order of a^k is $n/(n, k) = [n, k]/k$.
12. Suppose that the prime factorization of the positive integer n is

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

and let A_i be the set of all positive integers $m \in \{1, 2, \dots, n\}$ such that p_i divides m. Show that if $|S|$ is the number of elements in the set S, then

$$\begin{aligned}
|A_i| &= \frac{n}{p_i}, \\
|A_i \cap A_j| &= \frac{n}{p_i p_j} \quad \text{for } i \neq j, \\
|A_i \cap A_j \cap A_k| &= \frac{n}{p_i p_j p_k} \quad \text{for } i, j, k \text{ distinct},
\end{aligned}$$

and so on.
13. Continuing Problem 12, show that the number of positive integers less than or equal to n that are relatively prime to n is

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r}).$$

14. Give an example of a finite group G (of order at least 3) with the property that the only subgroups of G are $\{1\}$ and G itself.
15. Does an infinite group with the property of Problem 14 exist?

1.2 Permutation Groups

1.2.1 Definition

A *permutation* of a set S is a bijection on S, that is, a function $\pi\colon S \to S$ that is one-to-one and onto. (If S is finite, then π is one-to-one if and only if it is onto.) If S is not too large, it is feasible to describe a permutation by listing the elements $x \in S$ and the corresponding values $\pi(x)$. For example, if $S = \{1, 2, 3, 4, 5\}$, then

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{bmatrix}$$

is the permutation such that $\pi(1) = 3$, $\pi(2) = 5$, $\pi(3) = 4$, $\pi(4) = 1$, $\pi(5) = 2$. If we start with any element $x \in S$ and apply π repeatedly to obtain $\pi(x), \pi(\pi(x))$, $\pi(\pi(\pi(x)))$, and so on, eventually we must return to x, and there are no repetitions along the way because π is one-to-one. For the above example, we obtain $1 \to 3 \to 4 \to 1$, $2 \to 5 \to 2$. We express this result by writing

$$\pi = (1, 3, 4)(2, 5)$$

where the *cycle* $(1, 3, 4)$ is the permutation of S that maps 1 to 3, 3 to 4 and 4 to 1, leaving the remaining elements 2 and 5 fixed. Similarly, $(2, 5)$ maps 2 to 5, 5 to 2, 1 to 1, 3 to 3 and 4 to 4. The product of $(1, 3, 4)$ and $(2, 5)$ is interpreted as a composition, with the right factor $(2, 5)$ applied first, as with composition of functions. In this case, the cycles are disjoint, so it makes no difference which mapping is applied first.

The above analysis illustrates the fact that *any permutation can be expressed as a product of disjoint cycles, and the cycle decomposition is unique.*

1.2.2 Definitions and Comments

A permutation π is said to be *even* if its cycle decomposition contains an even number of even cycles (that is, cycles of even length); otherwise π is *odd.* A cycle can be decomposed further into a product of (not necessarily disjoint) two-element cycles, called *transpositions.* For example,

$$(1, 2, 3, 4, 5) = (1, 5)(1, 4)(1, 3)(1, 2)$$

where the order of application of the mappings is from right to left.

Multiplication by a transposition changes the parity of a permutation (from even to odd, or vice versa). For example,

$$\begin{aligned} (2, 4)(1, 2, 3, 4, 5) &= (2, 3)(1, 4, 5) \\ (2, 6)(1, 2, 3, 4, 5) &= (1, 6, 2, 3, 4, 5); \end{aligned}$$

$(1, 2, 3, 4, 5)$ has no cycles of even length, so is even; $(2, 3)(1, 4, 5)$ and $(1, 6, 2, 3, 4, 5)$ each have one cycle of even length, so are odd.

Since a cycle of even length can be expressed as the product of an odd number of transpositions, we can build an even permutation using an even number of transpositions, and an odd permutation requires an odd number of transpositions. A decomposition into transpositions is not unique; for example, $(1,2,3,4,5) = (1,4)(1,5)(1,4)(1,3)(1,2)(3,5)$, but as mentioned above, the cycle decomposition is unique. Since multiplication by a transposition changes the parity, it follows that if a permutation is expressed in two different ways as a product of transpositions, the number of transpositions will agree in parity (both even or both odd).

Consequently, *the product of two even permutations is even; the product of two odd permutations is even*; and *the product of an even and an odd permutation is odd.* To summarize very compactly, define the *sign* of the permutation π as

$$\operatorname{sgn}(\pi) = \begin{cases} +1 & \text{if } \pi \text{ is even} \\ -1 & \text{if } \pi \text{ is odd} \end{cases}$$

Then for arbitrary permutations π_1 and π_2 we have

$$\operatorname{sgn}(\pi_1\pi_2) = \operatorname{sgn}(\pi_1)\operatorname{sgn}(\pi_2).$$

1.2.3 Definitions and Comments

There are several permutation groups that are of major interest. The set S_n of *all* permutations of $\{1,2,\dots,n\}$ is called the *symmetric group on n letters*, and its subgroup A_n of all *even* permutations of $\{1,2,\dots,n\}$ is called the *alternating group on n letters.* (The group operation is composition of functions.) Since there are as many even permutations as odd ones (any transposition, when applied to the members of S_n, produces a one-to-one correspondence between even and odd permutations), it follows that A_n is half the size of S_n. Denoting the size of the set S by $|S|$, we have

$$|S_n| = n!, \quad |A_n| = \tfrac{1}{2}n!$$

We now define and discuss informally D_{2n}, the *dihedral group of order 2n.* Consider a regular polygon with center O and vertices $V_1, V_2, \dots, V_n$, arranged so that as we move counterclockwise around the figure, we encounter $V_1, V_2, \dots$ in turn. To eliminate some of the abstraction, let's work with a regular pentagon with vertices A, B, C, D, E, as shown in Figure 1.2.1.

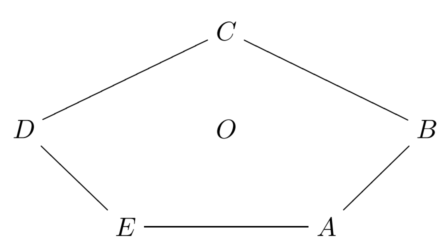

Figure 1.2.1

The group D_{10} consists of the *symmetries* of the pentagon, i.e., those permutations that can be realized via a rigid motion (a combination of rotations and reflections). All symmetries can be generated by two basic operations R and F:

R is counterclockwise rotation by $\frac{360}{n} = \frac{360}{5} = 72$ degrees,

F ("flip") is reflection about the line joining the center O to the first vertex (A in this case).

The group D_{2n} contains $2n$ elements, namely, I (the identity), $R, R^2, \ldots, R^{n-1}$, F, RF, R^2F, $\ldots$, $R^{n-1}F$ (RF means F followed by R). For example, in the case of the pentagon, $F = (B, E)(C, D)$ and $R = (A, B, C, D, E)$, so $RF = (A, B)(C, E)$, which is the reflection about the line joining O to D; note that RF can also be expressed as FR^{-1}. In visualizing the effect of a permutation such as F, interpret F's taking B to E as vertex B moving to where vertex E was previously.

D_{2n} will contain exactly n rotations $I, R, \ldots, R^{n-1}$ and n reflections $F, RF, \ldots, R^{n-1}F$. If n is odd, each reflection is determined by a line joining the center to a vertex (and passing through the midpoint of the opposite side). If n is even, half the reflections are determined by a line passing through two vertices (as well as the center), and the other half by a line passing through the midpoints of two opposite sides (as well as the center).

1.2.4 An Abstract Characterization of the Dihedral Group

Consider the *free group with generators R and F*, in other words all finite sequences whose components are R, R^{-1}, F and F^{-1}. The group operation is concatenation, subject to the constraint that if a symbol and its inverse occur consecutively, they may be cancelled. For example, $RFFFF^{-1}RFR^{-1}RFF$ is identified with $RFFRFFF$, also written as RF^2RF^3. If we add further restrictions (so the group is no longer "free"), we can obtain D_{2n}. Specifically, D_{2n} is the group defined by *generators* R and F, subject to the *relations*

$$R^n = I, \quad F^2 = I, \quad RF = FR^{-1}.$$

The relations guarantee that there are only $2n$ distinct group elements $I, R, \ldots, R^{n-1}$ and $F, RF, \ldots, R^{n-1}F$. For example, with $n = 5$ we have

$$F^2R^2F = FFRRF = FFRFR^{-1} = FFFR^{-1}R^{-1} = FR^{-2} = FR^3;$$

also, R cannot be the same as R^2F, since this would imply that $I = RF$, or $F = R^{-1} = R^4$, and there is no way to get this using the relations. Since the product of two group elements is completely determined by the defining relations, it follows that there cannot be more than one group with the given generators and relations. (This statement is true "up to isomorphism"; it is always possible to create lots of isomorphic copies of any given group.) The symmetries of the regular n-gon provide a concrete realization.

Later we will look at more systematic methods of analyzing groups defined by generators and relations.

Problems For Section 1.2

1. Find the cycle decomposition of the permutation

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 1 & 2 & 5 \end{bmatrix}$$

and determine whether the permutation is even or odd.

2. Consider the dihedral group D_8 as a group of permutations of the square. Assume that as we move counterclockwise around the square, we encounter the vertices A, B, C, D in turn. List all the elements of D_8.
3. In S_5, how many 5-cycles are there; that is, how many permutations are there with the same cycle structure as $(1, 2, 3, 4, 5)$?
4. In S_5, how many permutations are products of two disjoint transpositions, such as $(1, 2)(3, 4)$?
5. Show that if $n \geq 3$, then S_n is not abelian.
6. Show that the products of two disjoint transpositions in S_4, together with the identity, form an abelian subgroup V of S_4. Describe the multiplication table of V (known as the *four group*).
7. Show that the cycle structure of the inverse of a permutation π coincides with that of π. In particular, the inverse of an even permutation is even (and the inverse of an odd permutation is odd), so that A_n is actually a group.
8. Find the number of 3-cycles, i.e., permutations consisting of exactly one cycle of length 3, in S_4.
9. Suppose H is a subgroup of A_4 with the property that for every permutation π in A_4, π^2 belongs to H. Show that H contains all 3-cycles in A_4. (Since 3-cycles are even, H in fact contains all 3-cycles in S_4.)
10. Consider the permutation

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{bmatrix}.$$

    Count the number of *inversions* of π, that is, the number of pairs of integers that are out of their natural order in the second row of π. For example, 2 and 5 are in natural order, but 4 and 3 are not. Compare your result with the parity of π.
11. Show that the parity of any permutation π is the same as the parity of the number of inversions of π.

1.3 Cosets, Normal Subgroups, and Homomorphisms

1.3.1 Definitions and Comments

Let H be a subgroup of the group G. If $g \in G$, the *right coset* of H generated by g is

$$Hg = \{hg \colon h \in H\};$$

similarly, the *left coset* of H generated by g is

$$gH = \{gh \colon h \in H\}.$$

It follows (Problem 1) that if $a, b \in G$, then

$$Ha = Hb \quad \text{if and only if} \quad ab^{-1} \in H$$

and

$$aH = bH \quad \text{if and only if} \quad a^{-1}b \in H.$$

Thus if we define a and b to be equivalent iff $ab^{-1} \in H$, we have an equivalence relation (Problem 2), and (Problem 3) the equivalence class of a is

$$\{b\colon ab^{-1} \in H\} = Ha.$$

Therefore *the right cosets partition* G (*similarly for the left cosets*). Since $h \to ha$, $h \in H$, is a one-to-one correspondence, each coset has $|H|$ elements. There are as many right cosets as left cosets, since the map $aH \to Ha^{-1}$ is a one-to-one correspondence (Problem 4). If $[G : H]$, the *index* of H in G, denotes the number of right (or left) cosets, we have the following basic result.

1.3.2 Lagrange's Theorem

If H is a subgroup of G, then $|G| = |H|[G : H]$. In particular, if G is finite then $|H|$ divides $|G|$, and

$$\frac{|G|}{|H|} = [G : H].$$

Proof. There are $[G : H]$ cosets, each with $|H|$ members. ♣

1.3.3 Corollary

Let G be a finite group.

(i) If $a \in G$ then $|a|$ divides $|G|$; in particular, $a^{|G|} = 1$. Thus $|G|$ is a multiple of the order of each of its elements, so if we define the *exponent* of G to be the least common multiple of $\{|a|\colon a \in G\}$, then $|G|$ is a multiple of the exponent.

(ii) If G has prime order, then G is cyclic.

Proof. If the element $a \in G$ has order n, then $H = \{1, a, a^2, \dots, a^{n-1}\}$ is a cyclic subgroup of G with $|H| = n$. By Lagrange's theorem, n divides $|G|$, proving (i). If $|G|$ is prime then we may take $a \neq 1$, and consequently $n = |G|$. Thus H is a subgroup with as many elements as G, so in fact H and G coincide, proving (ii). ♣

Here is another corollary.

1.3.4 Euler's Theorem

If a and n are relatively prime positive integers, with $n \geq 2$, then $a^{\varphi(n)} \equiv 1 \mod n$. A special case is *Fermat's Little Theorem*: If p is a prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$.

Proof. The group of units mod n has order $\varphi(n)$, and the result follows from (1.3.3). ♣

We will often use the notation $H \leq G$ to indicate that H is a subgroup of G. If H is a proper subgroup, i.e., $H \leq G$ but $H \neq G$, we write $H < G$.

1.3.5 The Index is Multiplicative

If $K \leq H \leq G$, then $[G:K] = [G:H][H:K]$.

Proof. Choose representatives a_i from each left coset of H in G, and representatives b_j from each left coset of K in H. If cK is any left coset of K in G, then $c \in a_iH$ for some unique i, and if $c = a_ih, h \in H$, then $h \in b_jK$ for some unique j, so that c belongs to a_ib_jK. The map $(a_i, b_j) \to a_ib_jK$ is therefore onto, and it is one-to-one by the uniqueness of i and j. We therefore have a bijection between a set of size $[G:H][H:K]$ and a set of size $[G:K]$, as asserted. ♣

Now suppose that H and K are subgroups of G, and define HK to be the set of all products $hk, h \in H, k \in K$. Note that HK need not be a group, since $h_1k_1h_2k_2$ is not necessarily equal to $h_1h_2k_1k_2$. If G is abelian, then HK will be a group, and we have the following useful generalization of this observation.

1.3.6 Proposition

If $H \leq G$ and $K \leq G$, then $HK \leq G$ if and only if $HK = KH$. In this case, HK is the subgroup generated by $H \cup K$.

Proof. If HK is a subgroup, then $(HK)^{-1}$, the collection of all inverses of elements of HK, must coincide with HK. But $(HK)^{-1} = K^{-1}H^{-1} = KH$. Conversely, if $HK = KH$, then the inverse of an element in HK also belongs to HK, because $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$. The product of two elements in HK belongs to HK, because $(HK)(HK) = HKHK = HHKK = HK$. The last statement follows from the observation that any subgroup containing H and K must contain HK. ♣

The set product HK defined above suggests a multiplication operation on cosets. If H is a subgroup of G, we can multiply aH and bH, and it is natural to hope that we get abH. This does not always happen, but here is one possible criterion.

1.3.7 Lemma

If $H \leq G$, then $(aH)(bH) = abH$ for all $a, b \in G$ iff $cHc^{-1} = H$ for all $c \in G$. (Equivalently, $cH = Hc$ for all $c \in G$.

Proof. If the second condition is satisfied, then $(aH)(bH) = a(Hb)H = abHH = abH$. Conversely, if the first condition holds, then $cHc^{-1} \subseteq cHc^{-1}H$ since $1 \in H$, and $(cH)(c^{-1}H) = cc^{-1}H(= H)$ by hypothesis. Thus $cHc^{-1} \subseteq H$, which implies that $H \subseteq c^{-1}Hc$. Since this holds for all $c \in G$, we have $H \subseteq cHc^{-1}$, and the result follows. ♣

Notice that we have proved that if $cHc^{-1} \subseteq H$ for all $c \in G$, then in fact $cHc^{-1} = H$ for all $c \in G$.

1.3.8 Definition

Let H be a subgroup of G. If any of the following equivalent conditions holds, we say that H is a *normal subgroup* of G, or that H is *normal* in G:

(1) $cHc^{-1} \subseteq H$ for all $c \in G$ (equivalently, $c^{-1}Hc \subseteq H$ for all $c \in G$).

(2) $cHc^{-1} = H$ for all $c \in G$ (equivalently, $c^{-1}Hc = H$ for all $c \in G$).

(3) $cH = Hc$ for all $c \in G$.

(4) Every left coset of H in G is also a right coset.

(5) Every right coset of H in G is also a left coset.

We have established the equivalence of (1), (2) and (3) above, and (3) immediately implies (4). To show that (4) implies (3), suppose that $cH = Hd$. Then since c belongs to both cH and Hc, i.e., to both Hd and Hc, we must have $Hd = Hc$ because right cosets partition G, so that any two right cosets must be either disjoint or identical. The equivalence of (5) is proved by a symmetrical argument.

Notation: $H \trianglelefteq G$ indicates that H is a normal subgroup of G; if H is a proper normal subgroup, we write $H \triangleleft G$.

1.3.9 Definition of the Quotient Group

If H is normal in G, we may define a group multiplication on cosets, as follows. If aH and bH are (left) cosets, let

$$(aH)(bH) = abH;$$

by (1.3.7), $(aH)(bH)$ is simply the set product. If a_1 is another member of aH and b_1 another member of bH, then $a_1H = aH$ and $b_1H = bH$ (Problem 5). Therefore the set product of a_1H and b_1H is also abH. The point is that the product of two cosets does not depend on which representatives we select.

To verify that cosets form a group under the above multiplication, we consider the four defining requirements.

***Closure*:** The product of two cosets is a coset.

***Associativity*:** This follows because multiplication in G is associative.

***Identity*:** The coset $1H = H$ serves as the identity.

***Inverse*:** The inverse of aH is $a^{-1}H$.

The group of cosets of a normal subgroup N of G is called the *quotient group* of G by N; it is denoted by G/N.

Since the identity in G/N is $1N = N$, we have, intuitively, "set everything in N equal to 1".

1.3.10 Example

Let $GL(n, \mathbb{R})$ be the set of all nonsingular n by n matrices with real coefficients, and let $SL(n, \mathbb{R})$ be the subgroup formed by matrices whose determinant is 1 (GL stands for "general linear" and SL for "special linear"). Then $SL(n, \mathbb{R}) \triangleleft GL(n, R)$, because if A is a nonsingular n by n matrix and B is n by n with determinant 1, then $\det(ABA^{-1}) = \det A \det B \det A^{-1} = \det B = 1$.

1.3.11 Definition

If $f\colon G \to H$, where G and H are groups, then f is said to be a *homomorphism* if for all a, b in G, we have

$$f(ab) = f(a)f(b).$$

This idea will look familiar if G and H are abelian, in which case, using additive notation, we write

$$f(a + b) = f(a) + f(b);$$

thus a linear transformation on a vector space is, in particular, a homomorphism on the underlying abelian group. If f is a homomorphism from G to H, it must map the identity of G to the identity of H, since $f(a) = f(a1_G) = f(a)f(1_G)$; multiply by $f(a)^{-1}$ to get $1_H = f(1_G)$. Furthermore, the inverse of $f(a)$ is $f(a^{-1})$, because

$$1 = f(aa^{-1}) = f(a)f(a^{-1}),$$

so that $[f(a)]^{-1} = f(a^{-1})$.

1.3.12 The Connection Between Homomorphisms and Normal Subgroups

If $f\colon G \to H$ is a homomorphism, define the *kernel* of f as

$$\ker f = \{a \in G\colon f(a) = 1\};$$

then $\ker f$ is a normal subgroup of G. For if $a \in G$ and $b \in \ker f$, we must show that aba^{-1} belongs to $\ker f$. But $f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)(1)f(a)^{-1} = 1$.

Conversely, every normal subgroup is the kernel of a homomorphism. To see this, suppose that $N \trianglelefteq G$, and let H be the quotient group G/N. Define the map $\pi\colon G \to G/N$ by $\pi(a) = aN$; π is called the *natural* or *canonical* map. Since

$$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b),$$

π is a homomorphism. The kernel of π is the set of all $a \in G$ such that $aN = N (= 1N)$, or equivalently, $a \in N$. Thus $\ker \pi = N$.

1.3.13 Proposition

A homomorphism f is injective if and only if its kernel K is trivial, that is, consists only of the identity.

Proof. If f is injective and $a \in K$, then $f(a) = 1 = f(1)$, hence $a = 1$. Conversely, if K is trivial and $f(a) = f(b)$, then $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = f(a)[f(a)]^{-1} = 1$, so $ab^{-1} \in K$. Thus $ab^{-1} = 1$, i.e., $a = b$, proving f injective. ♣

1.3.14 Some Standard Terminology

A *monomorphism* is an injective homomorphism

An *epimorphism* is a surjective homomorphism

An *isomorphism* is a bijective homomorphism

An *endomorphism* is a homomorphism of a group to itself

An *automorphism* is an isomorphism of a group with itself

We close the section with a result that is applied frequently.

1.3.15 Proposition

Let $f\colon G \to H$ be a homomorphism.

(i) If K is a subgroup of G, then $f(K)$ is a subgroup of H. If f is an epimorphism and K is normal, then $f(K)$ is also normal.

(ii) If K is a subgroup of H, then $f^{-1}(K)$ is a subgroup of G. If K is normal, so is $f^{-1}(K)$.

Proof. (i) If $f(a)$ and $f(b)$ belong to $f(K)$, so does $f(a)f(b)^{-1}$, since this element coincides with $f(ab^{-1})$. If K is normal and $c \in G$, we have $f(c)f(K)f(c)^{-1} = f(cKc^{-1}) = f(K)$, so if f is surjective, then $f(K)$ is normal.

(ii) If a and b belong to $f^{-1}(K)$, so does ab^{-1}, because $f(ab^{-1}) = f(a)f(b)^{-1}$, which belongs to K. If $c \in G$ and $a \in f^{-1}(K)$ then $f(cac^{-1}) = f(c)f(a)f(c)^{-1}$, so if K is normal, we have $cac^{-1} \in f^{-1}(K)$, proving $f^{-1}(K)$ normal. ♣

Problems For Section 1.3

In Problems 1–6, H is a subgroup of the group G, and a and b are elements of G.

1. Show that $Ha = Hb$ iff $ab^{-1} \in H$.
2. Show that "$a \sim b$ iff $ab^{-1} \in H$" defines an equivalence relation.
3. If we define a and b to be equivalent iff $ab^{-1} \in H$, show that the equivalence class of a is Ha.
4. Show that $aH \to Ha^{-1}$ is a one-to-one correspondence between left and right cosets of H.

5. If aH is a left coset of H in G and $a_1 \in aH$, show that the left coset of H generated by a_1 (i.e., a_1H), is also aH.
6. If $[G : H] = 2$, show that H is a normal subgroup of G.
7. Let S_3 be the group of all permutations of $\{1, 2, 3\}$, and take a to be permutation $(1, 2, 3)$, b the permutation $(1, 2)$, and e the identity permutation. Show that the elements of S_3 are, explicitly, e, a, a^2, b, ab and a^2b.
8. Let H be the subgroup of S_3 consisting of the identity e and the permutation $b = (1, 2)$. Compute the left cosets and the right cosets of H in S_3.
9. Continuing Problem 8, show that H is not a normal subgroup of S_3.
10. Let f be an endomorphism of the integers $\mathbb{Z}$. Show that f is completely determined by its action on 1. If $f(1) = r$, then f is multiplication by r; in other words, $f(n) = rn$ for every integer n.
11. If f is an automorphism of $\mathbb{Z}$, and I is the identity function on $\mathbb{Z}$, show that f is either I or $-I$.
12. Since the composition of two automorphisms is an automorphism, and the inverse of an automorphism is an automorphism, it follows that the set of automorphisms of a group is a group under composition. In view of Problem 11, give a simple description of the group of automorphisms of $\mathbb{Z}$.
13. Let H and K be subgroups of the group G. If $x, y \in G$, define $x \sim y$ iff x can be written as hyk for some $h \in H$ and $k \in K$. Show that $\sim$ is an equivalence relation.
14. The equivalence class of $x \in G$ is $HxK = \{hxk \colon h \in H, k \in K\}$, called a *double coset* associated with the subgroups H and K. Thus the double cosets partition G. Show that any double coset can be written as a union of right cosets of H, or equally well as a union of left cosets of K.

1.4 The Isomorphism Theorems

Suppose that N is a normal subgroup of G, f is a homomorphism from G to H, and π is the natural map from G to G/N, as pictured in Figure 1.4.1.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd}$$

Figure 1.4.1

We would like to find a homomorphism $\overline{f} \colon G/N \to H$ that makes the diagram *commutative*. Commutativity means that we get the same result by traveling directly from G to H via f as we do by taking the roundabout route via π followed by $\overline{f}$. This requirement translates to $\overline{f}(aN) = f(a)$. Here is the key result for finding such an $\overline{f}$.

1.4.1 Factor Theorem

Any homomorphism f whose kernel K contains N can be factored through G/N. In other words, in Figure 1.4.1 there is a unique homomorphism $\overline{f}\colon G/N \to H$ such that $\overline{f} \circ \pi = f$. Furthermore:

(i) $\overline{f}$ is an epimorphism if and only if f is an epimorphism;

(ii) $\overline{f}$ is a monomorphism if and only if $K = N$;

(iii) $\overline{f}$ is an isomorphism if and only if f is an epimorphism and $K = N$.

Proof. If the diagram is to commute, then $\overline{f}(aN)$ must be $f(a)$, and it follows that $\overline{f}$, if it exists, is unique. The definition of $\overline{f}$ that we have just given makes sense, because if $aN = bN$, then $a^{-1}b \in N \subseteq K$, so $f(a^{-1}b) = 1$, and therefore $f(a) = f(b)$. Since

$$\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN),$$

$\overline{f}$ is a homomorphism. By construction, $\overline{f}$ has the same image as f, proving (i). Now the kernel of $\overline{f}$ is

$$\{aN\colon f(a) = 1\} = \{aN\colon a \in K\} = K/N.$$

By (1.3.13), a homomorphism is injective, i.e., a monomorphism, if and only if its kernel is trivial. Thus $\overline{f}$ is a monomorphism if and only if K/N consists only of the identity element N. This means that if a is any element of K, then the coset aN coincides with N, which forces a to belong to N. Thus $\overline{f}$ is a monomorphism if and only if $K = N$, proving (ii). Finally, (iii) follows immediately from (i) and (ii). ♣

The factor theorem yields a fundamental result.

1.4.2 First Isomorphism Theorem

If $f\colon G \to H$ is a homomorphism with kernel K, then the image of f is isomorphic to G/K.

Proof. Apply the factor theorem with $N = K$, and note that f must be an epimorphism of G onto its image. ♣

If we are studying a subgroup K of a group G, or perhaps the quotient group G/K, we might try to construct a homomorphism f whose kernel is K and whose image H has desirable properties. The first isomorphism theorem then gives $G/K \cong H$ (where $\cong$ is our symbol for isomorphism). If we know something about H, we may get some insight into K and G/K.

We will prove several other isomorphism theorems after the following preliminary result.

1.4.3 Lemma

Let H and N be subgroups of G, with N normal in G. Then:

(i) $HN = NH$, and therefore by (1.3.6), HN is a subgroup of G.

(ii) N is a normal subgroup of HN.

(iii) $H \cap N$ is a normal subgroup of H.

Proof. (i) We have $hN = Nh$ for every $h \in G$, in particular for every $h \in H$.

(ii) Since N is normal in G, it must be normal in the subgroup HN.

(iii) $H \cap N$ is the kernel of the canonical map $\pi\colon G \to G/N$, restricted to H. ♣

The subgroups we are discussing are related by a "parallelogram" or "diamond", as Figure 1.4.2 suggests.

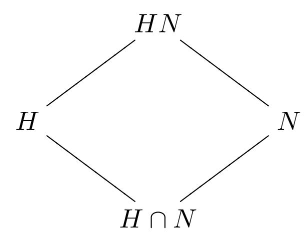

Figure 1.4.2

1.4.4 Second Isomorphism Theorem

If H and N are subgroups of G, with N normal in G, then

$$H/(H \cap N) \cong HN/N.$$

Note that we write HN/N rather than H/N, since N need not be a subgroup of H.

Proof. Let π be the canonical epimorphism from G to G/N, and let π_0 be the restriction of π to H. Then the kernel of π_0 is $H \cap N$, so by the first isomorphism theorem, $H/(H \cap N)$ is isomorphic to the image of π_0, which is $\{hN : h \in H\} = HN/N$. (To justify the last equality, note that for any $n \in N$ we have $hnN = hN$). ♣

1.4.5 Third Isomorphism Theorem

If N and H are normal subgroups of G, with N contained in H, then

$$G/H \cong (G/N)/(H/N),$$

a "cancellation law".

Proof. This will follow directly from the first isomorphism theorem if we can find an epimorphism of G/N onto G/H with kernel H/N, and there is a natural candidate: $f(aN) = aH$. To check that f is well-defined, note that if $aN = bN$ then $a^{-1}b \in N \subseteq H$, so $aH = bH$. Since a is an arbitrary element of G, f is surjective, and by definition of coset multiplication, f is a homomorphism. But the kernel of f is

$$\{aN \colon aH = H\} = \{aN \colon a \in H\} = H/N. \quad \clubsuit$$

Now suppose that N is a normal subgroup of G. If H is a subgroup of G containing N, there is a natural analog of H in the quotient group G/N, namely, the subgroup H/N. In fact we can make this correspondence very precise. Let

$$\psi(H) = H/N$$

be a map from the set of subgroups of G containing N to the set of subgroups of G/N. We claim that ψ is a bijection. For if $H_1/N = H_2/N$ then for any $h_1 \in H_1$, we have $h_1N = h_2N$ for some $h_2 \in H_2$, so that $h_2^{-1}h_1 \in N$, which is contained in H_2. Thus $H_1 \subseteq H_2$, and by symmetry the reverse inclusion holds, so that $H_1 = H_2$ and ψ is injective. Now if Q is a subgroup of G/N and $\pi \colon G \to G/N$ is canonical, then

$$\pi^{-1}(Q) = \{a \in G \colon aN \in Q\},$$

a subgroup of G containing N, and

$$\psi(\pi^{-1}(Q)) = \{aN \colon aN \in Q\} = Q,$$

proving ψ surjective.

The map ψ has a number of other interesting properties, summarized in the following result, sometimes referred to as the fourth isomorphism theorem.

1.4.6 Correspondence Theorem

If N is a normal subgroup of G, then the map $\psi \colon H \to H/N$ sets up a one-to-one correspondence between subgroups of G containing N and subgroups of G/N. The inverse of ψ is the map $\tau \colon Q \to \pi^{-1}(Q)$, where π is the canonical epimorphism of G onto G/N. Furthermore:

(i) $H_1 \leq H_2$ if and only if $H_1/N \leq H_2/N$, and, in this case,

$$[H_2 \colon H_1] = [H_2/N \colon H_1/N].$$

(ii) H is a normal subgroup of G if and only if H/N is a normal subgroup of G/N.

More generally,

(iii) H_1 is a normal subgroup of H_2 if and only if H_1/N is a normal subgroup of H_2/N, and in this case, $H_2/H_1 \cong (H_2/N)/H_1/N)$.

Proof. We have established that ψ is a bijection with inverse τ. If $H_1 \leq H_2$, we have $H_1/N \leq H_2/N$ immediately, and the converse follows from the above proof that ψ is injective. To prove the last statement of (i), let η map the left coset $aH_1, a \in H_2$, to the left coset $(aN)(H_1/N)$. Then η is a well-defined injective map because

$$\begin{aligned} aH_1 = bH_1 \quad &\text{iff} \quad a^{-1}b \in H_1 \\ &\text{iff} \quad (aN)^{-1}(bN) = a^{-1}bN \in H_1/N \\ &\text{iff} \quad (aN)(H_1/N) = (bN)(H_1/N); \end{aligned}$$

η is surjective because a ranges over all of H_2.

To prove (ii), assume that $H \trianglelefteq G$; then for any $a \in G$ we have

$$(aN)(H/N)(aN)^{-1} = (aHa^{-1})/N = H/N$$

so that $H/N \trianglelefteq G/N$. Conversely, suppose that H/N is normal in G/N. Consider the homomorphism $a \to (aN)(H/N)$, the composition of the canonical map of G onto G/N and the canonical map of G/N onto $(G/N)/(H/N)$. The element a will belong to the kernel of this map if and only if $(aN)(H/N) = H/N$, which happens if and only if $aN \in H/N$, that is, $aN = hN$ for some $h \in H$. But since N is contained in H, this statement is equivalent to $a \in H$. Thus H is the kernel of a homomorphism, and is therefore a normal subgroup of G.

Finally, the proof of (ii) also establishes the first part of (iii); just replace H by H_1 and G by H_2. The second part of (iii) follows from the third isomorphism theorem (with the same replacement). ♣

We conclude the section with a useful technical result.

1.4.7 Proposition

If H is a subgroup of G and N is a normal subgroup of G, we know by (1.4.3) that HN, the subgroup generated by $H \cup N$, is a subgroup of G. If H is also a normal subgroup of G, then HN is normal in G as well. More generally, if for each i in the index set I, we have $H_i \trianglelefteq G$, then $\langle H_i, i \in I\rangle$, the subgroup generated by the H_i (technically, by the set $\cup_{i\in I} H_i$) is a normal subgroup of G.

Proof. A typical element in the subgroup generated by the H_i is $a = a_1 a_2 \cdots a_n$ where a_k belongs to H_{i_k}. If $g \in G$ then

$$g(a_1 a_2 \cdots a_n)g^{-1} = (ga_1g^{-1})(ga_2g^{-1}) \cdots (ga_ng^{-1})$$

and $ga_kg^{-1} \in H_{i_k}$ because $H_{i_k} \trianglelefteq G$. Thus gag^{-1} belongs to $\langle H_i, i \in I\rangle$. ♣

Problems For Section 1.4

1. Let $\mathbb{Z}$ be the integers, and $n\mathbb{Z}$ the set of integer multiples of n. Show that $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$, the additive group of integers modulo n. (This is not quite a tautology if we view $\mathbb{Z}_n$ concretely as the set $\{0, 1, \ldots, n-1\}$, with sums and differences reduced modulo n.)

2. If m divides n then $\mathbb{Z}_m \le \mathbb{Z}_n$; for example, we can identify $\mathbb{Z}_4$ with the subgroup $\{0, 3, 6, 9\}$ of $\mathbb{Z}_{12}$. Show that $\mathbb{Z}_n/\mathbb{Z}_m \cong \mathbb{Z}_{n/m}$.
3. Let a be an element of the group G, and let $f_a\colon G \to G$ be "conjugation by a", that is, $f_a(x) = axa^{-1}, x \in G$. Show that f_a is an automorphism of G.
4. An *inner automorphism* of G is an automorphism of the form f_a (defined in Problem 3) for some $a \in G$. Show that the inner automorphisms of G form a group under composition of functions (a subgroup of the group of all automorphisms of G).
5. Let $Z(G)$ be the *center* of G, that is, the set of all x in G such that $xy = yx$ for all y in G. Thus $Z(G)$ is the set of elements that commute with everything in G. Show that $Z(G)$ is a normal subgroup of G, and that the group of inner automorphisms of G is isomorphic to $G/Z(G)$.
6. If f is an automorphism of Z_n, show that f is multiplication by m for some m relatively prime to n. Conclude that the group of automorphisms of $\mathbb{Z}_n$ can be identified with the group of units mod n.
7. The diamond diagram associated with the second isomorphism theorem (1.4.4) illustrates least upper bounds and greatest lower bounds in a lattice. Verify that HN is the smallest subgroup of G containing both H and N, and $H \cap N$ is the largest subgroup of G contained in both H and N.
8. Let g be an automorphism of the group G, and f_a an inner automorphism, as defined in Problems 3 and 4. Show that $g \circ f_a \circ g^{-1}$ is an inner automorphism. Thus the group of inner automorphisms of G is a normal subgroup of the group of all automorphisms.
9. Identify a large class of groups for which the only inner automorphism is the identity mapping.

1.5 Direct Products

1.5.1 External and Internal Direct Products

In this section we examine a popular construction. Starting with a given collection of groups, we build a new group with the aid of the cartesian product. Let's start with two given groups H and K, and let $G = H \times K$, the set of all ordered pairs (h, k), $h \in H, k \in K$. We define multiplication on G componentwise:

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2).$$

Since (h_1h_2, k_1k_2) belongs to G, it follows that G is closed under multiplication. The multiplication operation is associative because the individual products on H and K are associative. The identity element in G is $(1_H, 1_K)$, and the inverse of (h, k) is (h^{-1}, k^{-1}). Thus G is a group, called the *external direct product* of H and K.

We may regard H and K as subgroups of G. More precisely, G contains isomorphic copies of H and K, namely

$$\overline{H} = \{(h, 1_K)\colon h \in H\} \text{ and } \overline{K} = \{(1_H, k)\colon k \in K\}.$$

Furthermore, $\overline{H}$ and $\overline{K}$ are normal subgroups of G. (Note that $(h,k)(h_1,1_K)(h^{-1},k^{-1}) = (hh_1h^{-1},1_K)$, with $hh_1h^{-1} \in H$.) Also, from the definitions of $\overline{H}$ and $\overline{K}$, we have

$$G = \overline{H}\ \overline{K} \text{ and } \overline{H} \cap \overline{K} = \{1\}, \text{ where } 1 = (1_H, 1_K).$$

If a group G contains normal subgroups H and K such that $G = HK$ and $H \cap K = \{1\}$, we say that G is the *internal direct product* of H and K.

Notice the key difference between external and internal direct products. We *construct* the external direct product from the component groups H and K. On the other hand, starting with a given group we *discover* subgroups H and K such that G is the internal direct product of H and K. Having said this, we must admit that in practice the distinction tends to be blurred, because of the following result.

1.5.2 Proposition

If G is the internal direct product of H and K, then G is isomorphic to the external direct product $H \times K$.

Proof. Define $f\colon H \times K \to G$ by $f(h,k) = hk$; we will show that f is an isomorphism. First note that if $h \in H$ and $k \in K$ then $hk = kh$. (Consider $hkh^{-1}k^{-1}$, which belongs to K since $hkh^{-1} \in K$, and also belongs to H since $kh^{-1}k^{-1} \in H$; thus $hkh^{-1}k^{-1} = 1$, so $hk = kh$.)

(a) f is a homomorphism, since

$$f((h_1,k_1)(h_2,k_2)) = f(h_1h_2,k_1k_2) = h_1h_2k_1k_2 = (h_1k_1)(h_2k_2) = f(h_1,k_1)f(h_2,k_2).$$

(b) f is surjective, since by definition of internal direct product, $G = HK$.

(c) f is injective, for if $f(h,k) = 1$ then $hk = 1$, so that $h = k^{-1}$.Thus h belongs to both H and K, so by definition of internal direct product, h is the identity, and consequently so is k. The kernel of f is therefore trivial. ♣

External and internal direct products may be defined for any number of factors. We will restrict ourselves to a finite number of component groups, but the generalization to arbitrary cartesian products with componentwise multiplication is straightforward.

1.5.3 Definitions and Comments

If $H_1, H_2, \dots H_n$ are arbitrary groups, the *external direct product* of the H_i is the cartesian product $G = H_1 \times H_2 \times \cdots \times H_n$, with componentwise multiplication:

$$(h_1, h_2, \dots, h_n)(h_1', h_2', \dots h_n') = (h_1h_1', h_2h_2', \dots h_nh_n');$$

G contains an isomorphic copy of each H_i, namely

$$\overline{H}_i = \{(1_{H_1}, \dots, 1_{H_{i-1}}, h_i, 1_{H_{i+1}}, \dots, 1_{H_n}) \colon h_i \in H_i\}.$$

As in the case of two factors, $G = \overline{H}_1\overline{H}_2 \cdots \overline{H}_n$, and $\overline{H}_i \trianglelefteq G$ for all i; furthermore, if $g \in G$ then g has a unique representation of the form

$$g = \overline{h}_1\ \overline{h}_2 \cdots \overline{h}_n \text{ where } \overline{h}_i \in \overline{H}_i.$$

Specifically, $g = (h_1, \dots, h_n) = (h_1, 1, \dots, 1) \dots (1, \dots, 1, h_n)$. The representation is unique because the only way to produce the i-th component h_i of g is for h_i to be the i^{th} component of the factor from $\overline{H}_i$. If a group G contains normal subgroups $H_1, \dots, H_n$ such that $G = H_1 \cdots H_n$, and each $g \in G$ can be uniquely represented as $h_1 \cdots h_n$ with $h_i \in H_i, i = 1, 2, \dots, n$, we say that G is the *internal direct product* of the H_i. As in the case of two factors, if G is the internal direct product of the H_i, then G is isomorphic to the external direct product $H_1 \times \cdots \times H_n$; the isomorphism $f\colon H_1 \times \cdots \times H_n \to G$ is given by $f(h_1, \dots, h_n) = h_1 \cdots h_n$. The next result frequently allows us to recognize when a group is an internal direct product.

1.5.4 Proposition

Suppose that $G = H_1 \cdots H_n$, where each H_i is a normal subgroup of G. The following conditions are equivalent:

(1) G is the internal direct product of the H_i.

(2) $H_i \bigcap \prod_{j \neq i} H_j = \{1\}$ for $i = 1, \dots, n$; thus it does not matter in which order the H_i are listed.

(3) $H_i \bigcap \prod_{j=1}^{i-1} H_j = \{1\}$ for $i = 1, \dots, n$.

Proof. (1) implies (2): If g belongs to the product of the $H_j, j \neq i$, then g can be written as $h_1 \cdots h_n$ where $h_i = 1$ and $h_j \in H_j$ for $j \neq i$. But if g also belongs to H_i then g can be written as $k_1 \cdots k_n$ where $k_i = g$ and $k_j = 1$ for $j \neq i$. By uniqueness of representation in the internal direct product, $h_i = k_i = 1$ for all i, so $g = 1$.

(2) implies (3): If g belongs to H_i and, in addition, $g = h_1 \cdots h_{i-1}$ with $h_j \in H_j$, then $g = h_1 \cdots h_{i-1} 1_{H_{i+1}} \cdots 1_{H_n}$, hence $g = 1$ by (2).

(3) implies (1): If $g \in G$ then since $G = H_1 \cdots H_n$ we have $g = h_1 \cdots h_n$ with $h_i \in H_i$. Suppose that we have another representation $g = k_1 \cdots k_n$ with $k_i \in H_i$. Let i be the largest integer such that $h_i \neq k_i$. If $i < n$ we can cancel the $h_t (= k_t), t > i$, to get $h_1 \cdots h_i = k_1 \cdots k_i$. If $i = n$ then $h_1 \cdots h_i = k_1 \cdots k_i$ by assumption. Now *any product of the H_i is a subgroup of* G (as in (1.5.2), $h_i h_j = h_j h_i$ for $i \neq j$, and the result follows from (1.3.6)). Therefore

$$h_i k_i^{-1} \in \prod_{j=1}^{i-1} H_j,$$

and since $h_i k_i^{-1} \in H_i$, we have $h_i k_i^{-1} = 1$ by (3). Therefore $h_i = k_i$, which is a contradiction. ♣

Problems For Section 1.5

In Problems 1–5, C_n is a cyclic group of order n, for example, $C_n = \{1, a, \dots, a^{n-1}\}$ with $a^n = 1$.

1. Let C_2 be a cyclic group of order 2. Describe the multiplication table of the direct product $C_2 \times C_2$. Is $C_2 \times C_2$ cyclic?

2. Show that $C_2 \times C_2$ is isomorphic to the four group (Section 1.2, Problem 6).
3. Show that the direct product $C_2 \times C_3$ is cyclic, in particular, it is isomorphic to C_6.
4. If n and m are relatively prime, show that $C_n \times C_m$ is isomorphic to C_{nm}, and is therefore cyclic.
5. If n and m are not relatively prime, show that $C_n \times C_m$ is not cyclic.
6. If p and q are distinct primes and $|G| = p, |H| = q$, show that the direct product $G \times H$ is cyclic.
7. If H and K are arbitrary groups, show that $H \times K \cong K \times H$.
8. If G, H and K are arbitrary groups, show that $G \times (H \times K) \cong (G \times H) \times K$. In fact, both sides are isomorphic to $G \times H \times K$.