An introduction to group theory

Tony Gaglione[1]

[1]Supported by the NRL. Author's address: Mathematics, Department, U.S. Naval Academy, Annapolis, MD 21402.amg@usna.edu.

This book was written in the summer of 1992 in the Radar Division of the NRL and is in the public domain. It is document PU/NRL/5350-92-231. Typed into latex by David Joyner (wdj@usna.edu).

Contents

Chapter 1

Preliminaries

In this introductory chapter, we will introduce required notation and, at the same time, review very briefly some set theory. Our discussion of set theory will be strictly naive. (The interested reader may consult the bibliography (see [St]) for a more axiomatic treatment.) We shall next introduce and prove certain results from elementary number theory.

1.1 Sets and mappings

We begin our discussion with the concept of a set, the notion of which we will assume is intuitively clear; although this is in actuality far from so and an unrestricted use of the set concept has led to contradictions in mathematics. It was for this reason that an axiomatic treatment became necessary.

In this discussion, we will usually designate sets by capital Roman letters such as A, B, C, etc, and elements of sets by small Roman letters. We will also indicate that an element a belongs to a set A by writing $a \in A$, while if this is not the case, we write $a \notin A$, read "a does not belong to the set A."

If we have a collection of sets indexed by elements α belonging to a set Λ, then this collection will be denoted by $\{A_\alpha\}_{\alpha\in\Lambda}$. For example, if $\Lambda = \mathbb{N}$, the set of positive integers or natural numbers, we could write $\{A_i\}_{i\in\mathbb{N}}$, meaning that we have a countable number of sets which are being considered. (Note, in general, it is not necessary that Λ be even countable. The set of all real numbers denoted by $\mathbb{R}$ is an example of an uncountable set as compared to $\mathbb{N}$, which is a countable set.)

Let $\{A_\alpha\}_{\alpha\in\Lambda}$ be a collection of sets. The **union** of these sets, denoted by

$\cup_{\alpha\in\Lambda}A_\alpha$, is the set of all elements which belong to at least one of the A_α. In case the index set Λ is equal to $\mathbb{N}$ or is finite, say is equal to $\{1, ..., n\}$, we use the following notations: $\cup_{i=1}^{\infty}A_i$, $\cup_{i=1}^{n}A_i$, respectively or

$$\cup_{i=1}^{\infty}A_i = A_1 \cup A_2 \cup ... \cup A_n \cup ...,$$

$$\cup_{i=1}^{;}A_i = A_1 \cup A_2 \cup ... \cup A_n.$$

Again let $\{A_\alpha\}_{\alpha\in\Lambda}$ be a collection of sets. The **intersection** of the sets, denoted by $\cap_{\alpha\in\Lambda}A_\alpha$, is the set of all elements which belong to all the A_α. Similar notations as for unions are adopted in the case of intersections when the index set Λ is countable or finite.

Next let A and B be two sets. If every element of A is also an element of B, one says that A is a **subset** of B, denoted $A \subset B$ (or $A \subseteq B$). If $A \subset B$ and $B \subset A$, then the sets A and B are said to be **equal**, denoted $A = B$. Finally, if $A \subset B$ but $A \neq B$, then A is called a **proper subset** of B, denoted $A \subsetneq B$.

If A and B are two sets, the **cartesian product**, $A \times B$, is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$. Here it is to be emphasized that $(a_1, b_1) = (a_2, b_2)$ if and only if $a_1 = a_2$ and $b_1 = b_2$. Similarly we can define the cartesian product of any finite number of sets. For example, $\mathbb{R}^n = \mathbb{R} \times ...\mathbb{R}$ (n times), consists of ordered n-tuples $(x_1, ..., x_n)$ where each $x_i \in \mathbb{R}$, for $1 \leq i \leq n$.

The set consisting of no elements at all is called the **null set** or **empty set** and is designated by $\emptyset$. If A and B are two sets such that $A \cap B = \emptyset$, then A and B are called **disjoint sets**.

We next introduce a particularly useful notation which will be used throughout: If A is a set, we denote by

$$\{x \in A \mid P(x)\}$$

the set of all elements x belonging to A for which the proposition $P(x)$ is true. For example, the set of even positive integers equals $\{x \mid x \text{ is even}\}$. In the way of notation and abbreviation, we shall also, sometimes, adopt the following convention: If A is a finite set consisting of the elements $x_1, ..., x_n$, one writes $A = \{x_1, ..., x_n\}$. In particular if A consists of just a single element x, we write $A = \{x\}$. A similar notation is frequently adopted in the case where A consists of a denumerable or countable number of elements. Finally, we define the **order** of a finite set A, written $|A|$, to be the number of elements in the set A. If A is not finite we write, $|A| = \infty$.

We now turn to the next item of business involving sets, namely the notion of a mapping between two sets. Let A and B be two sets. If for every $a \in A$ there is associated a unique $b \in B$, we say that there is a **mapping** or **function** f from A into B and we write $f(a) = b$. Here A is called the **domain** of f, B is the **co-domain** of f, and if $b = f(a)$, then b is the **image** of a under f. We denote this by

$$f : A \to B, \quad \text{or} \quad A \xrightarrow{f} B.$$

Let f be a mapping from A into B. If distinct elements of A have distinct images in B under f, i.e., if $a_1, a_2 \in A$ and $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$, then f is called a **one-to-one** (1-1) (or **injective**) mapping. Put another way, f is 1-1 if and only if $f(a_1) = f(a_2)$ implies $a_1 = a_2$. If for every $b \in B$, there is an element $a \in A$ such that $f(a) = b$, then the mapping f is said to be **onto** B.

Again, let $f : A \to B$, and suppose that E is a subset of A, $E \subset A$. The **image set** $f[E]$ is defined by

$$f[E] = \{f(x) \in B \mid x \in E\}.$$

If $F \subset B$ then the **pre-image** $f^{-1}[F]$ is defined by

$$f^{-1}[F] = \{x \in A \mid f(x) \in F\}.$$

Notice that an image set $f[E]$ can be empty only if E is empty, but that a pre-image set $f^{-1}[F]$ can be empty even if F is nonempty.

Suppose now that f is a 1-1 mapping of A onto B. Then for each $b \in B$, there exists a unique $a \in A$ such that $f(a) = b$. This allows us to define a mapping called the **inverse mapping** of f, which we denote by f^{-1}, where

$$f^{-1} : B \to A.$$

is defined by $f^{-1}(b) = a$ provided a is the unique element of A such that $f(a) = b$. It is easy to show that f^{-1} is also one-to-one and onto. This usage of the notation f^{-1} should not be confused with its usage for the pre-image of a set, which is defined even if f is NOT one-to-one and onto.

For any set A, we define the **identity map** on A, denoted by 1_A or simply 1 if the set involved is clear, as that mapping which leaves every element of A fixed, i.e., $1_A(x) = x$ for all $x \in A$.

Next let $f : A \to B$, and let $E \subset A$. The restriction of f to E is the mapping denoted by $f|_E$, and defined by $f|_E(x) = f(x)$ for all $x \in E$. (Here it is assumed that E is non-empty.)

Now let A, B, and C be sets and suppose that f is a mapping from A into B and g is a mapping from B into C. Thus we have

$$A \xrightarrow{f} B \xrightarrow{g} C.$$

Then the **composite map** (or **product map** or **composition**) gf is defined as

$$(gf)(x) = g(f(x))$$

for all $x \in A$; thus $gf : A \to C$. Since $g(f(x))$ is uniquely determined by x, gf is indeed a mapping. In the special case of $f : A \to A$, we speak of powers of f : f^2, f^3, etc., and mean $f^2(x) = f(f(x))$, $f^3(x) = f(f^2(x))$, etc., for all $x \in A$.

Using the notations introduced above and assuming f is a 1-1, onto mapping from A to B, it is easy to see that $ff^{-1} = 1_B$ and $f^{-1}f = 1_A$.

Let S be a set and furthermore let $\sim$ denote a relation defined between ordered pairs of elements of S such that given any two elements $a, b \in S$ either $a \sim b$ (read "a is equivalent to b") is true or it is false. In other words, using the previously introduced terminology and notation, we assume we are given a mapping:

$$S \times S \to \{T, F\},$$

i.e., a mapping of the cartesian product of S with itself into a two-element set consisting of T ("true") and F ("false"). If (a, b) is mapped into T, we write $a \sim b$ and say that "a is equivalent to b". If (a, b) is mapped into F, we say that "a is not equivalent to b". The relation, $\sim$, is called an **equivalence relation** on S if it satisfies the following three conditions:

1. (Reflexivity) $a \sim a$ for all $a \in S$.
2. (Symmetry) If $a \sim b$, then $b \sim a$.
3. (Transitivity) If $a \sim b$, and $b \sim c$, then $a \sim c$.

The following are examples of equivalence relations:

Example 1.1.1. *Take S to be the set of all triangles in the plane and take $\sim$ to be the relation of congruence, $\equiv$, or equally well, take $\sim$ to be the relation of similarity.*

Example 1.1.2. *Take S to be the set of all lines in the plane and $\sim$ to be the relation of being parallel. (By convention, a line is parallel to itself.)*

Example 1.1.3. *Take $S = \mathbb{Z}$, the set of all integers, and let m be a fixed positive integer. Define $a \sim b$ if and only if m divides $a - b$. This special equivalence relation is denoted by $a \equiv b \pmod m$, read a is* **congruent** *to b modulo (or just mod) m. It will be treated in more detail in the next section.*

Now suppose that we have a set S and an equivalence relation defined on S. We denote by $[a]$, the set of all elements of S which are equivalent to a, i.e.,

$$[a] = \{x \in S \mid a \sim x\}.$$

Such a set is called an **equivalence class**. Clearly $a \in [a]$ by the first condition for an equivalence relation, hence $[a] \neq \emptyset$, for all $a \in S$. We claim, next, that for $a, b \in S$ either $[a] = [b]$ or $[a]$ and $[b]$ are disjoint sets, i.e., $[a] \cap [b] = \emptyset$. To this end, suppose that $[a] \cap [b] \neq \emptyset$. Then there is a d such that $d \in [a]$ and $d \in [b]$. Let c be any element in $[a]$. Then $c \sim a$ and $a \sim d$. Hence $c \sim d$. Since also $d \sim b$, it follows that $c \sim b$, which implies $c \in [b]$. Thus $[a] \subset [b]$. Similarly, $[b] \subset [a]$. We have, therefore shown that either $[a]$ and $[b]$ are disjoint or are equal.

Summarizing, we have the following result.

Theorem 1.1.4. *If S is a set with an equivalence relation defined on it, then S is decomposed into disjoint, nonempty equivalence classes. (We say S is* **partitioned***.) This is denoted by $S = [a]$, where it is understood that the union is taken over only certain $a \in S$ so that the classes are disjoint.*

Next, we want to consider one further equivalence relation of great importance. It will occur in more specialized settings latter, and we consider the general case now. For this purpose let E and F be sets, and let $f : E \to F$. For $a, b \in E$ define $a \sim b$ if and only if $f(a) = f(b)$. It is readily seen that this is an equivalence relation on E. Let $\overline{E}$ denote the set of all equivalence classes and consider the following mappings:

$$E \overset{\kappa}{\to} \overline{E} \overset{g}{\to} f[E] \overset{i}{\to} F,$$

where $\kappa(a) = [a]$, $g([a]) = f(a)$, and $i(f(a))) = f(a)$. Clearly κ is an onto mapping. We *claim* that g is, first of all, well-defined: $[a] = [b]$ implies $g([a]) = g([b])$. Indeed, if $[a] = [b]$, then $a \in [b]$ or $a \sim b$, because $a \in [a]$,

so $f(a) = f(b)$; hence $g([a]) = g([b])$, proving the claim. Moreover, g is 1-1. Namely if $g([a]) = g([b])$, then $f(a) = f(b)$, so $a \sim b$ and, therefore, $[a] = [b]$. Also g is onto; for if $c \in f[E]$, then $c = f(a)$ for some $a \in E$, so $c = g([a])$. Finally, i is clearly a 1-1 mapping, and it is also clear that $f = ig$.

Thus it is seen that an arbitrary mapping f of one set into another can be written (factored) as a product of three mappings each of which has certain nice features which f in general need not possess.

1.1.1 Exercises

1. Let $f : A \to B$ and let $\{E_\alpha\}_{\alpha\in\Lambda}$ be a collection of subsets of A. Prove that

   (a) $f[\cup_\alpha E_\alpha] = \cup_\alpha f[E_\alpha]$,

   (b) $f[\cap_\alpha E_\alpha] \subset \cap_\alpha f[E_\alpha]$.

2. Let $f : A \to B$ and let $\{F_\alpha\}_{\alpha\in\Lambda}$ be a collection of subsets of B. Prove that

   (a) $f^{-1}[\cup_\alpha F_\alpha] = \cup_\alpha f^{-1}[F_\alpha]$,

   (b) $f^{-1}[\cap_\alpha F_\alpha] = \cap_\alpha f^{-1}[F_\alpha]$.

3. Construct examples of the following:

   (a) A mapping which is not one-to-one and not onto.

   (b) A mapping which is not one-to-one, but is onto.

   (c) A mapping which is one-to-one, but is not onto.

4. Construct an example of a mapping $f : A \to B$ such that $f[E \cap F] \neq f[E] \cap f[F]$, where $E, F \subset A$.

5. Using the notation in problem 1, show that if f is one-to-one, then $f[\cap_\alpha E_\alpha] = \cap_\alpha f[E_\alpha]$.

6. Let $f : A \to B$. Show that

   (a) if f is one-to-one then $f^{-1}[f[A]] = A$,

   (b) if f is onto, $f(f^{-1}(B)) = B$.

7. Let $A \xrightarrow{f} B \xrightarrow{g} C$. Show that if f is one-to-one and onto and if g is one-to-one and onto, then gf is one-to-one and onto.

8. Let $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$. Show that $(hg)f = h(gf)$. (Composition is associative).

9. Give examples of relations on a set S which satisfy all but one of the axioms for an equivalence relation on S.

10. Determine the equivalence classes for Example 1.1.3.

11. Show that if $S \neq \emptyset$ has a partition into disjoint nonempty subsets, then an equivalence relation may be defined on S (actually find this equivalence relation and show that it is an equivalence relation) for which the subsets of the partition are the equivalence classes. (Converse of Theorem 1.1.4)

12. Let $f : \mathbb{R} \to \mathbb{R}$ be the map given by $f(x) = x^2$. Let

$$A = [1, 2] = \{x \in \mathbb{R} \mid 1 \leq x \leq 2\},$$
$$B = (-1, 1) = \{x \in \mathbb{R} \mid -1 < x < 1\},$$
$$C = (4, 9) = \{x \in \mathbb{R} \mid 4 < x < 9\},$$
$$D = [0, 9] = \{x \in \mathbb{R} \mid 0 \leq x \leq 9\}.$$

Find

(a) $f[A]$,

(b) $f[B]$,

(c) $f^{-1}[C]$,

(d) $f^{-1}[D]$,

(e) a nonempty set $E \subset \mathbb{R}$ such that $f^{-1}[E] = \emptyset$.

1.2 Number theory

Just as in the case of set theory, our discussion of number theory will be strictly naive, e.g., we shall not develop $\mathbb{N}$ from axioms, we shall just assume that if $S \subset \mathbb{N}$ and $S \neq \emptyset$, then S has a smallest element, etc. We first establish the division algorithm:

Theorem 1.2.1. *(Division Algorithm): Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers q and r such that*

$$a = bq + r \quad \text{and} \quad 0 \leq r < |b|.$$

Proof: Let

$$S = \{m|b| \mid m \in Z \text{ and } m|b| \leq a\}.$$

Note that $S \neq \emptyset$ because $-|a||b| \in S$. The set S must therefore contain a largest element, say $t|b|$. Then, by the definition of S, $t|b| \leq a$. Putting $r = a - t|b|$, we have

$$a = t|b| + r \quad \text{where} \quad r \geq 0. \tag{1.1}$$

But $(t+1)|b| = t|b|+|b| > t|b|$. Thus by the maximality of $t|b|$, $(t+1)|b| \notin S$, so $(t+1)|b| > a$. Hence

$$t|b| + |b| > t|b| + r$$

or $r < |b|$. Finally let

$$q = \begin{cases} t, & \text{if } b > 0, \\ -t, & \text{if } b < 0, \end{cases}$$

So that $qb = t|b|$ if $b > 0$ and $qb = -tb = t(-b) = t|b|$ if $b < 0$. Thus by (1.1)

$$a = qb + r \quad \text{where} \quad 0 \leq r < |b|,$$

and the existence part of the theorem has been established.

Suppose now that

$$a = bq + r = bq + r$$

where $0 \leq r < |b|$ and $0 \leq r < |b|$. Then

$$r - r' = b(q' - q), \tag{1.2}$$

but $-|b| < r - r' < |b|$, which in conjunction with (1.2) implies $r - r' = 0$; thus $bq = bq'$, thus $q = q'$ (since $b \neq 0$). So we have uniqueness and our proof is complete. □

Let $a, b \in \mathbb{Z}$. We say that b **divides** a, written $b|a$, if there exists a $c \in \mathbb{Z}$ such that $a = bc$. If b does not divide a, we write $b \not| a$.

Definition 1.2.2. *The* **greatest common divisor** *(g.c.d.) of two integers a and b is a positive integer d, denoted by $gcd(a, b)$, such that $d|a$ and $d|b$, and if c is any integer such that $c|a$ and $c|b$, then $c|d$. (Here we assume that a and b are not both 0; in that case, we define $gcd(0, 0) = 0$.)*

We observe first that if the $gcd(a,b) exists$, then it is unique. To see this, suppose we have two g.c.d.'s d and d'. Since $d|a$ and $d|b$, and since $d = gcd(a,b)$, then we must have $d|d'$. Similarly, $d'|d$; hence $d = d$ (since the g.c.d. > 0, by definition).

Now let us show the g.c.d exists. Suppose $a, b \in \mathbb{Z}$ and also suppose $a \neq 0$ or $b \neq 0$. We let S denote the set of all positive integers of the form $xa + yb$ where $x, y \in \mathbb{Z}$. $S \neq \emptyset$, and therefore, S must contain a smallest integer, d. We claim that $d = gcd(a,b)$. Since $d \in S$, there exist $x_1, y_1 \in \mathbb{Z}$ such that

$$d = x_1 a + y_1 b. \tag{1.3}$$

If $c|a$ and $c|b$, then clearly from (1.3) $c|d$. Therefore, we must simply show that $d|a$ and $d|b$. By the Division Algorithm,

$$a = dq + r, \qquad \text{where} \qquad 0 \leq r < d.$$

Hence $r = a - dq = a - q(x_1 a + y_1 b) = x_2 a + y_2 b$, where $x_2 = 1 - q x_1$ and $y_2 = q y_1$. Thus if $r > 0$, then $r \in S$, which would contradict the minimality of d. Thus $r = 0$ and $d|a$. Similarly, $d|b$.

Summarizing, we have the following result.

Theorem 1.2.3. *The greatest common divisor $d = gcd(a,b)$ of any two integers exists, is unique, and can be expressed in the form $d = xa + yb$ where $x, y \in \mathbb{Z}$.*

Note that while d is unique, x and y are not, e.g., if $a = 6$ and $b = 4$, then $d = 2$ and (x,y) can be $(1,1)$, $(1,2)$, $(3,4)$. etc. We note that the proof we have given for the existence of the g.c.d. is not constructive. We wish now to given an alternate proof for the existence of the g.c.d. which at the same time yields a systematic finite constructive way (or an algorithm) for obtaining it. (This is called the **Euclidean Algorithm**.) We assume without loss of generality that $b > 0$ (go through this for $b < 0$ to convince yourself that it can be done!). We then write

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b.$$

Now if $r_1 = 0$, the process stops. If not, we write

$$b = r_1 q_2 + r_2, \qquad 0 \leq r_2 < r_1.$$

If $r_2 = 0$, the process stops. If not, write

$$r_1 = r_2 q_3 + r_3, \qquad 0 \leq r_3 < r_2$$

and continue until a 0 remainder is obtained, which must be the case eventually since $b > r_1 > r_2 > r_3 > ...$ is a sequence of decreasing *positive* integers. Thus we have

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1}, \end{aligned} \tag{1.4}$$

i.e., r_n is the last nonzero remainder.

Now we claim that the above Euclidean Algorithm yields the gcd.

Proof: Note that $r_n | r_{n-1}$, so from the next to the last equation in (1.4), we see that $r_n | r_{n-2}$, and continuing up the "scale" in (1.4), we eventually see that $r_n | b$ and $r_n | a$. Now if $c|a$ and $c|b$, then the first equation in (1.4) implies that $c|r_1$, which implies, by the second equation that $c|r_2$, and continuing down in this fashion, we finally have that $c|r_n$. Thus $r_n = gcd(a, b)$. □

The reader should have no difficulty in applying this algorithm to particular cases. It also should be noted that the Euclidean Algorithm, in particular equations (1.4), may also easily be used to write the g.c.d. of a and b as a linear combination of a and b, i.e., in the form $xa + yb$ with $x, y \in \mathbb{Z}$.

For $a, b \in \mathbb{Z}$, if $gcd(a, b) = 1$, then we say that the integers a and b are **relatively prime** (or **coprime**).

Definition 1.2.4. *The* **least common multiple** *(l.c.m.) of two nonzero integers a and b is a positive integer t, written $lcm(a, b)$, such that $a|t$ and $b|t$, and if $a|c$ and $b|c$, then $t|c$. We define $lcm(0, a) = 0$ for any integer a.*

As in the case of the g.c.d., it is easy to see that if the l.c.m. exists it is unique. Therefore we consider the existence. Since by Definition 1.2.4 $lcm(0, a) = 0$ for any $a \in \mathbb{Z}$, we now assume that both a and b are nonzero integers. Note that there is at least one positive common multiple, namely $\pm ab$. Thus there must exist a smallest positive common multiple. Call it t. Let c be any common multiple of a and b. Clearly, $gcd(t, c) \leq t$. However, $a|t$ and $a|c$; therefore, $a|gcd(t, c)$. Similarly, $b|gcd(t, c)$. Hence, $gcd(t, c)$ is a common multiple of a and b. Since t was chosen as the smallest positive

common multiple, we must have $t = gcd(t, c)$. This implies $t|c$, and completes the existence proof.

We will now establish a few useful properties regarding the g.c.d. and l.c.m. which will be used quite frequently.

Theorem 1.2.5. *If m is a positive integer, then $gcd(ma, mb) = mgcd(a, b)$.*

Proof: Let $d = gcd(a, b)$ and $\delta = gcd(ma, mb)$. Since $d|a$ and $d|b$, we have that $md|ma$ and $md|mb$; consequently $md|\delta$. On the basis of Theorem 1.2.3, we can write $d = xa + yb$, where $x, y \in \mathbb{Z}$. Then $md = x(ma) + y(mb)$ from which it is clear that $\delta|md$. Thus $\delta = md$, i.e., $gcd(ma, mb) = mgcd(a, b)$. □

The next theorem is actually a simple consequence of Theorem 1.2.5.

Theorem 1.2.6. *If m is a positive integer, and if $m|a$ and $m|b$, then $gcd(\frac{a}{m}, \frac{b}{m}) = \frac{gcd(a,b)}{m}$.*

Proof: $gcd(a, b) = gcd(m\frac{a}{m}, m\frac{b}{m}) = m \cdot gcd(\frac{a}{m}, \frac{b}{m})$, by Theorem 1.2.5. A division by m completes the proof. □

Corollary 1.2.7. *Let $d = gcd(a, b)$. Then $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proof: $gcd(\frac{a}{d}, \frac{b}{d}) = \frac{gcd(a,b)}{d} = 1$. □

In other words, the corollary states that when two numbers are divided by their g.c.d., the resulting quotients will be relatively prime.

Theorem 1.2.8. *If $c|ab$, and $gcd(c, b) = 1$, then $c|a$.*

Proof: Since $gcd(c, b) = 1$, there exist integers x and y such that $1 = bx + cy$. Thus $a = abx + acy$, and since $c|ab$ and $c|ac$, it is clear that $c|a$. □

Definition 1.2.9. *A positive integer $p > 1$ is called a* **prime** *if its only divisors are ± 1 and $\pm p$.*

Using this notion, we can immediately state the following corollary to Theorem 1.2.8.

Corollary 1.2.10. *If p is a prime such that $p|ab$, then $p|a$ or $p|b$.*

Proof: If $p|a$, are done. If $p|a$, then we claim that the $gcd(a, p) = 1$. For if $d = gcd(a, p)$, then $d|a$ and $d|p$. From the definition of prime, $d|p$ implies $d = 1$ or $= p$ (recall that the g.c.d. > 0). Since $p \not| a$, d must be 1. Now from Theorem 1.2.8, $p|ab$ and $gcd(a, p) = 1$ imply $p|b$. □

As our final theorem pertaining directly to divisibility in $\mathbb{Z}$, we establish the following connection between the g.c.d. and l.c.m.

Theorem 1.2.11. *If a and b are positive integers, then $gcd(a,b) \cdot lcm(a,b) = ab$.*

Proof: Consider $\frac{ab}{gcd(a,b)}$. We can write this as

$$\frac{ab}{gcd(a,b)} = \frac{a}{gcd(a,b)}b,$$

which is certainly a multiple of b. Similarly,

$$\frac{ab}{gcd(a,b)} = \frac{b}{gcd(a,b)}a,$$

is a multiple of a. Hence $\frac{ab}{gcd(a,b)}$ is a common multiple of a and b. Thus $lcm(a,b)|\frac{ab}{gcd(a,b)}$ or

$$lcm(a,b)gcd(a,b)|ab. \tag{1.5}$$

Next, consider $\frac{ab}{lcm(a,b)}$. This is integral since $lcm(a,b)|ab$. Also, since $a|lcm(a,b)$, we have $lcm(a,b) = ac$, for some $c \in \mathbb{Z}$. This imples

$$\frac{ab}{lcm(a,b)} = \frac{ab}{ac} = \frac{b}{c},$$

and so b/c is integral. However, $\frac{b}{c}|b$. Thus $\frac{ab}{lcm(a,b)}|b$, Similarly, $\frac{ab}{lcm(a,b)}|a$, and therefore $\frac{ab}{lcm(a,b)}|gcd(a,b)$, or

$$ab|lcm(a,b) \cdot gcd(a,b). \tag{1.6}$$

Comparing (1.6) and (1.5) yields the theorem. □

As our final consideration in this section, we turn to the equivalence relation introduced in Example 1.1.3. We recall that $a \equiv b \pmod{m}$ means $m|(a-b)$.

We next note that any integer a is congruent modulo m to one of the integers $0, 1, 2, ..., m-1$. For by the Division Algorithm, we can write $a = qm+r$, where $0 \leq r < m$, so $a-r = qm$, i.e., $a \equiv r \bmod m$, where $0 \leq r < m$.

We therefore have m distinct equivalence classes [0], [1], [2], ..., $[m-1]$ such that any integer is in one of these classes, and the classes are disjoint. The equivalence classes for this special equivalence relation are usually called **residue classes modulo** m, and a set of elements, exactly one from each class, is referred to as a **complete residue system modulo** m.

We shall now establish a few properties of the congruence relation.

Theorem 1.2.12. *If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then*

(1) $a + c \equiv b + d \pmod m$,

(2) $ac \equiv bd \pmod m$.

Proof: For (1), $m|(a-b)$ and $m|(c-d)$ imply $m|(a-b+c-d)$, i.e., $m|(a+c-(b+d))$ which is equivalent to (1). For (2), $m|(c-d)$ and $m|(a-b)$ imply $m|a(c-d)$ and $m|d(a-b)$. Thus $m|a(c-d)+d(a-b)$ or $m|(ac-bd)$, which is equivalent to (2). □

Thus with regard to addition and multiplication, the congruence relationship behaves like equality. This ceases to be the case with divisibility; e.g., it does not follow from $ac \equiv bc \pmod m$ that $a \equiv b \pmod m$. For example $9 \equiv 6 \pmod 3$ but $3 \not\equiv 2 \pmod 3$. We do, however, have the following theorem pertaining to division.

Theorem 1.2.13. *If $ac \equiv bc \pmod m$ and if $d = gcd(c, m)$, then $a \equiv b \pmod{\frac{m}{d}}$.*

Proof: By the hypothesis, $m|c(a-b)$.

Let $c = dc'$ and $m = dm'$ where $c', m' \in \mathbb{Z}$, and $gcd(c', m') = 1$ by the Corollary 1.2.7. Then $dm'|dc(a-b)$, or $m'|c'(a-b)$. Since $(c', m') = 1$, Theorem 1.2.8 implies that $m'|(a-b)$. This means that $a \equiv b \pmod{m'}$ and since $m' = \frac{m}{d}$ this completes the proof. □

We can see from this theorem that should $gcd(c, m) = 1$ (i.e., if c and m are relatively prime), then we can divide by c in a relationship of the form $ac \equiv bc \pmod m$.

Definition 1.2.14. *If n is a positive integer, the* **Euler ϕ-function**, *$\phi(n)$ is defined to be the number of positive integers less than or equal to n and relatively prime to n.*

One can show, that if $gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. Such functions are called **multiplicative**. (See Theorem 9.2.5.)

Finally, suppose that a is an integer prime to the positive integer m, i.e., $gcd(a, m) = 1$. We claim that every element of the residue class $[a]$ is also prime to m. Thus suppose that $b \in [a]$, so $b \equiv a \pmod m$. If $d = gcd(b, m)$, then since $m|(b-a)$, $d|(b-a)$, but $d|b$, so $d|a$. Consequently, $d|a$ and $d|m$ which implies $d = 1$ since $gcd(a, m) = 1$. On the basis of this it makes sense to say that a residue class is prime to m. We know that there are $\phi(m)$

residue classes prime to m, and a set of elements, exactly one from each of these classes, is called a **reduced residue system modulo** m.

We shall denote the set of residue classes prime to m by $\mathcal{R}(m)$.

1.2.1 Exercises

1. Prove that if two positive integers divide each other, then they must be equal; i.e., if $a, b \in \mathbb{N}$, $a|b$, and $b|a$, then $a = b$.

2. Extend the definition of g.c.d. to three elements $a, b, c \in \mathbb{Z}$ and denote it by $gcd(a, b, c)$. Prove that $gcd(a, b, c) = gcd(gcd(a, b), c) = gcd(a, gcd(b, c))$. (Note that $gcd(a, b, c) = 1$ does not imply that a, b, c are pairwise relatively prime.)

3. Show that for $a, b, c \in \mathbb{Z}$ if $a|c$ and $b|c$, and $gcd(a, b) = 1$, then $ab|c$.

4. Suppose $gcd(a, b) = 1$. Show that $gcd(a + b, a - b) = 1$ or $= 2$.

5. Prove that the product of any three consecutive integers is divisible by $6(= 3!)$. Try to generalize this.

6. Show that the set of integers $1^2, 2^2, ..., m^2$ is not a complete residue system modulo m if $m > 2$.

7. Let $a_1, a_2, ..., a_m$ be a complete residue system modulo m. Show that, if $gcd(a, m) = 1$, then $aa_1, aa_2, ...aa_m$ is also a complete residue system modulo m.

8. Let $a_1, a_2, ..., a_{\phi(m)}$ be a reduced residue system modulo m and let $gcd(a, m) = 1$. Show that $aa_1, aa_2, ..., aa_{\phi(m)}$ is also a reduced residue system modulo m.

9. If $gcd(a, m) = 1$ show that there is an integer b such that $ab \equiv 1 \pmod{m}$. Also show that $gcd(b, m) = 1$.

Chapter 2

Introduction to Groups

In this chapter, we shall consider in some detail the algebraic structure which will be of primary concern to us throughout, namely the notion of a group. Actually the reader has come in contact, during his or her mathematical career, with specific examples of groups as will be seen by the examples we shall give. All these examples have features in common which are desirable to axiomatize. When we prove results for the general structure, they apply automatically to all the specific examples.

2.1 Definition of a group

Before giving the definition of a group, it is necessary to define a binary operation on a set S.

Definition 2.1.1. *A* **binary operation** *on a set S is a mapping of $S \times S$ into S.*

In other words a binary operation on S is given when to every pair (a, b) of elements of S another element $c \in S$ is associated. The fact that $c \in S$ is sometimes expressed by saying a binary operation, or just an operation, on S is **closed**. This image element, c, is usually denoted by ab or $a + b$; still other notations such as $a \circ b$ or $a * b$ are also frequently used. We will adopt for the most part the "multiplicative" notation ab instead of the "additive" notation $a + b$. As a word of warning, we remind the reader that S is an arbitrary set not necessarily a set of numbers and one should not give any special significance to the juxtaposition (or product) ab, such as the product

of numbers. The elements of S, for example, could be mappings (functions). We shall at times speak of the "product of a and b" as the image element ab, and we also sometimes will use "sum of a and b" for $a+b$, when this notation is in use, but again the reader should not in general think of these elements as numbers. The reader should also note that a binary operation is defined on an *ordered* pair of set elements, so that in general, ab and ba are distinct.

We now proceed to the definition of a group.

Definition 2.1.2. *A* **group** *is a set G together with a binary operation defined on G such that*

1. *$a(bc) = (ab)c$, for all $a, b, c \in G$ (associative law),*
2. *There exists an element $e \in G$, called the* **identity** *element, such that $ae = ea = a$ for all $a \in G$,*
3. *To each $a \in G$, there exists an element $a^{-1} \in G$, called the inverse of a, such that $aa^{-1} = a^{-1}a = e$.*

Let us remark immediately that since a group G has a binary operation defined on it the operation is closed, i.e., for any $a, b \in G$ it must be true that $ab \in G$. We also note that it is customary to talk of a group G in a given discussion. This is actually not precise because a group, as just defined, is a set G together with a binary operation and it is possible that on a given set G a number of binary operations can be introduced such that the set G together with each of these operations is a group. In any discussion, however, the binary operation will be fixed and there will be no confusion in speaking just of the group G.

A set G together with a binary operation which satisfies condition (1) of Definition 2.1.2 is called a **semi-group**.

Before proving some simple consequences of the axioms of a group, we shall give a number of examples of groups, semi-groups, and objects which are neither. More examples will appear during the course of our development.

Example 2.1.3. *Take $G = \mathbb{Z}_+$, the set of positive integers (also denoted by $\mathbb{N}$), and let the binary operation be usual addition of integers. Clearly G is a semi-group, but G lacks an identity element and inverses, so that G is not a group.* □

Example 2.1.4. *Let $G = \mathbb{Z}_+$, but now take the binary operation to be usual multiplication of integers. Again, it is clear that G is a semi-group, but not a group since inverses (except for the integer 1) are missing.* □

Example 2.1.5. *Let $G = \mathbb{Z}$, the set of all integers, and let the operation be addition of integers. Then G is readily seen to be a group. G has identity 0, and each x in G has inverse $-x$.* □

Example 2.1.6. *Let $G = \mathbb{Z}$, and take the operation to be multiplication of integers. Then G is just a semi-group. (WHY?)* □

Example 2.1.7. *Let $G = \mathbb{Z}$, the set of all negative integers and let the operation be multiplication of integers. This is not a binary operation on $\mathbb{Z}$ since it is not closed, or in other words it is not a mapping into $\mathbb{Z}$, and therefore, G with respect to this operation is not even a semi-group.* □

Example 2.1.8. *Let G be the set of all rotations of the plane about the origin including the rotation through 0^o and take the binary operation to be composition of maps. Then it is easy to see that G is a group.* □

Example 2.1.9. *Let $G = \mathbb{Q}$, the set of all rational numbers, and let the binary operation be addition of rationals. Then G is a group. Similarly, the set, $G = \mathbb{Q}^\times$, of all nonzero rationals with respect to the usual multiplication of rationals is a group.* □

Example 2.1.10. *Let $G = \{1, -1\}$, i.e., the 2-element set consisting of the integers ± 1, and take the binary operation to be usual multiplication. Then G is a group.* □

Example 2.1.11. *Let G be the set of all complex n-th roots of unity, i.e., $G = \{z \in \mathbb{C} \mid z^n = 1\}$, where $\mathbb{C} = \{a + bi \mid a, b$ are real and $i = \sqrt{-1}\}$ is the set of all complex numbers. Let the binary operation be multiplication of complex numbers. Then G is a group. This example is a generalization of the preceding one in which $n = 2$. Note the order of G, $|G|$, is n.*

This group shall be denoted by μ_n. □

Example 2.1.12. *Let G be the set of all complex numbers which are roots of unity of any degree with the usual multiplication of complex numbers. Again G is a group, but this time G is infinite (cf. Example 2.1.11).* □

Example 2.1.13. *Let G be the set of all $n \times n$ matrices with real entries and determinant not 0. Take the binary operation to be matrix multiplication. Then G is a group. This group is called the general linear group of $n \times n$ matrices over $\mathbb{R}$, the set of real numbers. It is denoted by $GL(n, \mathbb{R})$. (Recall that if A and B are $n \times n$ matrices, $\det(AB) = \det A \det B$.) This group can also be interpreted as a set of functions: The set of 1-1, onto, linear transformations from the vector space $\mathbb{R}^n$ to itself. Matrix multiplication corresponds to composition of these functions.* □

Example 2.1.14. *Let $G = \mathbb{C}^n$, all n-tuples of complex numbers, i.e., $G = \mathbb{C} \times ... \times \mathbb{C}$ (n times). Let $x, y \in G$, then $x = (a_1, ..., a_n)$ and $y = (b_1, ..., b_n)$, where the a_i and b_i are complex numbers. Define $x + y = (a_1 + b_1, ..., a_n + b_n)$. It is easy to see that G with respect to this binary operation is a group.* □

Example 2.1.15. *Let A be any set. Then a mapping $f : A \to A$ which is both 1-1 and onto is called a* **permutation** *of A. To be more concrete, let $A = \{1, 2, ..., n\}$. Any 1-1, onto function, f, from A to A is a permutation (sometimes called a* **permutation of degree** *n) of A. Suppose f is a permutation of degree n, and let $f(1) = a_1$, $f(2) = a_2$, ..., $f(n) = a_n$, where $a_1, a_2, ..., a_n$ is just some rearrangement of the set A (thus the name permutation). We shall denote this situation by writing*

$$f = \begin{pmatrix} 1 & 2 & ... & n \\ a_1 & a_2 & ... & a_n \end{pmatrix} \tag{2.1}$$

i.e., the bottom entries indicate the images of the top entries under the mapping f. S_n denotes the set of all permutations of degree n. Clearly [1]*, $S_n = n!$. If $f, g \in S_n$, we take the binary operation to be composition of mapping fg; that this is, indeed, a binary operation follows as a special case of exercise 7 in the exercises for Section 1.1. The identity permutation, here denoted by 1, is just*

$$1 = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$$

i.e., $1 = 1_A$ in previous notation. If f is given by (2.1), then f^{-1} is just

$$f = \begin{pmatrix} a_1 & a_2 & ... & a_n \\ 1 & 2 & ... & n \end{pmatrix}$$

[1] To determine a permutation f as above, there are n possibilities for a_1, $n-1$ possibilities for a_2, ..., 1 possibility for a_n. By the multiplicative principle of counting (in any combinatorics book), it follows that the number of possibly permutations f is $n \cdot (n-1) ... \cdot 1 = n!$.

Then S_n is a group since the associative law is true in general for mappings (see exercise 8 in the exercises for Section 1.1). This group S_n is called the **symmetric group of degree** n.

Let us take a look at S_3, i.e., all permutations of the set $\{1,2,3\}$:

$$1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad r_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad r_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$
$$f_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad f_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad f_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

The operation here is composition of functions; e.g., to find f_1r_2, we note that

$$f_1r_2(1)=f_1(r_2(1))=f_1(3)=2,$$
$$f_1r_2(2)=f_1(r_2(2))=f_1(1)=1,$$
$$f_1r_2(3)=f_1(r_2(3))=f_1(2)=3.$$

Thus $f_1r_2=f_3$. Observe in f_1r_2, r_2 is applied first and f_1 next, so we read from right to left. We could also write

$$f_1r_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=f_3,$$

and again reading from right to left, we begin with $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ to get for example that $1\longmapsto 3$ and then $3\longmapsto 2$ so $1\longmapsto 2$ under f_1r_2. As another example, consider

$$r_2f_1=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=f_2.$$

Note that $f_1r_2\neq r_2f_1$. □

If a group G contains only a finite number of elements, i.e., $|G|<\infty$, then G is called a **finite group**; otherwise it is called an **infinite group**. Often when working with groups, especially finite groups, it is useful to draw a multiplication table (sometimes called a **Cayley table**). In general, let $G=\{g_1,...,g_n\}$ be a group with binary operation $*$, the **multiplication table** of G is:

$*$	g_1	g_2	...	g_j	...	g_n
g_1						
g_2						
$\vdots$						
g_i				$g_i * g_j$		
$\vdots$						
g_n						

The entry in the row of $x \in G$ and column of $y \in G$ is $x * y \in G$ (in that order). The reader should check that using the notation of the previous Example 2.1.15, that S_3 has the Cayley table

S_3	1	r_1	r_2	f_1	$f_2 4$	f_3
1	1	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	1	f_3	f_1	f_2
r_2	r_2	1	r_1	f_2	f_3	f_1
f_1	f_1	f_2	f_3	1	r_1	r_2
f_2	f_2	f_3	f_1	r_2	1	r_1
f_3	f_3	f_1	f_2	r_1	r_2	1

If G is a group and $ab = ba$ for all $a, b \in G$, then G is called a **commutative** group or an **abelian** group. Note from Example 2.1.15, S_3 is not abelian (as a matter of fact, this implies that S_n is a non-abelian for any $n \geq 3$). In the case of G being abelian, it is customary to adopt an additive notation and write $a + b$ instead of ab, 0 instead of e (or 1), and $-a$ instead of a^{-1}.

2.2 Some consequences of the axioms

We shall now proceed to obtain a number of direct consequences from the axioms of a group. Other such consequences will be given in the exercises. We shall call all these consequences elementary properties of groups.

2.2.1 Elementary Properties of Groups

Property 1. *Generalized associative law: We shall not give a careful formulation of this property nor shall we prove it (the interested reader can consult*

[Sc], p. 3, 4). This property essentially means that parentheses can be inserted or deleted at will (just as long as the order is not changed) without affecting the value of a product involving any number of group elements; e.g., if $a, b, c, d \in G$, G a group, then $aa(bcdbb) = (aa)b(cd)bb = ((aa)b)(cd)(bb)$, etc.

Property 2. *Uniqueness of the identity element: We claim that the element e of condition 2 of Definition 2.1.2 is unique.*

Proof: For suppose that f is also an identity of G; i.e., $af = fa = a$ for all $a \in G$. Then $ef = e$, but on the other hand $ef = f$, since e is an identity element. Consequently, $e = f$. □

Property 3. *Uniqueness of the inverse element: We claim that for each element a in G the element a^{-1} of condition 3 of Definition 2.1.2 is unique.*

Proof: Namely, suppose $ab = ba = e$ and $ac = ca = e$. Then $b = be = b(ac) = (ba)c = ec = c$. For each $a \in G$ we call this unique element $a^{-1} \in G$. □

Property 4. *If a and b are elements of a group G, then there exist unique elements x and y of G such that $xa = b$ and $ay = b$.*

Proof: If $x_0a = b$, then multiplying both sides on the right by a^{-1}, yields $(x_0a)a^{-1} = ba^{-1}$ or that $x_0 = ba^{-1}$. Conversely, if $x = ba^{-1}$, then $xa = (ba^{-1})a = b(a^{-1}a) = be = b$. Hence, the equation $xa = b$ has the unique solution $x = ba^{-1}$. Similarly, one shows that the equation $ay = b$ has the unique solution $y = a^{-1}b$. □

Property 5. *Alternate group definition (A): If G is a semi-group in which the equations $xa = b$ and $ay = b$ are solvable for arbitrary $a, b \in G$, then G is a group.*

Proof: Let e be a solution of the equation $xa = a$. Thus $ea = a$. Moreover, for any $b \in G$, there exists an element $y \in G$ such that $ay = b$. Now $eb = e(ay) = (ea)y = ay = b$. This shows that there exists an element $e \in G$ such that $eb = b$ for any $b \in G$. Now, analogously, consider the equation $ay = a$ and let f be a solution so that $af = a$. Then for any $b \in G$ there exists an $x \in G$ such that $xa = b$; thus $bf = (xa)f = x(af) = xa = b$, and

we have shown that there exists an element $f \in G$ such that $bf = b$ for any $b \in G$. Thus, we have

$$ef = f \quad \text{and} \quad ef = e,$$

so $e = f$, and consequently G contains an identity element. Now it follows from the hypothesis, that there exist $x_0, y_0 \in G$ such that $x_0 a = e$ and $ay_0 = e$. Hence, $y_0 = ey_0 = (x_0 a)y_0 = x_0(ay_0) = x_0 e = x_0$, so $x_0 = y_0 = a^{-1}$. This shows that the given statement is sufficient for G being a group. The fact that it is also necessary is a consequence of Property 4 of our elementary group properties. □

Property 6. *Cancellation laws: If G is any group, then*

(a) (Left Cancellation) $wx = wy$ implies $x = y$ for $w, x, y \in G$.

(b) (Right Cancellation) $xz = yz$ implies $x = y$ for $x, y, z \in G$.

Proof: Multiply both sides of (a) by w^{-1} on the left; (b) is done similarly. □

We note that as a consequence of the cancellation laws, if we write the Cayley table for G there will be no duplications in any row or column. As a matter of fact, this property of groups is quite useful to keep in mind when constructing the table in the first place. (See also Exercise 8 for this chapter.)

Property 7. *Alternate finite group definition: A finite semi-group (i.e., a semi-group with a finite number of elements) in which the cancellation laws hold is a group.*

Proof: Clearly this property is necessary for being a group from property 6. Now suppose that $A = \{a_1, a_2, ..., a_n\}$ is a finite semi-group satisfying the cancellation laws (see Property 6). Let a be an arbitrary element of A. The n elements $aa_1, ..., aa_n$ are then all distinct by the left cancellation law. Hence, if b is an arbitrary element of A, then there exists an a_i such that $aa_i = b$, i.e., the equation $ay = b$ is solvable. Similarly, the equation $xa = b$ is solvable in A, and therefore, by Property 5, A is a group. □

Property 8. *Alternate group definition (B): If G is a semi-group which has at least one element $e \in G$ such that $ae = a$ for all $a \in G$ (such an element is called a* **right identity***), and, if among all such elements e, there is an element f such that to each $a \in G$ there exists an element $a^* \in G$ such that $aa^* = f$ (such an element is called a* **right inverse***), then G is a group.*

Proof: If G is a group, it is clear that these conditions are satisfied. Now suppose G is a semi-group satisfying our conditions. Let $aa^* = f$. Then $faa^* = ff = f = aa^*$. Now there exists an $a^{**} \in G$ such that $a^*a^{**} = f$. Thus, $faa^*a^{**} = aa^*a^{**}$, or $faf = af$, so $fa = a$ since f is a right identity. Thus f is an identity, i.e., $af = fa = a$ for all $a \in G$. Thus if G is a group then $f = e$ is the unique identity element. To prove that G is a group, let $aa^* = f$. Then

$$\begin{gathered} a^*aa^* = a^*, \\ a^*aa^*a^{**} = a^*a^{**}, \\ a^*af = f, \\ a^*a = f. \end{gathered}$$

Hence $f = e$ is the unique identity and $a^* = a^{-1}$ is the unique inverse of a. □

Property 9. *Laws of exponents: By (1), we know that we can unambiguously write $a_1a_2...a_n$ where all the $a_i \in G$, G a group. If all the $a_i = g$, one writes this expression as g^n and speaks of the n^{th} power of g. (Note: g may not be a number. So even though $g \in G$ and $g^n \in G$ it may be that $n \notin G$, e.g., if $G = GL(n, \mathbb{R})$.) Negative powers of g can be defined as follows:*

$$g^{-n} = (g^n)^{-1} = (g^{-1})^n.$$

(Note: If we just defined $g^{-n} = (g^{-1})^n$, then it can be proven by induction on n that $g^{-n} = (g^n)^{-1}$ for all $n \in \mathbb{N}$.) Finally, one defines $g^0 = e$. It is then not hard to show that for m,n arbitrary integers, the following laws of exponents hold in G:

$$g^m g^n = g^n g^m = g^{m+n}, \tag{2.2}$$

$$(g^m)^n = g^{mn}. \tag{2.3}$$

In the case of an abelian group G written with the binary operation $+$, for $n \in \mathbb{Z}_+$ and $a \in G$, one writes na instead of a^n, $na = a + ... + a$ (n times), and $(-n)a = -(na) = n(-a)$. The laws corresponding to (2.2) and (2.3) become for abelian groups

$$ma + na = na + ma = (m + n)a,$$

$$n(ma) = (mn)a,$$

where $m, n \in \mathbb{Z}$.

Definition 2.2.1. *Consider now an element $g \in G$, a group. If all the powers, g^n $(n = 0, 1, 2, ...)$, of the element are distinct, then g is called an element of* **infinite order** *in G.*

Let us suppose that this is not the case. So there exist m, n, where $m \neq n$, say $m > n$, such that $g^m = g^n$. Then

$$g^{m-n} = e,$$

where $m - n > 0$. In other words, if g is not an element of infinite order, then there exist positive integers k such that $g^k = e$.

Definition 2.2.2. *Let G be a group and $a \in G$. Let n be the smallest positive integer, if it exists, such that $a^n = e$ then n is called the* **order** *of a and we shall write $o(a) = n$. One also says that a is of* **finite order** *with order n.*

If $o(a) = n$, then all the elements

$$e, a, a^2, ..., a^{n-1} \tag{2.4}$$

are distinct. For just as above, if any were equal we would get $a^t = e$ for $t < n$ in contradiction to the definition of n. Moreover, we also contend that any power a^k is equal to one of the elements in (2.4). For the Division Algorithm gives that $k = nq + r$, $0 \leq r < n$. Then

$$a^k = (a^n)^q a^r = a^r,$$

by the laws of exponents. In addition, we see from this same relationship that if $o(a) = n$, and $a^k = e$, then $n|k$. Indeed, $r < n$, $a^r = e$, and n is the smallest positive integer such that $a^n = e$, we must have $r = 0$. Thus $n|k$.

In summary, we have our last elementary property.

Property 10. *If G is a group, $a \in G$, and $o(a) = n < \infty$, then $e, a, ..., a^{n-1}$ are distinct, any power of a is equal to one of these, and finally $a^k = e$ if and only if $n|k$.*

We have seen (Example 2.1.12) that there exist infinite groups all of whose elements have finite orders; such groups are called periodic. In any group, G, the identity e, of course, has finite order 1. If this is the only element of G with finite order, then G is called **torsion free**.

We conclude this chapter with an important definition, viz., the notion of a subgroup of a group G. We shall make use of this concept throughout the text.

Definition 2.2.3. *A nonempty subset H of a group G is called a* **subgroup** *of G if*

(a) $a, b \in H$ *implies that* $ab \in H$,

(b) $e \in H$ *(where e is the identity of G),*

(c) $a \in H$ *implies that* $a^{-1} \in H$.

Notation: We write

$$H \leq G,$$

when H is a subgroup of G.

It is clear that a subgroup H of a group G is itself a group with respect to the same binary operation given on G. The definition can be given in a more succinct fashion, but we refer the reader to the exercises for this and related matters. We now list a few examples of subgroups of some of the groups given earlier in this chapter. Many more examples of subgroups will be encountered in the course of our investigations.

Example 2.2.4. *Let $G = \mathbb{Q}$ (Example 2.1.9) with binary operation to be addition of rationals and let $H = \mathbb{Z}$. Clearly $H \leq G$.* □

Example 2.2.5. *Let $G = GL(n, \mathbb{R})$ be the group of Example 2.1.13 and take $H = \{A \in G \mid \det(A) = 1\}$. Then $H \leq G$. (H is called the* **special linear group***, denoted $SL(n, \mathbb{R})$.)* □

Example 2.2.6. *Take $G = \mathbb{C}^n$ (Example 2.1.14) and H to be those n-tuples for which the first entry is 0. Then $H \leq G$.* □

Example 2.2.7. *Let $G = \{1, -1, i, -i\}$, i.e., the 4^{th} roots of unity (see Example 2.1.11) and take $H = \{1, -1\}$. Then $H \leq G$.* □

2.3 Exercises for Chapter 2

1. Let $a, b \in G$, G a group. Suppose $o(a) = o(b) = o(ab) = 2$. Then show that $ab = ba$.

2. Let G be a group and $H \subset G$, $H \neq \emptyset$. Prove $H \leq G$ if and only if $a, b \in H$ implies $ab^{-1} \in H$. (1 step subgroup test)

3. Let G be a group and let $a \in G$. Let $C_G(a) = \{x \in G \mid ax = xa\}$. Prove: $C_G(a) \leq G$. This subgroup is called the **centralizer** of a in G.

4. Suppose G is a group which has only one element $a \in G$ such that $o(a) = 2$. Prove that $ax = xa$, for all $x \in G$.

5. (Finite Subgroup Test) Let H be a nonempty finite subset of a group G such that $a, b \in H$ implies $ab \in H$. Then show that H is a subgroup of G.

6. Show that the intersection of any collection of subgroups of a group G is a subgroup.

7. Let G be a group. Referring to exercises 3 and 6, the subgroup $Z(G) = \cap_{a \in G} C_G(a)$ is called the **center** of G. Describe in words what $Z(G)$ is, i.e., without using intersections.

8. Show that if G is a finite group, its multiplication table is a Latin square, i.e., each element of the group appears once and only once in each row and in each column of the table.

Chapter 3

Permutations

We return in this chapter to the group Sn considered in Example 2.1.15. There we represented a permutation f in the form (2.1). This representation is not the most convenient for many purposes, and so we shall first introduce a much more useful representation.

3.1 Cycles and cycle notation

Again we denote by $A = \{1, 2, ..., n\}$ the set on which the permutation acts. We shall frequently denote by a_i, a_j, etc. arbitrary elements of A.

Definition 3.1.1. *Suppose that f is a permutation of $A = \{1, 2, ..., n\}$, which has the following effect on the elements of A: There exists an element $a_1 \in A$ such that. $f(a1) = a2$, $f(a2) = a3$, ..., $f(a_{k-1}) = a_k$, $f(a_k) = a_1$, and f leaves all other elements (if there are any) of A fixed, i.e., $f(a_j) = a_j$ for $j \neq 1, 2, ..., k$. Such a permutation f is called a* **cycle** *or a k-***cycle**.

We use the following notation for a k-cycle, f, as given above

$$f = (a_1, a_2, ..., a_k). \tag{3.1}$$

Let us elaborate a little further on the notation employed in (3.1). The cycle notation is read from left to right, it says f takes a_1 into a_2, a_2 into a_3, etc., and finally a_k, the last symbol, into a_1, the first symbol. Moreover, f leaves all the other elements not appearing in the representation (3.1) fixed. Note that one can write the same cycle in many ways using this type of notation; e.g., $f = (a_2, a_3, ..., a_k, a_1)$, etc. (How many ways?) Also we call k the **length**

of the cycle. Note we allow a cycle to have length 1, i.e., $f = (a_1)$; moreover, this is just the identity map. For this reason, we will usually designate the identity of S_n by (1). (Of course, it also could be written as (a_i) where $a_i \in A$.)

If f and g are two cycles, they are called **disjoint** if the elements moved by one are left fixed by the other, i.e., their representations (3.1) contain different elements of the set A (their representations are disjoint as sets).

We *claim* that if f and g are disjoint cycles, then they must commute, i.e., $fg = gf$. Indeed, since the cycles f and g are disjoint, each element moved by f is fixed by g and vice versa. First suppose $f(a_i) \neq a_i$. This implies that $g(a_i) = a_i$ and $f^2(a_i) \neq f(a_i)$ (WHY?). But since $f^2(a_i) \neq f(a_i)$, $g(f(a_i)) = f(a_i)$. Thus $(fg)(a_i) = f(g(a_i)) = f(a_i)$ while $(gf)(a_i) = g(f(a_i)) = f(a_i)$. Similarly if $g(a_j) \neq a_j$, then $(fg)(a_j) = (gf)(a_j)$. Finally, if $f(a_k) = a_k$ and $g(a_k) = a_k$ then clearly $(fg)(a_k) = a_k = (gf)(a_k)$. Thus $gf = fg$, proving the claim.

Before proceeding further with the theory, let us consider a specific example. Let $A = \{1, 2, ..., 8\}$ and let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 5 & 1 & 7 & 3 & 8 \end{pmatrix}$$

using the representation in (2.1). We pick an arbitrary number from the set A, say 1. Then $f(1) = 2$, $f(2) = 4$, $f(4) = 5$, $f(5) = 1$. Now select an element from A not in the set $\{1, 2, 4, 5\}$, say 3. Then $f(3) = 6$, $f(6) = 7$, $f(7) = 3$. Next select any element of A not occurring in the set $\{1, 2, 4, 5\} \cup \{3, 6, 7\}$. The only element left is 8, and $f(8) = 8$. It is clear that we can now write the permutation f as a product of cycles:

$$f = (1, 2, 4, 5)(3, 6, 7)(8),$$

where the order of the cycles is immaterial since they are disjoint and therefore commute. It is customary to omit such cycles as (8), i.e., elements left fixed by f, and write f simply as

$$f = (1245)(367);$$

it being understood that the elements of A not appearing are left fixed by f.

It is not difficult to generalize what was done here for a specific example, and show that any permutation f can be written uniquely, except for order,

as a product of disjoint cycles. Thus let f be a permutation on the set $A = \{1, 2, ...n\}$, and let $a_1 \in A$. Let $f(a_1) = a_2$, $f^2(a_1) = f(a_2) = a_3$, etc., and continue until a repetition is obtained. We claim that this first occurs for a_1, i.e., the first repetition is say $f^k(a_1) = f(a_k) = a_{k+1} = a_1$. For suppose the first repetition occurs at the kth iterate of f and

$$f^k(a_1) = f(a_k) = a_{k+1},$$

and $a_{k+1} = a_j$, where $j < k$. Then

$$f^k(a_1) = f^{j-1}(a_1),$$

and so $f^{k-j+1}(a_1) = a_1$, However, $k - j + 1 < k$ if $j \neq 1$, and we assumed that the first repetition occurred for k. Thus, $j = 1$ and so f does cyclically permute the set $\{a_1, a_2, ..., a_k\}$. If $k < n$, then there exists $b_1 \in A$ such that. $b_1 \notin \{a_1, a_2, ..., a_k\}$ and we may proceed similarly with b_1. We continue in this manner until all the elements of A are accounted for. It is then seen that f can be written in the form

$$f = (a_1, ..., a_k)(b_1, ..., b_\ell)(c_1, ..., c_m)...(h_1, ..., h_t). \tag{3.2}$$

Note that all powers $f^i(a_1)$ belong to the set $\{a_1 = f^0(a_1) = f^k(a_1), a_2 = f^1(a_1), ..., a_k = f^{k-1}(a_1)\}$, all powers $f^i(b_1)$ belong to the set $\{b_1 = f^0(b_1) = f^\ell(b_1), b_2 = f^1(b_1), ..., b_\ell = f^{\ell-1}(b_1)\}$, ... Here, by definition, b_1 is the smallest element in $\{1, 2, ..., n\}$ which does not belong to $\{a_1 = f^0(a_1) = f^k(a_1), a_2 = f^1(a_1), ..., a_k = f^{k-1}(a_1)\}$, c_1 is the smallest element in $\{1, 2, ..., n\}$ which does not belong to

$$\{a_1 = f^0(a_1) = f^k(a_1), a_2 = f^1(a_1), ..., a_k = f^{k-1}(a_1)\} \cap \{b_1 = f^0(b_1) = f^\ell(b_1), b_2 = f^1(b_1), ..., b_\ell = f^{\ell-1}$$

Therefore by construction, all the cycles in (3.2) are disjoint. From this it follows that $k + \ell + m + ... + t = n$. It is clear that this factorization is unique except for the order of the factors since it tells explicitly what effect f has on each element of A.

In summary we have proven the following result.

Theorem 3.1.2. *Every permutation of S_n can be written uniquely as a product of disjoint cycles.*

Let us pause to consider some examples. It is readily seen that the elements of S_3 (see Example 2.1.15) can be written in cycle notation as

$1 = (1), (1,2), (1,3), (2,3), (1,23,), (1,3,2)$. This is the largest symmetric group which consists entirely of cycles. In S_4, for example, the element $(1,2)(3,4)$ is not a cycle. Suppose we multiply two elements of S_3 say $(1,2)$ and $(1,3)$. Now we recall from Example 2.1.15, that in forming the product or composite here, we read from right to left. Thus to compute $(1,2)(1,3)$: We note the permutation $(1,3)$ takes 1 into 3 and then the permutation $(1,2)$ takes 3 into 3 so the composite $(1,2)(1,3)$ takes 1 into 3. Continuing the permutation $(1,3)$ takes 3 into 1 and then the permutation $(1,2)$ takes 1 into 2, so the composite $(1,2)(1,3)$ takes 3 into 2. Finally $(1,3)$ takes 2 into 2 and then $(1,2)$ takes 2 into 1 so $(1,2)(1,3)$ takes 2 into 1. Thus we see

$$(1,2)(1,3) = (1,3,2).$$

The reader should note that $(1,2) = f_3$ and $(1,3) = f_2$ so $(1,2)(1,3) = f_3 f_2 = r_2$ and $r_2 = (1,3,2)$ by the notation used in Example 2.1.15.

As another example of "cycle multiplication," consider the product in S_5,

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

Reading from right to left $1 \longmapsto 2 \longmapsto 2 \longmapsto 4 \longmapsto 4$ so $1 \longmapsto 4$. Now $4 \longmapsto 4 \longmapsto 4 \longmapsto 5 \longmapsto 5$ so $4 \longmapsto 5$. Next $5 \longmapsto 1 \longmapsto 3 \longmapsto 3 \longmapsto 3$ so $5 \longmapsto 3$. Then $3 \longmapsto 3 \longmapsto 1 \longmapsto 1 \longmapsto 2$ so $3 \longmapsto 2$. Finally $2 \longmapsto 5 \longmapsto 5 \longmapsto 2 \longmapsto 1$, so $2 \longmapsto 1$. Since all the elements of $A = \{1,2,3,4,5\}$ have been accounted for, we have

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

3.1.1 Exercises

1. In S_5 perform the indicated operations; write each of the following in the 2-row form (2.1):

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

   (b) $(1,3,4)^{-1}(1,2)(1,5,3,2)$,

   (c) $(1,3)^{-1}(1,2,4,5)(1,3)$.

2. Determine all the elements of S_4. Write each such permutation as a product of disjoint cycles.

3. Determine all subgroups of S_3.

4. Let the permutation f be a cycle of length $k \geq 1$ (called a k-**cycle**). Show that $o(f) = k$.

5. Let $f = g_1 g_2 ... g_r$ be the factorization of the permutation $f \in S_n$ into disjoint cycles g_k. If each g_k is an n_k-cycle, $k = 1, 2, ..., r$, determine $o(f)$ and justify your answer.

   HINT: Use the result of problem 4.

3.2 Transpositions

We return again to the general situation with S_n. Let $f \in S_n$. If f is a cycle of length 2, i.e., $f = (a_1, a_2)$ where $a_1, a_2 \in A$, then f is called a **transposition**. It is easy to see that any cycle can be written as a product of transpositions, namely

$$(a_1, ..., a_k) = (a_1, a_k)(a_1, a_{k-1})...(a_1, a_2). \tag{3.3}$$

According to (3.2) any permutation can be written in terms of cycles, but the above (3.3) shows any cycle can be written as a product of transpositions. Thus we have the following result.

Theorem 3.2.1. *Let $f \in S_n$ be any permutation of degree n. Then f can be written as a product of transpositions.*

Furthermore using (3.3) and (3.2), it is readily seen that if f is any permutation as in (3.2), then f can be written as a product of

$$W(f) = (k-1) + (j-1) + ... + (t-1) \tag{3.4}$$

transpositions. The number $W(f)$ is uniquely associated with the permutation f since f is uniquely represented (up to order) as a product of disjoint cycles. However, there is nothing unique about the number of transpositions occurring in an arbitrary representation of f as a product of transpositions, e.g., in S_3

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

since $(1, 2)(1, 2) = (1)$, the identity permutation of S_3. Although the number of transpositions is not unique in the representation of a permutation, f, as a product of transpositions, we shall show, however, that the parity (even

or oddness) of that number *is* unique. Moreover, this depends solely on the number $W(f)$ uniquely associated with the representation of f given in (3.2). More explicitly, we have the following result.

Theorem 3.2.2. *If f is a permutation written as a product of disjoint cycles and if $W(f)$ is the associated integer given by (3.4), then if $W(f)$ is even (odd) any representation of f as a product of transpositions must contain an even (odd) number of transpositions.*

Proof: We first observe the following:

$$(a,b)(b,c_1,...,c_t)(a,b_1,...,b_k) = (a,b_1,...,b_k,b,c_1,...,c_t), \tag{3.5}$$

$$(a,b)(a,b_1...,b_k,b,c_1,...,c_t) = (a,b_1,...,b_k)(b,c_1,...,c_t). \tag{3.6}$$

Suppose now that f is represented as a product of disjoint cycles, where we include all the 1-cycles of elements of A which f fixes, if any. If a and b occur in the same cycle in this representation for f, i.e.,

$$f = ...(a,b_1,...,b_k,b,c_1,...,c_t)..., \tag{3.7}$$

as in (3.5), then in the computation of $W(f)$ this cycle contributes $k+t+1$. Now consider $(a,b)f$. Since the cycles in (3.7) are disjoint and disjoint cycles commute,

$$(a,b)f = ...(a,b)(a,b_1...,b_k,b,c_1,...,c_t)...$$

since neither a nor b can occur in any factor of f other than $(a,b_1,...,b_k,b,c_1,...,c_t)$. So that using (3.5) (a,b) cancels out and we find that $(a,b)f = ...(b,c_1,...,c_t)(a,b_1,...,b_k)...$. Since $W((b,c_1,...,c_t)(a,b_1,...,b_k)) = k+t$ but $W(a,b_1,...,b_k,b,c_1,...,c_t) = k+t+1$, we have $W((a,b)f) = W(f)-1$.

A similar analysis, using (3.6), shows that in the case where a and b occur in different cycles in the representation of f, then $W((a,b)f) = W(f)+1$. (The reader should verify this!) Combining both cases, we have

$$W((a,b)f) = W(f) \pm 1. \tag{3.8}$$

Now let f be written as a product of m transpositions, say

$$f = (a_1,b_1)(a_2,b_2)...(a_m,b_m).$$

Then

$$(a_m,b_m)...(a_2,b_2)(a_1,b_1)f = 1. \tag{3.9}$$

Iterating (3.8), together with the fact that $W(1) = 0$, shows using (3.9) that

$$W(f) \pm 1 \pm 1 \pm ... \pm 1 = 0,$$

where there are m terms of the form ± 1. Thus

$$W(f) = \pm 1 \pm 1 ... \pm 1,$$

m times. Note if exactly p are $+$ and $q = m - p$ are $-$ then $m = p + q$ and $W(f) = p - q$. Hence $m \equiv W(f) \pmod 2$. (WHY?) Thus, $W(f)$ is even if and only m is even and this completes the proof. $\square$

It now makes sense to state the following definition since we know that the parity is indeed unique.

Definition 3.2.3. *A permutation $f \in S_n$ is said to be* **even** *if it can be written as a product of an even number of transpositions. Similarly, f is called* **odd** *if it can be written as a product of an odd number of transpositions.*

We note that if f and g are even permutations then so are fg and f^{-1} and also the identity permutation is even. Thus the set of all even permutation on $\{1, ...n\}$, denoted by A_n, is a subgroup of S_n. A_n is called the **alternating group**. We know that $|S_n| = n!$. Let us compute $|A_n|$.

Suppose $A_n = \{f_1, ..., f_k\}$ so $|A_n| = k$. Let t be the number of odd permutations so $t + k = n!$. If g is any odd permutation then $f_1 g, ..., f_k g$ are certainly all odd permutations and are all distinct, since $f_i g = f_j g$ if and only $i = j$ (see Elementary Property 6). Therefore $k \leq t$. Similarly, if $\{g_1, ..., g_t\}$ designates the set of all odd permutations, and, again, if g is any odd permutation, then $g_1 g, ..., g_t g$ are all even and are all distinct. Therefore $t \leq k$. Thus $t = k$ and since $t + k = n!$, $k = A_n = n!/2$.

3.2.1 Exercises

1. Write the elements of both S_3 and S_4 as products of transpositions

   HINT: use the result of problem 2 from Section 3.1.

2. Prove that any element of S_n, $n > 1$, can be written as a product of transpositions of the form $(1, k)$ where $k = 2, ..., n$.

   HINT: First prove that for any transposition (a, b), $(a, b) = (1, b)(1, a)(1, b)$.

3. Establish the two equations (3.5) and (3.6) used in the proof of Theorem 3.2.2.

4. Verify the case in the proof of Theorem 3.2.2 not done in the text. In particular, if $f \in S_n$ and a, b occur in different cycles in the disjoint cycle representation of f, then use (3.6) to show $W((a,b)f) = W(f)+1$.

5. Finally in the proof of Theorem 3.2.2, verify that

   (a) $m \equiv W(f) \pmod 2$;

   (b) $W(f)$ is even if and only if m is even.

6. Using the result of problem 1 above, determine both A_3 and A_4.

7. Prove that for $n > 2$, any element of A_n can be written as a product of cycles of the form $(1, 2, k)$, where $k = 3, 4, ...n$.

   HINT: Use the result of problem 2 and also establish that $(1, i, j) = (1, i, 2)(1, 2, i)(1, 2, j)$ *and* $(1, j, 2) = (1, 2, j)^{-1} = (1, 2, j)^2$.

Chapter 4

Subsets of a Group and Lagrange's Theorem

In this chapter, we establish one of the most important theorems in finite group theory, i.e., Lagrange's Theorem. This theorem gives a relationship between the order of a finite group and the order of any subgroup (in particular, if $|G| < \infty$ and $H \subset G$ is a subgroup, then $|H| \mid |G|$). In order to establish Lagrange's theorem we first investigate subsets of a group and partitions of the group with respect to these subsets.

4.1 Conjugacy

We now return from an investigation of permutation groups to the general situation where G is an arbitrary group. In this section, we will consider two special subgroups of G. Also we investigate a partition of G into equivalence classes with respect to a certain equivalence relation (conjugacy) on G. Another partition of G into equivalence classes (cosets) will be considered in the final section.

If $a \in G$, we define the **centralizer** of a in G, $C_G(a)$, as follows:

$$C_G(a) = \{g \in G \mid ag = ga\}.$$

Thus the centralizer of a in G consists of those elements in G which commute with a. In exercise 3 for Chapter 2, it was shown that $C_G(a)$ is a subgroup of G.

Next we consider the set

$$Z(G) = \cap_{a \in G} C_G(a).$$

Recall from exercise 7 for Chapter 2, that $Z(G) \subset G$ is called the **center** of G. Clearly, $g \in Z(G)$ if and only if $ga = ag$, for all $a \in G$, i.e., the center of a group consists precisely of those elements which commute with all elements of the group. Thus G is abelian if and only if $G = Z(G)$. Since $Z(G)$ is a subgroup of G, the identity element $e \in Z(G)$. It is entirely possible that for a given group G, $Z(G) = \{e\}$ (e.g., see exercise 1 of this section). In this case, one says that the group G has a **trivial center**; otherwise, one says the center of G is **non-trivial**.

Again let G be an arbitrary group. We introduce a relation on G as follows: for $a, b \in G$, define $a \sim b$ if and only if there is a $g \in G$ such that

$$a = gbg^{-1}. \tag{4.1}$$

Elements $a, b \in G$ related as in (4.1) are called conjugate. We claim that (4.1) is an equivalence relation on G; viz,

(1) (Reflexivity) $a \sim a$ since $a = eae^{-1}$.

(2) (Symmetry) $a \sim b$ implies that there exists a $g \in G$ such that $a = gbg^{-1}$. Solving for b, $b = g^{-1}ag = (g^{-1})a(g^{-1})^{-1}$. Thus $b \sim a$.

(3) (Transitivity) If $a \sim b$ and $b \sim c$, then there exist elements $g, h \in G$ such that $a = gbg^{-1}$ and $b = hch^{-1}$. Therefore $a = ghch^{-1}g^{-1} = (gh)c(gh)^{-1}$. So $a \sim c$.

Now G is therefore partitioned according to Theorem 1.1.4 into disjoint equivalence classes $[a]$. For this particular equivalence relation, that of (4.1), we call the equivalence classes **conjugacy classes** and write $Cl(a)$ instead of $[a]$. Theorem 1.1.4 also yields

$$G = \coprod Cl(a),$$

where this disjoint union ($\coprod$ has the same meaning as $\cup$, except that the union is disjoint) is taken over certain $a \in G$. Let us see next what it means that $Cl(a) = \{a\}$. This is equivalent to the fact that $gag^{-1} = a$ for all $g \in G$;

i.e., $a \in Z(G)$. Thus $Cl(a) = \{a\}$ if and only if $a \in Z(G)$. If we collect all such one element conjugacy classes together, then we can write

$$G = Z(G) \cup (\coprod Cl(a)), \tag{4.2}$$

where the union is taken over certain $a \in G$ such that $|Cl(a)| \geq 2$.

We turn to the case of S_n to illustrate in a specific example the concept of conjugate elements. Let $f \in S_n$, then using the 2-row form of (2.1), we can display the effect of f on the set $A = \{1, 2, ..., n\}$ by writing

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

Now if $g \in S_n$ also, then gfg^{-1} maps $g(i)$ into $gf(i)$. So gfg^{-1} can be displayed by

$$gfg^{-1} = \begin{pmatrix} g(1) & g(2) & ... & g(n) \\ gf(1) & gf(2) & ... & gf(n) \end{pmatrix}.$$

(Note: since g is 1-1 and onto $g[A] = \{g(1), g(2), ..., g(n)\} = A$.) Thus, using the cycle representation of f from Theorem 3.1.2, we may write f as in (3.2), i.e., $f = (a_1, ..., a_k)(b_1, ..., b_\ell)...(h_1, ..., h_t)$, Then since e.g. $f(a_i) = a_{i+1}$ $(1 \leq i < k)$ and $f(a_k) = a_1$ then $gfg^{-1}(g(a_i)) = g(a_{i+1})$ $(1 \leq i < k)$ and $gfg^{-1}(g(a_k)) = g(a_1)$, we can write

$$gfg^{-1} = (g(a_1), ..., g(a_k))(g(b_1), ..., g(b_\ell))...(g(h_1), ..., g(h_t)). \tag{4.3}$$

As an illustration, consider S_5 and let $f = (1, 5)(2, 3, 4)$, and $g = (1, 2, 3, 4, 5)$. To obtain gfg^{-1}, we must just see what g does to the elements occurring in f, e.g., $g(1) = 2$, $g(5) = 1$, etc.; hence, $gfg^{-1} = (2, 1)(3, 4, 5)$.

Going back to the more general situation, let us assume now that the cycle representation of f given in (3.2) above is such that $k \geq \ell \geq ... \geq t$ and also let's assume that all cycles, including even the 1-cycles, i.e., elements left fixed by f, are present. Then

$$M = k + \ell + ... + t.$$

This is called a **partition** of n. If f and $\hat{f}$ are two permutations of $\{1, 2, ..., n\}$ which are conjugate by an element of S_n, then observing that the cycle structure of (4.3) is the same as that of (3.2), we see that the *same* partition of n is associated with them. Conversely, it is easy to see that permutations having the same cycle structure must be conjugate (see exercise 2 of this section).

We have thus proven the following result.

Theorem 4.1.1. *Two permutations of degree n are conjugate (in S_n) if and only if they have the same cycle structure, i.e., if and only if they induce the same partition of n. Moreover, the number of conjugacy classes in S_n is equal to the number of partitions of n.*

4.1.1 Exercises

1. Prove that for $n > 2$, S_n has a trivial center, i.e., $Z(S_n) = \{1\}$.

   (HINT: Suppose $f \in Z(S_n)$ and $f \neq 1$. Write f in its disjoint cycle form (see equation (3.2) and Theorem 3.1.2). Consider the following three cases:

   Case 1 *f has at least one m-cycle with $m \geq 3$. Without loss of generality, assume $(a_1, a_2, ..., a_k)$ in (3.2) is such that $k \geq 3$. Then calculate $f \cdot (a_1, a_2)$ and $(a_1, a_2) \cdot f$.*

   Case 2 *the disjoint cycle decomposition of f has at least two transpositions (2-cycles), say $k = j = 2$ in (3.2), i.e., $f = (a_1, a_2)(b_1, b_2)....$ Then calculate $(a_1, b_1, a_2) \cdot f$ and $f \cdot (a_1, b_1, a_2)$.*

   Case 3 *$f = (a_1, a_2)$; then calculate $(a_1, a_2, a_3)f$ and $f(a_1, a_2, a_3)$ - recall $n \geq 3$.*

   In each case $a_1, a_2, a_3, b_1, b_2 \in \{1, 2, ..., n\}$ and we can "calculate" all we need to know by computing the effect of each permutation (remember permutation is a function) acting on a_1.)

2. (a) Suppose $f, g \in S_n$ and they have the same cycle structure. Prove $f \sim g$ ($\sim$ means the relation of being conjugate).

   (b) Explain why there are as many conjugacy classes in S_n as there are partitions of n. (HINT: Do it for $n = 3$, S_3, first!)

3. In S_5 perform the indicated operations. Write the result first as a product of disjoint cycles and then in the 2-row form (2.1):

   (a) $(1, 2, 3)(1, 3, 5)(2, 4)(1, 2, 3)^{-1}$,

   (b) $(1, 3, 4, 5, 2)(1, 2)(3, 5)(1, 3, 4, 5, 2)^{-1}$.

4. In S_4, determine the number of conjugacy classes and the number of permutations in each class. (See problem 2 for Section 3.1.)

4.2 Subsets of a group

We return again to the general case where G is an arbitrary group. Let S be an arbitrary nonempty subset of G, $S \subset G$ and $S \neq \emptyset$; such a set S is usually called a **complex** of G. If S_1 and S_2 are two complexes of G, the product S_1S_2 is defined as follows:

$$S_1S_2 = \{g_1g_2 \in G \mid g_1 \in S_1 \text{ and } g_2 \in S_2\}.$$

If $S_1 = \{g\}$, a singleton set, we shall write gS_2 instead of $\{g\}S_2$. (A similar notation will be followed if S_2 is a singleton set.) It is clear, by the associative law, that if S_1, S_2, and S_3 are complexes of G, then

$$S_1(S_2S_3) = (S_1S_2)S_3.$$

Finally if S is a complex of G, we denote by S^{-1} the following set

$$S^{-1} = \{g^{-1} \mid g \in S\}.$$

Using the notation just introduced, we can characterize, according to exercise 2 of Chapter 2, a subgroup as follows: a nonempty subset H of a group G is a subgroup if and only if

$$H \cdot H^{-1} = H. \tag{4.4}$$

It is also clear that if $S = H \leq G$, then $H^2 = HH = H$, and $H^{-1} = H$.

Next suppose that $H_1 \leq G$ and $H_2 \leq G$. Assume that $H_1H_2 \leq G$. If $a_1 \leq H_1$ and $a_2 \leq H_2$, then $a_1^{-1} \in H_1$ and $a_2^{-1} \in H_2$, therefore $a_1^{-1}a_2^{-1} \in H_1H_2$. But since H_1H_2 is assumed itself to be a subgroup, it must contain which is the general element of H_2H_1, i.e., we have shown that $H_2H_1 \subset H_1H_2$. Similarly,to show that $H_1H_2 \subset H_2H_1$, we need to show that a general element a_1a_2 of H_1H_2 is in fact in H_2H_1. Since $H_2H_1 \subset H_1H_2$, we have $(a_1a_2)^{-1} = a_2^{-1}a_1^{-1} = b_1b_2$, where $b_1 \in H_1$, $b_2 \in H_2$. This implies $a_1a_2 = b_2^{-1}b_1^{-1}$, so $H_1H_2 \subset H_2H_1$. Together, these imply $H_1H_2 = H_2H_1$.

Conversely, suppose that $H_1H_2 = H_2H_1$. Then $H_1H_2(H_1H_2)^{-1} = H_1H_2H_2^{-1}H_1^{-1} = H_1H_2H_1 = H_2H_1H_1 = H_2H_1 = H_1H_2$, hence $H_1H_2 \leq G$ from the characterization of subgroups given in (4.4).

We, therefore, have established the following result.

Theorem 4.2.1. *The product H_1H_2 of two subgroups H_1, H_2 of a group G is itself a subgroup if and only if H_1 and H_2 commute, i.e., if and only if $H_1H_2 = H_2H_1$.*

Warning: We caution the reader that when we say H_1 and H_2 commute, we do *not* demand that this is so elementwise. In other words, it is not demanded that $h_1h_2 = h_2h_1$ for all $h_1 \in H_1$ and all $h_2 \in H_2$; all that we demand is that for any $h_1 \in H_1$ and $h_2 \in H2$ $h_1h_2 = h_2'h_1'$, for some elements $h_1' \in H_1$ and $h_2' \in H_2$. For example, in S_3, if $H_1 = \{(1), (123), (132)\}$ and $H_2 = \{(1), (12)\}$ then as the reader can verify $H_1H_2 = S_3$ and $H_2H_1 = S_3$, so that $H_1H_2 = H_2H_1$. But note that $(1,2,3)(1,2) \neq (1,2)(1,2,3)$ whereas $(1,2,3)(1,2) = (1,2)(1,3,2)$.

4.2.1 Exercises

1. If G is a group written additively and S_1, S_2, are complexes we write $S_1 + S_2$ instead of S_1S_2. Let $G = \mathbb{Z}$ under $+$. Let $H = \{0, \pm 4, \pm 8, ...\}$ and $K = \{0, \pm 10, \pm 20, ...\}$. Clearly $H \leq G$, $K \leq G$. Determine $H+K$. More generally, if $H = \{na \mid n \in \mathbb{Z}\}$ and $K = \{nb \mid n \in \mathbb{Z}\}$. Determine $H + K$. (HINT: Think of the g.c.d.)

2. Complete the proof of Theorem 4.2.1 by showing that if $H_1 \leq G$, $H_2 \leq G$ and $H_1H_2 \leq G$, then $H_1H_2 \subset H_2H_1$.

3. Suppose H is a finite nonempty subset of a group G such that $H^2 = HH \subset H$. Prove that $H \leq G$. Is this still true if H is infinite? Why or why not?

4. Consider the following two subgroups of S_4: $H = \{1, (1,2)\}$ and $V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Is $HV_4 \leq S_4$? Why or why not? (V_4 is sometimes called the **Klein 4-group**.)

4.3 Cosets and Lagrange's Theorem

Again let G be an arbitrary group and let $H \subset G$. We shall now introduce another equivalence relation on G. Namely, define for $a, b \in G$

$$a \sim b \quad \text{if and only if} \quad a^{-1}b \in H. \tag{4.5}$$

Let us show, first of all, that this is indeed an equivalence relation.

(1) (Reflexivity) $a \sim a$ since $a^{-1}a = e \in H$.

(2) (Symmetry) $a \sim b$ implies $a^{-1}b \in H$, but since $H \subset G$, so $b^{-1}a = (a^{-1}b)^{-1} \in H$ and $b \sim a$.

(3) (Transitivity) If $a \sim b$ and $b \sim c$ then $a^{-1}b \in H$ and $b^{-1}c \in H$, so $a^{-1}b \cdot b^{-1}c = a^{-1}c \in H$, and $a \sim c$.

Therefore we do have an equivalence relation on G.

Let us investigate what the equivalence classes, $[a]$, for $a \in G$, look like for this equivalence relation. We have $a \sim b$ if and only if $a^{-1}b \in H$, i.e., if and only if $b \in aH$. Thus $[a] = aH$. These classes, aH, are called **left cosets** of H (recall from the previous section $aH = \{ah \mid h \in H\}$). We know from properties of equivalence relations (Theorem 1.1.4) that either $aH = bH$ or $aH \cap bH = \emptyset$. Moreover,

$$G = \coprod aH, \tag{4.6}$$

where, as usual, the (disjoint) union is taken over certain $a \in G$.

We also note that $aH = bH$ if and only if $a \sim b$, i.e., if and only if $a^{-1}b \in H$, i.e., $b = ah$, for some $h \in H$. In particular, $bH = H = eH$ if and only if $b \in H$.

One could define another equivalence relation by defining $a \sim b$ if and only if $ba^{-1} \in H$. Again this can be shown to be an equivalence relation on G, and the equivalence classes here are sets of the form Ha, called **right cosets** of H. Also, of course, one can write $G = \coprod Ha$, where, as above, the (disjoint) union is taken over certain $a \in G$.

It is easy to see that any two left (right) cosets have the same order (number of elements). To demonstrate this consider the mapping $aH \to bH$ via $ah \longmapsto bh$ where $h \in H$. It is not hard to show that this mapping is 1-1 and onto (see exercise 1 for this section). Thus we have $aH = bH$. (This is also true for right cosets and can be established in a similar manner.) Letting $b \in H$ in the above discussion, we see $|aH| = |H|$, for any $a \in G$.

One can also see that the collection $\{aH\}$ of all distinct left cosets has the same number of elements as the collection $\{Ha\}$ of all distinct right cosets. In other words, the number of left cosets equals the number of right cosets (this number may be infinite). For consider the map

$$f : aH \to Ha^{-1}. \tag{4.7}$$

This mapping is well-defined: for if $aH = bH$, then $b = ah$ where $h \in H$. Thus $f(bH) = Hb^{-1} = Hh^{-1}a^{-1} = f(aH)$. We did not choose the more

suggestive "mapping" $aH \to Ha$, which need not be well-defined. The reader should find an example where $aH \to Ha$ is not well-defined. (Hint: Think of $H = \{1, (1,2)\}$ in $G = S_3$.) It is not hard to show that the mapping in (4.7) is 1-1 and onto (see exercise 2 for this section). Hence the number of left cosets equals the number of right cosets; this number is called the **index** of H in G, denoted by $[G : H]$.

From the decomposition (4.6), in the special case where G is finite, we have

$$|G| = [G : H]|H|, \tag{4.8}$$

or

$$[G : H] = \frac{|G|}{|H|}. \tag{4.9}$$

This establishes the following extremely important theorem in the theory of finite groups.

Theorem 4.3.1. *(Lagrange's Theorem) The order of a subgroup of a finite group is a divisor of the order of the group.*

As an immediate corollary, we have the following result.

Corollary 4.3.2. *If $|G| = n$, then $a^n = e$ for all $a \in G$.*

Proof: Let $a \in G$ and $o(a) = m$. Then $H = \{e, a, ..., a^{m-1}\}$ is a subgroup of G. Moreover $m = |H|$. So $m|n$, i.e., $n = mk$ for $k \in \mathbb{Z}$. Hence, $a^n = a^{mk} = e$. $\square$

In the course of proving Corollary 4.3.2, we have shown the following result.

Corollary 4.3.3. *The order of any element of a finite group is a divisor of the order of the group.*

Let us now return to the relation of conjugacy (see (4.1)) introduced in the previous section. We first wish to get some information on the number of elements in a conjugacy class.

Theorem 4.3.4. *Let a be an element of the finite group G. Then $Cl(a) = [G : C_G(a)]$.*

Proof: Let $G = \coprod_{\alpha\in\Lambda} g_\alpha C_G(a)$, where Λ is an indexing set such that $|\Lambda| = [G : C_G(a)]$. If we can show that any 2 elements of $g_\alpha C_G(a)$ yield the same conjugate of a while elements from different left cosets, $g_\beta C_G(a)$, yield different conjugates of a then we will be done. This is because the number of distinct conjugates of a will then be equal to the number of distinct left cosets of $C_G(a)$ in G, that number being $[G : C_G(a)]$. Thus consider $g_\alpha x$ and $g_\alpha y$, where $x, y \in C_G(a)$, then

$$g_\alpha x a x^{-1} g_\alpha^{-1} = g_\alpha a g_\alpha^{-1},$$

and

$$g_\alpha y a y^{-1} g_\alpha^{-1} = g_\alpha a g_\alpha^{-1}.$$

(WHY?) However if $\alpha, \beta \in \Lambda$ with $\alpha \neq \beta$ and if

$$g_\alpha a g_\alpha^{-1} = g_\beta a g_\beta^{-1},$$

then $g_\beta^{-1} g_\alpha a g_\alpha^{-1} g_\beta (g_\beta^{-1} g_\alpha) a (g_\beta^{-1} g_\alpha)^{-1} = a$, which means that $g_\beta^{-1} g_\alpha \in C_G(a)$. In other words, $g_\alpha \in G_\beta C_G(a)$, which implies that $g_\alpha C_G(a) = g_\beta C_G(a)$. This is a contradiction because the decomposition was assumed to be a disjoint one. □

Since the number of elements conjugate to a in a finite group G is $[G : C_G(a)]$, that number is a divisor of G. With this information at our disposal, we can prove the important fact that any prime power group (i.e., a group of order p^m, where p is a prime) has a non-trivial center.

Theorem 4.3.5. *Let $|G| = p^m$, p a positive prime and G a group; then $Z(G)$ is non-trivial.*

Proof: We first decompose G via (4.2): $G = Z(G) \cup Cl(a) \cup Cl(b) \cup ... \cup Cl(h)$ (disjoint), where $Cl(a)$, $Cl(b)$, ..., $Cl(h)$ are called nontrivial conjugacy classes because in each case their order is > 1. Moreover, each of their orders divides G from Theorem 4.3.4. However since $|G| = p^m$, it is clear then that $p||Cl(a)|$, $p||Cl(b)|$, ..., $p||Cl(h)|$. However from the disjoint decomposition it follows that

$$|G| = |Z(G)| + |Cl(a)| + |Cl(b)| + ... + |Cl(h)|, \tag{4.10}$$

and we see that p must divide $|Z(G)|$ which completes the proof. □

We remark that equation (4.10) is itself an important result which holds in any finite group. It is called the **class equation**. The class equation says

that the order of the group is the order of the center added to the sum of the orders of the non-trivial conjugacy classes.

We next consider a rather useful theorem. Denote again by $|S|$, the number of elements in the complex S of the group G.

Theorem 4.3.6. *If $H_1 \leq G$, $H_2 \leq G$, G a finite group, then*

$$|H_1H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}.$$

Proof: Let $H = H_1 \cap H_2$. Then $H \leq G$ since H_1 and H_2 are subgroups. Moreover, $H \leq H_2$ and so we can decompose H_2 into right cosets relative to H. In other words,

$$H_2 = Ha_1 \cup Ha_2 \cup ... \cup Ha_n \quad \text{(disjoint)},$$

where $n = [H_2 : H] = |H_2|/|H|$. Now from this decomposition, we see that

$$H_1H_2 = H_1Ha_1 \cup H_1Ha_2 \cup ... \cup H_1Ha_n.$$

Since $H \leq H_1$, $H_1H = H_1$,

$$H_1H_2 = Ha_1 \cup Ha_2 \cup ... \cup Ha_n. \tag{4.11}$$

Moreover, we contend that this union is disjoint. For suppose $H_1a_i \cap H_1a_j \neq \emptyset$, where $i \neq j$. Then there exist elements $b, c \in H_1$ such that $ba_i = ca_j$ or $c^{-1}b = a_ja_i^{-1}$. But $c^{-1}b \in H_1$ and also $a_ja_i^{-1} \in H_2$. Thus $c^{-1}b = a_ja_i^{-1} \in H_1 \cap H_2 = H$ and so $Ha_j = Ha_i$. This implies that the decomposition for H_2 given above is not disjoint, a contradiction. Thus the union in (4.11) is disjoint and we have then

$$|H_1H_2| = n|H_1| = \frac{|H_1| \cdot |H_2|}{|H|}.$$

□

We end this section with an application of Lagrange's theorem, in particular of the first corollary of this theorem, to number theory.

Consider $\mathcal{R}(m)$, the residue classes prime to m which was first discussed at the end of section 1.2. $\mathcal{R}(m)$ is a group with respect to the binary operation

$$[a][b] = [ab], \tag{4.12}$$

where $[a], [b] \in \mathcal{R}(m)$. First of all this operation is well-defined, for if $[a] = [c]$ and $[b] = [d]$, then

$$a \equiv c \pmod{m} \quad \text{and} \quad b \equiv d \pmod{m}.$$

Hence $ab \equiv cd \pmod{m}$, using Theorem 1.2.12, i.e., $[ab] = [cd]$. Also $[ab] \in \mathcal{R}(m)$, for if $gcd(a, m) = 1$ and $gcd(b, m) = 1$, then it follows, by the corollary to Theorem 1.2.8 that $gcd(ab, m) = 1$.

It is now a simple matter to check that the group axioms are satisfied. We shall do so this just for one of the axioms, viz, the existence of inverses. (See exercise 3 of this section for verification of the other group axioms.) Indeed, let $[a] \in \mathcal{R}(m)$, therefore $gcd(a, m) = 1$. By Theorem 1.2.3 there exist $x, y \in \mathbb{Z}$ such that

$$1 = ax + my \quad \text{or} \quad [1] = [a][x] + [m][y], \tag{4.13}$$

where we define $[a + b] = [a] + [b]$, a well-defined operation also by Theorem 1.2.12. (However, this addition is not necessarily a mapping into $\mathcal{R}(m)$ - actually this is a binary operation on the set of all equivalence classes. See exercise 4 for this section.)

But $[m] = [0]$. Therefore (4.13) gives that $[1] = [a][x]$. To be done, we must show $[x] \in \mathcal{R}(m)$, i.e., $gcd(x, m) = 1$. Suppose $c|x$ and $c|m$, then by (4.13) $c|1$, so $gcd(x, m) = 1$, and $[x] \in \mathcal{R}(m)$. Hence, $\mathcal{R}(m)$ is a group and $|\mathcal{R}(m)| = \phi(m)$. Thus by Corollary 1 to Lagrange's Theorem,

$$[a]^{\phi(m)} = [1],$$

which implies the following result.

Theorem 4.3.7. *(Euler's theorem): If $gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

In the special case where $m = p$, a prime, $\phi(m) = \phi(p) = p - 1$, and we get **Fermat's Little Theorem**.

Corollary 4.3.8. *(Fermat) If p is a positive prime such that $p \not| a$, then $a^{p-1} \equiv 1 \pmod{p}$..*

4.3.1 Exercises

1. If $H \leq G$, a group, and $a, b \in H$, show that the mapping $f : aH \to bH$ defined by $f(ah) = bh$, for any $h \in H$, is 1-1 and onto.

2. Prove that the map in (4.7) is 1-1 and onto.

3. Verify the other two group axioms for the multiplication of equivalence classes in $\mathcal{R}(m)$ defined by (4.12) (i.e., associativity and existence of an identity element).

4. Let $\mathbb{Z}_m = \{[0], ..., [m-1]\}$, for m a positive integer, where $[x]$ is the equivalence class with respect to the equivalence relation of congruence modulo m. (Later, we shall also denote $\mathbb{Z}_m$ by the notation $\mathbb{Z}/m\mathbb{Z}$ - see Example 6.2.1 below.)

   (a) Show that $\mathbb{Z}_m$ contains all the equivalence classes.

   (b) Show that addition of equivalence classes defined by $[n] + [k] = [n + k]$ is a well defined operation on $\mathbb{Z}_m$.

   (c) Show that multiplication of equivalence classes defined by $[n] \cdot [k] = [n \cdot k]$ is a well defined operation on $\mathbb{Z}_m$.

   (d) Finally show $\mathbb{Z}_m$ is a group with respect to the + operation.

   Use Theorem 1.2.12 above.

5. Find the left and right coset decompositions (partitions) of S_3 with respect to all of its subgroups. (See problem 3 from Section 3.1.)

6. Let G be an abelian group of order 6. Show that there exists an element $a \in G$ such that $G = \{e, a, a^2, a^3, a^4, a^5\}$, i.e., $o(a) = 6$.

   (HINT: Use Corollary 4.3.3 of Lagrange's Theorem first to determine the possible orders of elements in G. Next show that if G has more than one element of order 2, then G must have a subgroup of order 4. This is a contradiction (why?). Thus G can only have at most one element of order 2, say x. Similarly, show G can have at most one element of order 3, say y. Let $y \in G$ such that $y \notin \{e, x\}$ but $o(y) = 3$. Show this implies G must have an element of order 6 by considering xy.)

7. Suppose G is a finite group with precisely 2 conjugacy classes. Prove $|G| = 2$.

(HINT: Decompose G into conjugacy classes, where one of the classes is the $Cl(e)$. Write an equation for the $|G|$ from this decomposition - like the class equation (4.10). What is $|Cl(e)|$? Next use Theorem 4.3.4 to find the order of the other conjugacy class. Finally, use Lagrange's Theorem 4.3.1, in particular equation (4.9), to write this in terms of $|G|$. Solve your equation for $|G|$ and use this to prove $|G| = 2$.)

Chapter 5

Generating Sets, Cyclic Groups and Isomorphisms

In this chapter, we shall consider the important notion of cyclic groups. This class of groups is particularly easy to treat and all relevant structural properties of cyclic groups will be determined here something which is at best quite difficult or hopeless, at the present time, for other large classes of groups. We shall also discuss in this section the concept of isomorphic groups.

5.1 Generators and isomophisms

Let G be an arbitrary group, let S be a complex of G, and let $\{H_\alpha\}_{\alpha\in\Lambda}$ be the collection of all subgroups of G which contain S, i.e., $S \subset H_\alpha$ for all $\alpha \in \Lambda$. The collection, $\{H_\alpha\}_{\alpha\in\Lambda}$, is clearly not empty since G itself is a subgroup which contains S. We denote the intersection of all subgroups of G containing S by $gp_G(S)$. That is

$$gp_G(S) = \cap_{\alpha\in\Lambda} H_\alpha,$$

or

$$gp_G(S) = \cap_{S\subset H\leq G} H.$$

(When it is clear that G is the group being considered, we use $gp(S)$.) From exercise 6 for Chapter 2, we have $gp(S) \leq G$. From its very definition, we have $S \subset gp(S)$ and $gp(S)$ is contained in any other subgroup which contains

S. In this sense, $gp_G(S)$ is the smallest subgroup of G containing S. We call $gp(S)$ the group **generated by** S.

Proposition 5.1.1. *Let G be a group, S a complex of G, and let E be the set of all finite products of elements of S and their inverses (including single elements of S). Then $gp(S) = E$.*

Proof: It is readily seen that E is a subgroup of G (see exercise 1 for this section) and $S \subset E$. Thus $gp(S) \subset E$. However, since $gp(S) \leq G$ and $S \subset gp(S)$, $gp(S)$ must certainly contain all finite products of elements of S and of inverses of elements of S, i.e., $E \subset gp(S)$. Thus $E = gp(S)$. □

Let us consider some examples.

Example 5.1.2. *Proposition 5.1.1 shows that in S_4, $gp(\{(1,2,4),(2,3,4)\}) = gp(\{(1,2,3),(1,2)(3,4)\})$. To see this, we note that*

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

$$(2,3,4) = (1,3,2)(1,2)(3,4) = (1,2,3)^{-1}(1,2)(3,4),$$

which shows $gp(\{(1,2,4),(2,3,4)\}) \subset gp(\{(1,2,3),(1,2)(3,4)\})$. To get the reverse inclusion, we note that

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

$$(1,2)(3,4) = (2,3,4)(1,4,2) = (2,3,4)(1,4,2)^{-1}.$$

□

We now turn our attention to the important case for this chapter. If $S = \{a\}$, then we shall write $\langle a \rangle$ for $gp(\{a\})$; and $\langle a \rangle$ will be referred to as the **cyclic subgroup generated by** a. The group G itself is called **cyclic** (or a **cyclic group**) if there exists an $a \in G$ such that $G = \langle a \rangle$, and such an element a is called a **generator** of G.

Example 5.1.3. *The set of integers $\mathbb{Z}$ under ordinary addition is cyclic generated by 1. (Note that -1 is also a generator. Also recall that when the operation is addition, 1^n is interpreted as $n \cdot 1 = 1 + 1 + ... + 1$ (n times), when $n > 0$, and as $n \cdot 1 = (-1) + (-1) + ... + (-1)$ ($|n|$ times), when $n < 0$.)*
□

Example 5.1.4. *If G is the group of example 2.1.11, then G is cyclic and $G = \langle \zeta_n \rangle$, where ζ_n is what is called a* **primitive n^{th} root of unity**. *If one recalls that $e^{i\theta} = \cos(\theta) + i\sin(\theta)$ (Euler's Formula), then we can take $\zeta_n = e^{2\pi i/n}$. We should note that this example gives us a cyclic group of order n for every positive integer n.*

This group is the same as that in Example 2.1.11. □

Before proceeding further in our discussion of cyclic groups, it will be convenient to introduce the notion of isomorphic groups.

Definition 5.1.5. *Two groups G_1 and G_2 are said to be* **isomorphic** *if there exists a mapping*

$$f : G_1 \to G_2$$

such that

(1) f is 1-1 and onto,

(2) $f(ab) = f(a)f(b)$, for all $a, b \in G$.

The second condition is sometimes referred to by saying that "f preserves the group operation." Also it should be noted, we have designated the operation in a multiplicative fashion (or juxtapositive) in both groups; although we warn the reader that the elements of G_1 and G_2 might be of an entirely different nature, as well as the operations defined between them. Nevertheless from an abstract point of view, isomorphic groups are indistinguishable. In other words, if G_1 and G_2 are isomorphic, then any relationship involving the binary operation holding for elements of one of the G_i $(i = 1, 2)$ holds for the corresponding elements under the mapping for the other G_i $(i = 1, 2)$. For example, suppose $f : G_1 \to G_2$ satisfies the conditions of Definition 5.1.5, i.e., G_1 and G_2 are isomorphic. Then if G_1 is abelian, G_2 must be abelian. If e_1 is the identity of G_1, then $f(e_1) = e_2$ is the identity of G_2 (see exercise 3 for this section). If $a^n = e_1$ in G_1, then $f(a)^n = f(a^n) = f(e_1) = e_2$, etc. Thus although their elements might be quite different, G_1 and G_2 are abstractly indistinguishable.

A mapping f satisfying the conditions of Definition 5.1.5 is called an **isomorphism** of G_1 onto G_2. If G_1 and G_2 are isomorphic, we will write $G_1 \cong G_2$. What we have noted above in words is that an isomorphism takes an identity into an identity, an element of order n into an element of order n (this is somewhat stronger than just saying $a^n = e_1$ implies $f(a)^n = e_2$.

Why?), etc. We also note that if we have the Cayley table for G_1, then we can use f to write the Cayley table for G_2 since f preserves the operation.

Example 5.1.6. *Consider $\mathbb{C}$ the additive group of all complex numbers and the subgroup $\hat{\mathbb{C}}$ of the group $\mathbb{C}^n$ of example 2.1.14 of all n-tuples of the form $(\alpha, 0, ..., 0)$, $\alpha \in \mathbb{C}$. Clearly the mapping*

$$\begin{array}{ccc} \mathbb{C} & \rightarrow & \mathbb{C} \\ \alpha & \longmapsto & (\alpha, 0, ..., 0). \end{array}$$

is an isomorphism of $\mathbb{C}$ onto $\hat{\mathbb{C}}$, or $\mathbb{C} \cong \hat{\mathbb{C}}$. (Verify this for yourself!) $\square$

5.1.1 Exercises

1. Let G be a group and S a complex of G. Let E be the set of all finite products of elements and of inverses of elements of S. Prove: $E \leq G$.

2. Show that the relation of being isomorphic, $\cong$, on the class of all groups is an equivalence relation. Describe the equivalence classes of $\cong$.

3. Let $f : G_1 \rightarrow G_2$ be an isomorphism of the group G_1 onto the group G_2. Let e_i be the identity of G_i $(i = 1, 2)$. Prove

   (a) $f(e_1) = e_2$,

   (b) $f(a^{-1}) = f(a)^{-1}$ for all $a \in G_1$.

   HINT: For (a), apply f to both sides of $e_1 e_1 = e_1$. For (b) use (a) together with the definition of inverse.)

4. Prove that any group of prime order is cyclic.

   (Note: If $G = \langle a \rangle$ is a finite cyclic group, $|G| = o(a)$ - see Property 10 of the elementary properties of groups from Chapter 2.)

5. (a) Show that the group $\mathbb{Z}_n$ of problem 4 for Section 4.3 is cyclic of order n.

   (b) Show that $\mathbb{Z}_n \cong G$ where G is the group of Example 5.1.3. (You must show your map is well-defined!)

6. Let G be a group of order pq, where p and q are primes such that $p < q$. Prove that G does not contain two distinct subgroups of order q.

   HINT: Use a proof by contradiction using Theorem 4.3.6 and problem 4 above.

5.2 Cyclic Groups

Now we return to the case of $G = \langle a \rangle$, a cyclic group. Clearly, $G = \{a^n \mid n \in \mathbb{Z}\}$. If G is finite, then of course $o(a)$ must be finite, say $o(a) = n$. Then recalling our discussion of elements of finite order (see Property 10 from Chapter 2),

$$G = \{e, a, a^2, ..., a^{n-1}\}.$$

Thus we see $|G| = o(a)$ in this case.

Next, let $G_1 = \langle a \rangle$ and $G_2 = \langle b \rangle$ be two infinite cyclic groups. Consider the mapping given by $f(a^n) = b^n$ $(n = 0, 1, 2, ...)$. This mapping is well-defined since G_1 is an infinite cyclic group generated by a (all powers of a are distinct since G_1 is infinite) and f is onto G_2. Also, so f preserves the operation. Finally if $f(a^n) = f(a^m)$ then $b^n = b^m$. Since G_2 is infinite cyclic, generated by b, however, this implies $n = m$; hence $a^n = a^m$. Thus f is an isomorphism mapping G_1 onto G_2 and so $G_1 \cong G_2$. We have shown that any two infinite cyclic groups are isomorphic. We note that since $\mathbb{Z}$, the additive group of integers, is infinite cyclic generated by ± 1, we have proven *any infinite cyclic group is isomorphic to* $\mathbb{Z}$.

Next suppose that $G_1 = \langle a \rangle$ and $G_2 = \langle b \rangle$ are finite cyclic groups such that $|G_1| = |G_2| = n$. Then $G_1 = \{e, a, a^2, ..., a^{n-1}\}$, and $G_2 = \{e, b, b^2, ..., b^{n-1}\}$. Define again by $f(a^k) = b^k$. To show that f is well-defined, we note that if $a^t = a^m$, with $t \geq m$ say, then $a^{t-m} = e$ and therefore $o(a) = n|(t-m)$ (again see Property 10 Chapter 2). Therefore $b^{t-m} = e$, since $o(b) = n|(t-m)$, and $b^t = b^m$. Thus f is well-defined. The rest of the justification needed to show f is an isomorphism of G_1 ontp G_2 is left as an exercise (see exercise 1 for this section). Hence $G_1 \cong G_2$. This shows that *any finite cyclic group of order* n *is isomorphic to* μ_n (see Example 5.1.4).

As our next consideration, we wish to determine the subgroups of a cyclic group. Suppose that $G = \langle a \rangle$ is a cyclic group and let $H \neq \{e\}$ be any subgroup of G. Let t be the smallest positive integer such that $a^t \in H$; such a t exists because H must contain at least one positive power of a. For if $a^k \in H$ and $a^k \neq e$ then either $k > 0$ or $k < 0$. If $k > 0$, we have a positive power of a in H, i.e., a^k. If $k < 0$, then $a^{-k} = (a^k)^{-1} \in H$ and again we have a positive power of a in H, i.e., a^{-k}. We claim that $H = \langle a^t \rangle$. For suppose that $x \in H$. Then $x = a^m$ for some integer m since $H \leq G = \langle a \rangle$. By the Division Algorithm, $m = qt + r$, $0 \leq r < t$. Then $a^m = a^{qt}a^r$ and since $a^r = a^m a^{-qt} \in H$. This implies by the minimality of t, that $r = 0$ and

$m = qt$. So $x = a^m = (a^t)^q$, i.e., $H = \langle a^t \rangle$. Therefore we have shown that *any subgroup of a cyclic group is also cyclic.*

Now suppose that $G = \langle a \rangle$ is an infinite cyclic group. We *claim* that G has infinitely many subgroups. If t is any positive integer, then $H = \langle a^t \rangle = \langle a^{-t} \rangle \leq G$. Let $t_1 \neq t_2$ be positive integers. If $\langle a^{t_1} \rangle = \langle a^{t_2} \rangle$ then we could write $a^{t_2} = a^{mt_1}$ for some $m \in \mathbb{Z}$ and and $a^{t_1} = a^{nt_2}$ for some $n \in \mathbb{Z}$. Hence $a^{t_2} = a^{mt_1} = a^{mnt_2}$. But $o(a) = \infty$, thus $m, n = \pm 1$, and $a^{t_2} = a^{\pm t_1}$. Again since a has infinite order and since t_1 and t_2 are positive, we must have $t_2 = t_1$. The only way to avoid this contradiction is to conclude that the hypothesis $\langle a^{t_1} \rangle = \langle a^{t_2} \rangle$ is false. In other words, we have shown that if $t_1 \neq t_2$ then $\langle a^{t_1} \rangle \neq \langle a^{t_2} \rangle$. This proves the claim.

Suppose next that $G = \langle a \rangle$, and $|G| = n$. If $H \neq \{e\}$ is a subgroup, then we know, $H = \langle a^t \rangle$, where t is the smallest positive integer such that $a^t \in H$. We *claim* that in this case $t|n$. For $a^n = e \in H$, so $n = qt$ by our earlier argument on the minimality of t (in the paragraph above where we showed any subgroup of a cyclic group is also cyclic). Conversely if t is a positive integer such that $t|n$, then $H = \langle a^t \rangle \leq G$. Moreover if t_1 and t_2 are positive integers such that $t_1 \neq t_2$ and $t_1|n$ and $t_2|n$ then $\langle a^{t_1} \rangle \neq \langle a^{t_2} \rangle$. For otherwise (i.e., assume instead that $\langle a^{t_1} \rangle = \langle a^{t_2} \rangle$), we must have $a^{t_1} = a^{qt_2}$ and $a^{t_2} = a^{kt_1}$. Thus $n|(t_1 - qt_2)$, but $t_2|n$ so $t_2|(t_1 - qt_2)$, so $t_2|t_1$. Similarly $t_1|t_2$ and so since $t_1, t_2 > 0$ we must have $t_1 = t_2$, a contradiction.

Summarizing, we see that for a finite cyclic group $G = \langle a \rangle$, with $o(a) = n$, then any subgroup H of G is of the form $\langle a^t \rangle$, where $t > 0$ and $t|n$. Moreover, for each positive t dividing n, there is such a subgroup. Also distinct divisors determine distinct subgroups. Finally since for a positive divisor d of n one has $(a^t)^d = e$ if and only if $n|td$ if and only if $(n/t)|d$, we conclude from Property 10 that $|H| = o(a^t) = n/t$, as t runs through the positive divisors of n. Of course, if t goes through all the positive divisors of n, so does n/t. Also note that the trivial subgroup $\{e\} = \langle a^0 \rangle$. Thus in the case of cyclic groups of finite order, the converse of Lagrange's theorem is true, viz, for each $d|n$, $d > 0$, there exists a (cyclic) subgroup of order d. Moreover, in this case there is precisely one such subgroup (see exercise 2 for this section).

The converse of Lagrange's Theorem is not true in general, i.e., if $|G| = n$ and $d|n$, $d > 0$, there need not exist a subgroup of order d. The smallest example is the group A_4 of order 12; it turns out that A_4 has no subgroup of order 6. This will be left as an exercise (see exercise 4 for section 6.2) after more tools are developed to handle it efficiently. We shall meet further instances of this and will point it out for specific cases later. We point out

now that it was no accident that the divisor was taken to be composite, i.e., not a prime, for prime divisors or for prime power divisors for that matter, there must exist subgroups of such orders. These matters will be attended to when we discuss the Sylow theorems.

Let us now summarize our results for cyclic groups.

Theorem 5.2.1. *(a) Any two infinite cyclic groups are isomorphic (to $\mathbb{Z}$).*

(b) Any two finite cyclic groups of the same order are isomorphic (to some μ_n, $n \geq 1$ - see Example 5.1.4).

(c) Any subgroup of a cyclic group is cyclic. In particular if $H \leq G = \langle a \rangle$ and $H \neq \{e\}$, then $H = \langle a^t \rangle$, where t is the smallest positive integer such that $a^t \in H$.

(d) For an infinite cyclic group $G = \langle a \rangle$, and for each positive t, $H = \langle a^t \rangle \leq G$, and distinct positive t's determine distinct subgroups.

(e) If $G = \langle a \rangle$ is a finite cyclic group of order n, then the t in part (c) divides n. Moreover to each positive divisor of n there is one and only one cyclic subgroup of that order.

We shall see presently that (e) really characterizes finite cyclic groups, but first we establish an extremely useful theorem, which will be used many times. L

Theorem 5.2.2. *Let G be an arbitrary group and let a G such that $o(a) = m$. Then $o(a^k) = m/gcd(m, k)$.*

Proof: Let $t = o(a^k)$. Then $a^{kt} = (a^k)^t = e$ which implies that $m|kt$ (see Property 10 of elementary properties of groups, in chapter 2). Now write (see Corollary 1.2.7)

$$m = gcd(m, k)m', \qquad k = gcd(m, k)k',$$

where $gcd(m', k') = 1$. Hence,

$$gcd(m, k)m'|gcd(m, k)k't,$$

or $m'|k't$. because of Theorem 1.2.8 and the fact that $gcd(m', k') = 1$, we have $m'|t$. But $m' = m/gcd(m, k)$, so $\frac{m}{gcd(m,k)}|t$. Now $(a^k)^{m/gcd(m,k)} =$

$(a^m)^{k/gcd(m,k)} = e$. Thus $t|(m/(gcd(m,k))$. Therefore combining these two results, $o(a^k) = t = m/gcd(m,k)$. $\square$

We apply the theorem immediately to the case of a finite cyclic group G of order n. Let $G = \langle a \rangle = \{e, a, ..., a^{n-1}\}$. By the theorem $o(a^k) = n/gcd(n,k)$. Thus $o(a^k) = n$ (and a^k is consequently also a generator of G) if and only if $gcd(n,k) = 1$. In other words, if G is a cyclic group of order n, then G has $\phi(n)$ generators, where ϕ is the Euler ϕ-function. Summarizing, we have the following result.

Corollary 5.2.3. *Suppose $G = \langle a \rangle$ and $|G| = n$. Then a^k is a generator of G if and only if k and n are relatively prime. Thus there are $\phi(n)$ generators of G.*

Using the same notation as before, for G a cyclic group with $|G| = n$, let us see which elements, a^k, of G are of order d. Again by Theorem 5.2.4, $o(a^k) = d$ if and only if $d = n/gcd(n,k)$. Thus $gcd(n,k) = n/d$. In which case, we can write $n = \frac{n}{d}d$, $k = \frac{n}{d}i$, where $gcd(d,i) = 1$. Thus the elements of order d are those of the form $a^{\frac{n}{d}i}$, where $gcd(i,d) = 1$. and $0 < i \leq d-1$ since $k \leq n-1$. There are then, of course, $\phi(d)$ elements of order d. Since $|G| = n$, we have

$$\sum_{d|n} \phi(d) = n, \tag{5.1}$$

an interesting number theoretic relationship involving the ϕ-function.

We shall make use of (5.1) directly in the following theorem. The author is indebted to W. Wardlaw for pointing this theorem out to him. (Also see [R].)

Theorem 5.2.4. *If $|G| = n$ and if for each positive d such that $d|n$, G has at most one cyclic subgroup of order d, then G is cyclic (and consequently, has exactly one cyclic subgroup of order d).*

Proof: For each $d|n$, $d > 0$, let $\psi(d) =$ the number of elements of G of order d. Then

$$\sum_{d|n} \psi(d) = n.$$

Now suppose that $\psi(d) \neq 0$ for a given $d|n$. Then there exists an $a \in G$ of order d which generates a cyclic subgroup, $\langle a \rangle$, of order d, of G. We *claim* all elements of G of order d are in $\langle a \rangle$. Indeed, if $b \in G$ with $o(b) = d$ and

$b \notin \langle a \rangle$, then $\langle b \rangle$ is a second cyclic subgroup of order d, distinct from $\langle a \rangle$. This contradicts the hypothesis, so the claim is proven. Thus, if $\psi(d) \neq 0$, then $\psi(d) = \phi(d)$. In general, we have $\psi(d) \leq \phi(d)$, for all positive $d|n$. But $n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \phi(d)$, by our previous work. It follows, clearly, from this that $\psi(d) = \phi(d)$ for all $d|n$. In particular, $\psi(n) = \phi(n) \geq 1$. Hence, there exists at least one element of G of order n; hence G is cyclic. This completes the proof. □

Corollary 5.2.5. *If in a group G of order n, for each $d|n$, the equation $x^d = 1$ has at most d solutions in G, then G is cyclic.*

Proof: The hypothesis clearly implies that G can have at most one cyclic subgroup of order d since all elements of such a subgroup satisfy the equation. So Theorem 5.2.4 applies to give our result. □

We have given a few applications along the way in this section and the preceding one of some of our results to number theory. We end this chapter with one further application. In particular, we claim that Theorem 4.3.6 is a generalization of Theorem 1.2.11, i.e., $gcd(a, b) \cdot lcm(a, b) = ab$. Let us see how this result follows from Theorem 4.3.6. We shall apply the theorem to the case where $G = \langle a \rangle$ is a cyclic group of finite order. This frequently, as we shall see in other instances, yields a number theoretic result as a special case of a group theoretical result. Let s_1, s_2 be arbitrary positive integers. Choose a positive integer n such that $s_1|n$ and $s_2|n$. Then take $G = \langle a \rangle$ with $o(a) = n$. Let $H_1 = \langle a^{s_1} \rangle$ and $H_2 = \langle a^{s_2} \rangle$. Then from Theorem 5.2.2, $|H_1| = n/s_1$, and $|H_2| = n/s_2$. It is not difficult to show (see exercise 3 for this section) that

$$H_1 \cap H_2 = \langle a^{lcm(s_1,s_2)} \rangle, \quad \text{and} \quad H_1 H_2 = \langle a^{gcd(s_1,s_2)} \rangle.$$

Thus Theorem 5.2.2 also implies that

$$|H_1 \cap H_2| = n/lcm(s_1, s_2) \quad \text{and} \quad |H_1 H_2| = n/gcd(s_1, s_2).$$

Then Theorem 4.3.6 tells us that

$$n/gcd(s_1, s_2) = \frac{(n/s_1)(n/s_2)}{n/lcm(s_1, s_2)},$$

which implies that $lcm(s_1, s_2)gcd(s_1, s_2) = s_1 s_2$ as desired.

5.2.1 Exercises

1. If G_1 and G_2 are finite cyclic groups such that $|G_1| = |G_2| = n$ and $f : G_1 \to G_2$ is defined as in the text. Show f is 1-1, onto, and operation preserving.

2. Let $G = \langle a \rangle$ with $o(a) = n$. Prove that G has a unique subgroup of order d where $d|n$.

   HINT: Let $t = n/d$ then $H = \langle a^t \rangle$ is a subgroup of order d. Suppose H_1 is another subgroup of order d. Show $H_1 = H$.

3. Let $G = \langle a \rangle$ with $|G| = n$. Let $s_1, s_2 > 0$ be integers such that $s_i|n$ $(i = 1, 2)$. Suppose $H_1 = \langle a^{s_1} \rangle$ and $H_2 = \langle a^{s_2} \rangle$. Prove that $H_1 \cap H_2 = \langle a^{lcm(s_1,s_2)} \rangle$ and $H_1H_2 = \langle a^{gcd(s_1,s_2)} \rangle$.

   HINT: For the latter, use the fact that the gcd is a linear combination of s_1 and s_2, i.e., Theorem 1.2.3.)

4. Let G be a group and $a \in G$ such that $o(a) = mn$ where $gcd(m, n) = 1$. Show that one can write $a = bc$ where $o(b) = m$, $o(c) = n$, and $bc = cb$. Moreover, prove the uniqueness of such a representation.

   HINT: Write $mx + ny = 1$, let $b = a^{ny}$, $c = a^{mx}$ and use Theorem 5.2.2. For uniqueness, show using $mx + ny = 1$, that if b and c satisfy the stated conditions in the problem, then they must be given as stated in this hint.

5. Prove that a group of order p^m, where p is a prime and $m \in \mathbb{N}$, must contain a subgroup of order p.

   HINT: Use Theorem 5.2.1.

6. If in a group G of order n, for each positive $d|n$, the equation $x^d = 1$ has less than $d + \phi(d)$ solutions, then show G is cyclic.

   HINT: Use the Corollary 5.2.3 and Theorem 5.2.4.

7. (W. Wardlaw) Prove that a finite group G is cyclic if and only if G has no more than k $k-th$ roots of 1 for every $k \in \mathbb{N}$, where 1 is the identity of G. .

   HINT: A $k-th$ root of 1 is a solution to $x^k = 1$. Use Theorem 5.2.1 for the only if part and the Corollary 5.2.5 for the if part.

Chapter 6

Factor Groups

In the first section, we shall consider special subgroups of a group called normal subgroups which are quite important in all of group theory. We shall see that normal subgroups enable us to construct new groups using the set of cosets relative to these subgroups. Finally, the last section in this chapter considers a class of groups which contains no proper normal subgroups. Such groups are called simple groups. In recent years the problem of determining (or classifying) all finite simple groups has received more attention from group theorists than any other single problem. (See the article by D. Gorenstein [G].) The simple groups are important because they play a role in finite group theory somewhat analogous to that of the primes in number theory. As a matter of fact, the classification of finite simple groups has been completed. Its proof involves some 500 journal articles covering approximately 15,000 printed pages. In the words of D. Gorenstein this "... is unprecedented in the history of mathematics ..."

6.1 Normal subgroups

Let G be an arbitrary group and suppose that H_1 and H_2 are subgroups of G. We say that H_2 is **conjugate** to H_1 if there exists an element $a \in G$ such that $H_2 = aH_1a^{-1}$. It is easy to see, analogously to our consideration of conjugate elements, that this is an equivalence relation on the set of all subgroups of G. Thus one simply speaks of conjugate subgroups.

Analogous to the definition of the centralizer of an element $a \in G$, we

define **normalizer** of the subgroup H in G, denoted by $N_G(H)$ as follows:

$$N_G(H) = \{a \in G \mid aH = Ha\}.$$

$N_G(H)$ is clearly a subgroup of G and $H \subset N_G(H)$. (When it is clear which group we are working in, we may write $N(H)$ for $N_G(H)$.)

The following theorem is analogous to Theorem 4.3.4. The proof, which is the same except for notational changes, we leave to the reader as an exercise.

Theorem 6.1.1. *Let $H \leq G$, G a finite group. Then the number of subgroups of G conjugate to H (i.e., the order of the equivalence class containing H) is $[G : N_G(H)]$.*

Next, we define the important notion of a normal subgroup.

Definition 6.1.2. *A subgroup H of a group G is called a* **normal subgroup** *of G if $aHa^{-1} = H$ for all $a \in G$. We denote this by $H \lhd G$.*

Thus $H \lhd G$ if and only if $N_G(H) = G$. If G is abelian, then every subgroup of G is normal. For an arbitrary group G, it is clear that G itself and the trivial subgroup $\{e\}$ are normal subgroups. In S_3 it is not hard to see that A_3 is normal. In fact $A_n \lhd S_n$ for all $n \in \mathbb{N}$. This follows as a special case of exercise 4 for this section. (It also follows by considering the parity of gfg^{-1} for $f \in A_n$ and $g \in S_n$.)

Suppose now that $N \lhd G$. If aN and bN are any two left cosets, then

$$(aN)(bN) = a(Nb)N = abN^2 = abN \tag{6.1}$$

which is a left coset. Here we have used the obvious fact that if N is normal $bN = Nb$ for all $b \in G$. Thus if $N \lhd G$, we need not speak of left or right cosets with respect to N because they are the same, so we can just talk simply of a coset.

The converse of this statement given in (6.1) above is also true and has been left as an exercise (see exercise 5 for this section). Namely, if $H \leq G$ is such that (for all $a, b \in G$) $aHbH = cH$ for some $c \in G$, i.e., the product of any two left cosets is a left coset, then $H \lhd G$.

For the sake of examples and references, we include here a table for the group A_4 of even permutations on the set $\{1, 2, 3, 4\}$. Let

$$A_4 = \{f_1, f_2, ..., f_{12}\},$$

where

$$f_1 = (1), \quad f_2 = (1,2)(3,4), \quad f_3 = (1,3)(2,4), \quad f_4 = (1,4)(2,3),$$
$$f_5 = (1,2,3), \quad f_6 = (2,4,3), \quad f_7 = (1,4,2), \quad f_8 = (1,3,4),$$
$$f_9 = (1,3,2), \quad f_{10} = (2,4,3), \quad f_{11} = (2,3,4), \quad f_{12} = (1,2,4).$$

The Alternating Group A_4.

A_4	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}
f_1	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}
f_2	f_2	f_1	f_4	f_3	f_6	f_5	f_8	f_7	f_{10}	f_9	f_{12}	f_{11}
f_3	f_3	f_4	f_1	f_2	f_7	f_8	f_5	f_6	f_{11}	f_{12}	f_9	f_{10}
f_4	f_4	f_3	f_2	f_1	f_8	f_7	f_6	f_5	f_{12}	f_{11}	f_{10}	f_9
f_5	f_5	f_8	f_6	f_7	f_9	f_{12}	f_{10}	f_{11}	f_1	f_4	f_2	f_3
f_6	f_6	f_7	f_5	f_8	f_{10}	f_{11}	f_9	f_{12}	f_2	f_3	f_1	f_4
f_7	f_7	f_6	f_8	f_5	f_{11}	f_{10}	f_{12}	f_9	f_3	f_2	f_4	f_1
f_8	f_8	f_5	f_7	f_6	f_{12}	f_9	f_{11}	f_{10}	f_4	f_1	f_3	f_2
f_9	f_9	f_{11}	f_{12}	f_{10}	f_1	f_3	f_4	f_2	f_5	f_7	f_8	f_6
f_{10}	f_{10}	f_{12}	f_{11}	f_9	f_2	f_4	f_3	f_1	f_6	f_8	f_7	f_5
f_{11}	f_{11}	f_9	f_{10}	f_{12}	f_3	f_1	f_2	f_4	f_7	f_5	f_6	f_8
f_{12}	f_{12}	f_{10}	f_9	f_{11}	f_4	f_2	f_1	f_3	f_8	f_6	f_5	f_7

Example 6.1.3. *Let us consider the set $V_4 = \{f_1, f_2, f_3, f_4\}$. Referring to our table for A_4, it is easy to see that V_4 is a subgroup of A_4. (Recall from Exercise 4 in §4.2 that V_4 is called the Klein 4-group.) We claim that $V_4 \lhd A_4$. This can be shown by direct computation. (See exercise 7 for this section.) However, here we just note that since conjugacy preserves cycle structure, see Theorem 4.1.1, $gV_4g^{-1} = V_4$ for all $g \in A_4$, thus $V_4 \lhd A_4$.* □

We finally note that to show an arbitrary subgroup $N \lhd G$ it suffices to show $gng^{-1} \in N$ for all $g \in G$ because of the following result.

Proposition 6.1.4. *Let $N \leq G$, G a group. Then if $aNa^{-1} \subset N$ for all $a \in G$, then $aNa^{-1} = N$. In particular, $aNa^{-1} \subset N$ for all $a \in G$ implies $N \lhd G$.*

(See exercise 5(a) for this section for the proof.)

6.1.1 Exercises

1. Prove that conjugacy is an equivalence relation on the set of all subgroups of a group. Describe the equivalence classes.

2. Let G be a group and $H \leq G$. Prove

   (1) $H \subset N(H)$,

   (2) $N(H) \leq G$.

3. Prove Theorem 6.1.1.

4. Prove that any subgroup of index 2 is a normal subgroup.

   (HINT: Consider the partition in terms of left cosets and then in terms of right cosets.)

5. Let G be a group and $H \leq G$.

   (a) Prove that $aHa^{-1} \subset H$ for all $a \in G$ implies $aHa^{-1} = H$.

   (b) Suppose H has the property that the product of any two left cosets of H is also a left coset of H; then prove that $H \lhd G$.

   (HINT: For (a) note that the condition must be true for a^{-1}. For (b) note that the product of aH and $a^{-1}H$ must be a left coset. Moreover $e \in aHa^{-1}H$. Then apply (a).)

6. Show that $H = \{1, (1,2)\} = \langle (1,2) \rangle$ is not a normal subgroup of S_3.

7. Referring to the Cayley table for A_4, let

$$V_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\},$$

   i.e., $V_4 = \{f_1, f_2, f_3, f_4\}$.

   (a)Prove $V_4 \leq A_4$.

   (b) Write all the left cosets of V_4 in A_4 and then write all the right cosets of V_4 in A_4.

   (c) Use the result of (b) to show that $V_4 \lhd A_4$.

8. Let G be a group, $N \lhd G$, and $H \lhd N$. Does it follow that $H \lhd G$ (i.e., is the relation of being a normal subgroup transitive)?

   (HINT: Think of A_4, V_4, and $\langle (1,2)(3,4) \rangle$.)

9. Let G be a group and $N \leq G$. Prove $N \lhd G$ if and only if N consists of complete conjugacy classes of all its elements, i.e., $Cl(g) \subset N$ for all $g \in N$.

6.2 Factor groups

Again let $N \lhd G$ and consider the set

$$\{aN, bN, ...\} \tag{6.2}$$

of all cosets. This set will be denoted by G/N. We claim that a binary operation can be introduced such that G/N with respect to this operation is a group called the **factor group** (or **quotient group**) of G with respect to N. Thus we define

$$aN \cdot bN = (aN)(bN) = abN, \tag{6.3}$$

i.e., we define the operation to be the ordinary product of complexes. The operation is well-defined for if $a'N = aN$ and $b'N = bN$, then, as we know $b' = bn_1$ and $a' = an_2$ where $n_1, n_2 \in N$. Hence

$$a'b'N = an_2bn_1N = an_2bN \tag{6.4}$$

since $n_1 \in N$. But $b^{-1}n_2b = n_3 \in N$, since N is normal, so the right hand side of (6.4) can be written as

$$an_2bN = (ab)(b^{-1}n_2b)N = abn_3N = abN. \tag{6.5}$$

Thus (6.4) and (6.5) show that if $N \lhd G$ then $a'b'N = abN$, i.e., the operation of coset multiplication defined in (6.3) is, indeed, well-defined.

The associative law is, of course, true because coset multiplication as defined in (6.3) uses the ordinary group operation which is by definition associative.

We claim N serves as the identity element of G/N. Indeed,

$$aN \cdot N = aN^2 = aN,$$

and

$$N \cdot aN = aN^2 = aN.$$

The inverse of aN is $a^{-1}N$ since

$$aNa^{-1}N = aa^{-1}N2 = N.$$

Similarly $a^{-1}NaN = N$.

To emphasize: the elements of G/N are complexes (subsets) of G. If $|G| < \infty$, then $|G/N| = [G : N]$, i.e., the member of cosets of N in G. It is also to be emphasized that in order for G/N to be a group N must be a normal subgroup of G. Again, if G is finite from Lagrange's Theorem $[G : N] = G/N$, (see equation 4.9) thus

$$G/N = G/N \tag{6.6}$$

As some of our examples will show, it is possible to have infinite G, infinite N, but finite G/N.

We now consider some examples.

Example 6.2.1. *Let* $6\mathbb{Z} = \{..., 12, 6, 0, 6, 12, ...\}$*, i.e.,* $6\mathbb{Z}$ *is the subgroup* $\langle 6\rangle$ *of the group* $\mathbb{Z}$ *of integers under addition. Since* $\mathbb{Z}$ *is abelian,* $6\mathbb{Z} \lhd \mathbb{Z}$*. To construct* $\mathbb{Z}/6\mathbb{Z}$*, we first find all the (left) cosets of* $6\mathbb{Z}$ *in* $\mathbb{Z}$*. Consider the following 6 cosets:*

$$\begin{aligned}
0 + 6\mathbb{Z} &= \{..., -12, -6, 0, 6, 12, ...\},\\
1 + 6\mathbb{Z} &= \{..., -11, -5, 1, 7, 13, ...\},\\
2 + 6\mathbb{Z} &= \{..., -10, -4, 2, 8, 14, ...\},\\
3 + 6\mathbb{Z} &= \{..., -9, -3, 3, 9, 15, ...\},\\
4 + 6\mathbb{Z} &= \{..., -8, -2, 4, 10, 16, ...\},\\
5 + 6\mathbb{Z} &= \{..., -7, -1, 5, 11, 17, ...\}.
\end{aligned}$$

From the above, it is evident that $\mathbb{Z} = 6\mathbb{Z} \cup (1 + 6\mathbb{Z}) \cup ... \cup (5 + 6\mathbb{Z})$ *(disjoint) which shows that these are all the cosets of* $6\mathbb{Z}$ *in* $\mathbb{Z}$*. (This is also clear from the Division Algorithm, for if* $n \in \mathbb{Z}$*, then* $n = 6q + r$ *where* $0 \leq r < 6$*. Thus* $n + 6\mathbb{Z} = 6q + r + 6\mathbb{Z} = r + 6\mathbb{Z}$*. We also note that this shows that if* $[n]$ *is the equivalence class of* n *under the equivalence relation of congruence modulo 6 (see Section 1.2), then* $[n] = [r] = r + 6\mathbb{Z}$*.) Now that we know the elements of the factor group, we write its Cayley table*

$\mathbb{Z}/6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$
$0+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$
$1+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$
$2+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$
$3+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$
$4+6\mathbb{Z}$	$4+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$
$5+6\mathbb{Z}$	$5+6\mathbb{Z}$	$0+6\mathbb{Z}$	$1+6\mathbb{Z}$	$2+6\mathbb{Z}$	$3+6\mathbb{Z}$	$4+6\mathbb{Z}$

Here we note that since the group operation is +, (6.3) becomes $(a+6\mathbb{Z})+(b+6\mathbb{Z}) = (a+b)+6\mathbb{Z}$. *It is easy to see that* $|\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$. *(See problem 4 for Section 5.2. As a matter of fact* $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$ *from the above parenthesized remark.) More generally, if* $n \in \mathbb{N}$ *and we let* $n\mathbb{Z} = \langle n \rangle = \{0, \pm n, \pm 2n, ...\}$, *then* $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. □

Example 6.2.2. *Consider* $G = S_3$ *and* $N = \langle (123) \rangle$. *As already remarked* $\langle (1,2,3) \rangle = A_3 = \{(1), (1,2,3), (1,3,2)\} \lhd S_3$, *and so* $|G/N| = 6/3 = 2$. *The elements of* G/N *are* $N = \langle (1,2,3) \rangle = \{(1), (1,2,3), (1,3,2)\}$ *and* $(1,2)N = \{(1,2), (2,3), (1,3)\}$. *The group* $G/N = \{N, (1,2)N\}$ *is a group of order 2 where the element (coset) N is the identity and* $(1,2)N \cdot (12)N = (12)^2 N = N$. □

Example 6.2.3. *Let* $G = GL(n, \mathbb{R})$ *and* $N = SL(n, \mathbb{R})$ *(see Example 2.2.5). If* $A \in G$, $B \in N$, $\det(ABA^{-1}) = \det A \det B (\det A)^{-1} = 1$. *This implies* $N \lhd G$. *Then* $G/N = \{AN \mid A \in G\}$. *We claim that* $X \in AN$ *if and only if* $X = AB$, *where* $B \in N$ *is such that the element* AN *of* G/N *consists of all* $n \times n$ *matrices in G with the same determinant as A. Indeed, if* $X = AB$ *then* $\det(X) = \det(A)\det(B) = det(A)$. *It still remains to show that if* $C \in GL(n, \mathbb{R})$ *and* $\det(C) = \det(A)$, *then* $C \in AN$, *i.e., the other inclusion. (This is left as exercise 1 for this section). This proves the claim. Thus G is the disjoint union* $G = \coprod_A AN$ *(disjoint), where the union is taken over matrices A with different determinants. If we choose for each nonzero real number* α *(*$\alpha \in \mathbb{R} - \{0\}$*) an* $A_\alpha \in G$ *such that* $\det(A_\alpha) = \alpha$ *and let* $\Lambda = \mathbb{R} - \{0\}$, *then* $G = \coprod_{\alpha \in \Lambda} A_\alpha N$. *Moreover, if* $\alpha \in \Lambda$ *and* $\beta \in \Lambda$ *are distinct then in* G/N, $(A_\alpha N)(A_\beta N) = A_{\alpha\beta} N$. *As a matter of fact, if we just think of* A_α *and* A_β *as representatives of their respective cosets (equivalence class representatives), then we can suppress the N, and think of this multiplication in* G/N *as being given by* $A_\alpha A_\beta = A_{\alpha\beta}$. □

When we create the factor group G/N, it is important to understand that we are really defining every element of N to be the identity. This is apparent from the previous example where we just suppressed the N. In Example 6.2.1, we are saying that any multiple of 6 is 0 in the factor group $\mathbb{Z}/6\mathbb{Z}$. That is why $8 + 6\mathbb{Z} = 2 + 6 + 6\mathbb{Z} = 2 + 6\mathbb{Z}$, etc. In Example 6.2.2, we have $(1,2)N = (2,3)N$, since $(2,3) = (1,2)(1,2,3)$ in S_3 and going to the factor group makes $(1,2,3)$ the identity. Group theorists often refer to the process of creating the factor group G/N as "killing" N.

Example 6.2.4. *Let $G = S_4$ and $N = V_4$. We first note that for the same reason as in Example 6.1.3, $V_4 \lhd S_4$ (i.e., $gV_4g^{-1} = V_4$ for all $g \in S_4$, Why?). To construct S_4/V_4, we first find all the (left) cosets of V_4 in S_4. Consider the following $6 = |S_4/V_4| = 4!/4$ cosets:*

$$\begin{gathered} V_4 = \\ (1,2,3)V_4 = \{(1,2,3),(1,3,4),(2,4,3),(1,4,2)\}, \\ (1,3,2)V_4 = \{(1,3,2),(2,3,4),(1,2,4),(1,4,3)\}, \\ (1,2)V_4 = \{(1,2),(3,4),(1,3,2,4),(1,4,2,3)\}, \\ (1,3)V_4 = \{(1,3),(2,4),(1,2,3,4),(1,4,3,2)\}, \\ (2,3)V_4 = \{(1,4),(2,4),(1,3,4,2),(1,2,4,3)\}. \end{gathered}$$

We can therefore write the Cayley table for S_4/V_4.

S_4/V_4	V_4	$(1,2,3)V_4$	$(1,3,2)V_4$	$(1,2)V_4$	$(1,3)V_4$	$(2,3)V_4$
V_4	V_4	$(1,2,3)V_4$	$(1,3,2)V_4$	$(1,2)V_4$	$(1,3)V_4$	$(2,3)V_4$
$(1,2,3)V_4$	$(1,2,3)V_4$	$(1,3,2)V_4$	V_4	$(1,3)V_4$	$(2,3)V_4$	$(1,2)V_4$
$(1,3,2)V_4$	$(1,3,2)V_4$	V_4	$(1,2,3)V_4$	$(2,3)V_4$	$(1,2)V_4$	$(1,3)V_4$
$(1,2)V_4$	$(1,2)V_4$	$(2,3)V_4$	$(1,3)V_4$	V_4	$(1,3,2)V_4$	$(1,2,3)V_4$
$(1,3)V_4$	$(1,3)V_4$	$(1,2)V_4$	$(2,3)V_4$	$(1,2,3)V_4$	V_4	$(1,3,2)V_4$
$(2,3)V_4$	$(2,3)V_4$	$(1,3)V_4$	$(1,2)V_4$	$(1,3,2)V_4$	$(1,2,3)V_4$	V_4

The reader should note that this table gives a non-abelian group of order 6. As a matter of fact, $S_4/V_4 \cong S_3$, which can be seen immediately from the above if we think of killing off V_4. □

6.2.1 Exercises

1. Let $G = GL(n,\mathbb{R})$ and $N = SL(n,\mathbb{R})$ for $n \geq 1$.

   (a) Let $A \in G$ and show that the coset $AN = \{X \in GL(n,) \mid \det X = \det A\}$.

   (b) Let $\mathbb{R}^\times$ denote the group of non-zero real numbers with respect to the usual multiplication. Show $G/N \cong \mathbb{R}^\times$.

   (c) Is $G/N \cong G$? Why or why not?

2. Let $G = \langle a \rangle$ be a cyclic group. Let H be any subgroup of G.

(a) Show that $H = \langle a^s \rangle$, where s is an arbitrary positive integer if $|G| = \infty$, while if $|G| < \infty$, then $s||G|$.

HINT: Go back to §5.2 on cyclic groups.

(b) Explain why $H \lhd G$. Show that $G/H = \{H, aH, ..., a^{s-1}H\} = \langle aH \rangle$. In words this says, that a factor group of a cyclic group is cyclic.

3. Using your result from exercise 7 of Section 6.1, write the Cayley table for A_4/V_4.

4. Prove that A_4 has no subgroup of order 6.

HINT: Assume it does. Let $H \leq A_4$ with $|H| = 6$. Then $H \lhd A_4$ (Why?). So A_4/H makes sense. Moreover, this also implies that $f^2 \in H$ for all $f \in A_4$ (Why?). Now look at the table for A_4 and count the number of squares to come to a contradiction.) (Note this problem gives an example to show that the converse of Lagrange's Theorem is false.

6.3 Simple groups

For an arbitrary group, G, we recall that G and e are normal subgroups, if these are the only ones we say the group is simple.

Definition 6.3.1. *We say that a group $G \neq \{e\}$ is* **simple** *provided that $N \lhd G$ implies $N = G$ or $N = \{e\}$.*

One of the most outstanding problems in group theory has been to give a complete classification of all finite simple groups. In other words, this is the program to discover all finite simple groups and to prove that there are no more to be found. This was recently accomplished through the efforts of many mathematicians. The end result of which is called by D. Gorenstein "The Enormous Theorem," as noted in the introduction to this chapter. Certainly one trivial family of finite simple groups would be all groups of prime order p, since by Lagrange's Theorem the only subgroups of such groups are of orders 1 and p (i.e., $\{e\}$ and the whole group). We shall presently determine a less trivial class of simple groups. There are other families of finite simple groups, but their determination is beyond the scope of this book. One of the easiest-to-state results in the proof of the "Enormous Theorem" was a tremendous result in itself due to W. Feit and J.G. Thompson (see [FT]). This result took a whole volume of the Pacific Journal of Mathematics (255

pages) to prove; moreover, it is considered to have provided a great deal of impetus to the study of the classification problem. What the Feit-Thompson Theorem (as it is called) basically says (later we shall phrase it in a different form) is that if G is a finite simple group and $|G|$ is not of prime order then G must be even. This settled an old conjecture of W. Burnside. In the words of D. Gorenstein, "The complexity of the proof of this easily understood statement (the Feit-Thompson Theorem) foreshadowed the extreme length of the complete classification of the simple groups."

Let us now turn to the main theorem of this section. First note that A_3 is simple, since $|A_3| = 3!/2 = 3$. As Example 6.1.3 shows, A_4 is not simple. It contains a normal subgroup of order 4, viz, the Klein 4-group, $V_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. However, we have the following result.

Theorem 6.3.2. *A_n is simple for $n \geq 5$.*

Proof: Let $N \lhd A_n$ where $n \geq 5$. We want to show according to Definition 6.3.1 that if $N \neq \{e\}$, then $N = A_n$. In order to do this, we first show that if N contains a single 3-cycle, i.e., a cycle of length 3, then $N = A_n$. Thus, say $(i,j,k) \in N$. Observe that $(2,i)(1,j) \in A_n$ if $i \neq 2$ and $j \neq 1$, and since $N \lhd A_n$,

$$(2,i)(1,j)(i,j,k)(2,i)^{-1}(1,j)^{-1} \in N,$$

i.e. $(2,1,k) \in N$ (where we have used the fact that disjoint cycles commute). Let $f = (1,2)(k,m)$ where $m \neq 1,2,k$ but otherwise m is an arbitrary integer less than or equal to n. (This can be done since $n \geq 5$.) Then $f \in A_n$ and since $N \lhd A_n$,

$$f(2,1,k)f^{-1} = (1,2,m) \in N$$

also $(1,2,k) = (2,1,k)^2 \in N$. Thus N contains all $(1,2,m)$ for $3 \leq m \leq n$. By exercise 7, Section 3.2, these cycles generate A_n, so $N = A_n$, and we are done. If $i = 2$ and $j = 1$, then immediately $(2,1,k) \in N$, and we proceed analogously. If $i = 2$ and $j \neq 1$, then $(2,j,k) \in N$, and so $(1,j)(k,j)(2,j,k)((1,j)(k,j))^{-1} = (2,k,1) = (1,2,k) \in N$. Then we proceed analogously. Finally if $i \neq 2$ and $j = 1$, a similar argument can be given (see exercise 1 for this section).

Thus to complete the proof, all we must do is show that if $N \lhd A_n$ and $N \neq \{e\}$, then N must contain a 3-cycle. To this end, choose an $f \in N$, $f \neq (1)$, such that f leaves fixed a maximal number of the numbers $1, 2, ..., n$. Suppose f were not a 3-cycle, then there are just two cases:

Case 1 f, in its representation as a product of disjoint cycles, contains a cycle of length ≥ 3 and so must map more than 3 integers into images distinct from their pre-images. In other words, f has a representation of the form

$$f = (123...)(...)....$$

Moreover, f can't be of the form $(1, 2, 3, m)$ since this is an odd permutation (WHY?) Thus f must map at least two integers > 3, say 4 and 5, into elements distinct from 4 and 5, respectively. Now let $g = (3, 4, 5) \in A_n$. Then $h = gfg^{-1} \in N$, but $h = gfg^{-1} = g(1, 2, 3, ...)g^{-1}g(...)g^{-1}...g^{-1}$ (WHY?), and so $h = (1, 2, 4...)(...)....$ Now if $j > 5$ and $f(j) = j$, then clearly $h(j) = j$ (since $h = gfg^{-1}$), so However, $f^{-1}h \in N$, and $f^{-1}h(1) = 1$. In other words, $f^{-1}h \in N$, $f^{-1}h \neq (1)$ (WHY?), and $f^{-1}h$ leaves fixed more elements than f. This contradicts the choice of f. Thus this case is eliminated.

Case 2 f, in its representation as a product of disjoint cycles, contains at least 2 distinct transpositions, i.e., f is of the form

$$f = (12)(34)...$$

Again, choose $g = (3, 4, 5) \in A_n$. Then as above

$$h = gfg^{-1} = (1, 2)(4, 5)....$$

As before $f^{-1}h \in N$, and $f^{-1}h(j) = j$ if $f(j) = j$ and $j > 5$. It is possible though here that f leaves 5 fixed, whereas $f^{-1}h(5) = 4$. However $f^{-1}h(1) = 1$ and $f^{-1}h(2) = 2$. Thus again $f^{-1}h \neq (1)$ (WHY?) and has more fixed points than f, a contradiction.

Since the two cases exhaust the possible representations for f other than f being a 3-cycle, we conclude that f must indeed be a 3-cycle, and by the first part of the proof, we than get $N = A_n$. $\square$

On the basis of this theorem and exercise 4 of Section 6.1, we can easily get further examples which show the converse of Lagrange's theorem is false. For example, $A_5 = 5!/2 = 60$, but A_5 has no subgroup of order 30 for such a subgroup would be normal, whereas we know A_5 is simple.

We conclude this section and chapter with a nice application of factor groups and of some of our earlier results (i.e., Theorem 6.3.4 obtained from Proposition 6.3.3). With this in mind, we first prove the following result.

Proposition 6.3.3. *: If G is a group such that $G/Z(G)$ is cyclic, then G is abelian.*

Proof: We will write $Z = Z(G)$, the center of G. We first remark that G/Z is defined since $Z \lhd G$ (WHY?). Now since G/Z is a cyclic group, let's write $G/Z = \langle aZ \rangle$ for $a \in G$. Since

$$G = \cup_{n\in\mathbb{Z}} a^n Z,$$

if g and h are any elements of G then $g \in a^k Z$ and $h \in a^m Z$ for integers k, m. Thus $g = a^k z_1$ and $h = a^m z_2$ where $z_1, z_2 \in Z$. Then

$$gh = (a^k z_1)(a^m z_2) = a^k a^m z_1 z_2 = (a^m z_2)(a^k z_1) = hg.$$

Hence G is abelian. □

We can now obtain our desired application, i.e.,

Theorem 6.3.4. *A group of order p^2 is abelian.*

Proof: Let G be a group such that $|G| = p^2$ and let $Z = Z(G)$ be the center of G. By Theorem 4.3.5, we know that Z is non-trivial. Thus from Lagrange's Theorem $|Z| = p$ or $= p^2$. If $|Z| = p^2$, then $G = Z = Z(G)$, and so G is abelian. On the other hand if $|Z| = p$, then we consider G/Z. Now $|G/Z| = p^2/p = p$. Thus by exercise 4 of Section 5.1, G/Z is cyclic. Hence G is again abelian by Proposition 6.3.3, and actually $|Z| = p^2$. □

Actually one can prove more and also show that there are precisely two non-isomorphic groups of order p^2, but we shall not go into these enumeration matters here.

6.3.1 Exercises

1. Suppose $N \lhd A_n$ for $n \geq 5$ and that $(i, j, k) \in N$ where $i \neq 2$ and $j = 1$, show as in the proof of Theorem 6.3.2 that this again implies that $N = A_n$.

2. Go through the proof of Theorem 6.3.2 and answer all the questions asked there.

3. Use the main result of this section, i.e., Theorem 6.3.2, to give another example, different from that in the text or in exercise 4 of Section 6.2, showing the converse of Lagrange's Theorem is false.

4. Let G be an abelian simple group. Prove $|G| = p$, p a prime. (It is *not* assumed initially that G is finite.)

5. Let G be a non-abelian group s.t. $|G| = p^3$. Prove $|Z(G)| = p$.

6. If $|G| = pq$, where p and q are not necessarily distinct primes, prove $|Z(G)| = 1$ or $= pq$.

Chapter 7

Homomorphisms

In this chapter, we consider a generalization of an isomorphism. In particular, we consider mappings on groups called homomorphisms which preserve the group operation. (They need not be 1-1 nor onto.) In the first section, we discuss several easy consequences of the definition of homomorphism. We also find that the important Fundamental Homomorphism Theorem is just a consequence of some of our previous work. Finally, in the second section we consider some special isomorphisms and homomorphisms.

7.1 Definition and Elementary Properties

We return to a consideration of mappings from one group to another.

Definition 7.1.1. *Let G_1 and G_2 be two groups (both denoted multiplicatively) and let $f : G_1 \to G_2$. The mapping f is called a* **homomorphism** *if $f(ab) = f(a)f(b)$ for all $a, b \in G_1$. If f is an onto homomorphism, i.e., $G_2 = f[G_1]$, then G_2 is called a* **homomorphic image** *of G_1.*

In words, a homomorphism is just a map from one group to another which preserves the operation. Let us consider two examples of homomorphisms: the first rather general, the second quite specific.

Example 7.1.2. *Let G be a group and $N \lhd G$. Consider the canonical (or natural) mapping κ of G onto G/N given by $\kappa(a) = aN$ for all $a \in G$. κ is clearly onto G/N, and*

$$\kappa(ab) = abN = (aN)(bN) = \kappa(a)\kappa(b).$$

Thus G/N is a homomorphic image of G. This example shows that a factor group of a group is always a homomorphic image of the group. □

Example 7.1.3. *Let $G = \mathbb{C}^n$, as in Example 2.1.14. Map $\mathbb{C}^n$ to itself by*

$$f : \mathbb{C}^n \to \mathbb{C}^n$$

where $f(\alpha_1, ..., \alpha_n) = (\alpha_1, 0, ..., 0)$. It is easy to see that f is a homomorphism of $\mathbb{C}^n$ into itself (see exercise 1 for this section). □

We now consider some general properties of homomorphisms.

Theorem 7.1.4. *Let $f : G_1 \to G_2$ be a homomorphism. Then $f[G_1] \leq G_2$.*

Proof: Let e be the identity of G_1. We have $f(e) \in f[G_1]$, so $f[G_1] \neq \emptyset$. Let $f(a), f(b) \in f[G_1]$. Then $f(a)f(b) = f(ab) \in f[G_1]$. But $f(e) = f(e \cdot e) = f(e)f(e)$ which implies by cancellation that $f(e)$ is the identity element of G_2. Finally, $f(a)f(a^{-1}) = f(aa^{-1}) = f(e)$, so $f(a)^{-1} = f(a^{-1}) \in f[G_1]$. This shows that $f[G_1] \leq G_2$ by Definition 2.2.3. □

Let us remark that in the above proof we showed two other important properties of a homomorphism. They are:

- $f(e_1) = e_2$, where e_i is the identity of G_i $(i = 1, 2)$,
- $f(a^{-1}) = f(a)^{-1}$, for every $a \in G_1$.

Definition 7.1.5. *Let $f : G_1 \to G_2$ be a homomorphism, and let e designate the identity of G_1 as well as of G_2. Let $K = \{a \in G_1 \mid f(a) = e\}$. The set K is called the* **kernel** *of f. We write $Ker(f)$.*

We shall presently show that if $f : G_1 \to G_2$ is a homomorphism then $Ker(f) \lhd G_1$, but first we note the following basic property.

Theorem 7.1.6. *f is 1-1 if and only if $Ker(f) = \{e\}$.*

Proof: If f is 1-1, since $f(e) = e$, e can be the only element which maps to e, i.e., $Ker(f) = \{e\}$. Conversely, if $Ker(f) = \{e\}$, then if $f(a) = f(b)$, we have $f(a^{-1}b) = f(a^{-1})f(b) = f(a)^{-1}f(b) = e$ since $f(a) = f(b)$. Thus $a^{-1}b \in K = \{e\}$. So $a^{-1}b = e$, and $a = b$. □

Theorem 7.1.7. *If $f : G_1 \to G_2$ is a homomorphism then $Ker(f) \lhd G_1$.*

Proof: We have already seen that $e \in Ker(f)$. If $a, b \in Ker(f)$, then $f(a) = e$ and $f(b) = e$, so $f(ab) = f(a)f(b) = e$; hence $ab \in Ker(f)$. Also $f(a^{-1}) = f(a)^{-1} = e^{-1} = e$, i.e., if $a \in Ker(f)$, then $a^{-1} \in Ker(f)$. We have so far shown that $Ker(f) \leq G_1$. To see that it is normal, suppose $k \in Ker(f)$ and $a \in G$. Then $f(aka^{-1}) = f(a)f(k)f(a^{-1}) = f(a)ef(a)^{-1} = e$. Therefore $k \in Ker(f)$ implies that $aka^{-1} \in Ker(f)$. This says $aKer(f)a^{-1} \subset Ker(f)$ for all $a \in G_1$. This is sufficient to show $Ker(f) \lhd G$, according to Proposition 6.1.4. □

In the case of the canonical map $\kappa : G \to G/N$ (see Example 7.1.2), $\kappa(a) = N$ (the identity element of G/N) if and only if $aN = N$ if and only if $a \in N$. Thus $Ker(\kappa) = N$.

We observe (see exercise 2 for this section) that if G_1, G_2, G_3 are groups and if $f_1 : G_1 \to G_2$ and $f_2 : G_2 \to G_3$ are homomorphisms then $f_2 f_1 : G_1 \to G_3$ is a homomorphism.

Suppose again that $f : G_1 \to G_2$ is a homomorphism with $K = Ker(f)$. We observed, for general mappings in section 1.1 that there is associated with f a factorization

$$G_1 \xrightarrow{\kappa} \overline{G_1} \xrightarrow{g} f[G_1] \xrightarrow{i} G_2,$$

such that $f = ig\kappa$, κ is onto, g is 1-1 and onto, while i is an injection mapping. Also recall that was a set of equivalence classes, determined by the equivalence relation: $a \sim b$ if and only if $f(a) = f(b)$. Consider the equivalence class of $a \in G_1$, namely $[a]$. Now $b \in [a]$ if and only if $b \sim a$ if and only if $f(a) = f(b)$ if and only if $f(a^{-1}b) = e$ if and only if $a^{-1}b \in K$ if and only if $b \in aK$. Thus $[a] = aK$ and $\overline{G_1}$ is precisely G_1/K and κ is the canonical homomorphism. Thus we have

$$G_1 \xrightarrow{\kappa} G_1/K \xrightarrow{g} f[G_1] \xrightarrow{i} G_2.$$

Now i, being an injection mapping, is an isomorphism of $f[G_1]$ into G_2. Finally we claim that g is an isomorphism of G_1/K onto $f[G_1]$. We know, in general that g is 1-1 and onto, thus all that needs to be shown is that g preserves the operation. Now $g(aK) = f(a)$, recalling the definition of g, so

$$g(aKbK) = g(abK) = f(ab) = f(a)f(b) = g(aK)g(bK).$$

Consequently, we have $f[G_1] \cong G_1/Ker(f)$.

We have thus established the fundamental result stated below.

Theorem 7.1.8. *(Fundamental Homomorphism Theorem (FHT))*

(I) If $N \lhd G$, a group, then G/N is a homomorphic image of G.

(II) If $f : G_1 \to G_2$ is a homomorphism, then $G_1/Ker(f) \cong f[G_1]$. In particular, if G_2 is a homomorphic image of G_1, then $G_1/Ker(f) \cong G_2$.

We note that the significance of this theorem is that it relates two seemingly unrelated concepts, i.e., concepts of factor group and homomorphic image. In particular, the FHT basically says that these two concepts coincide.

Example 7.1.9. *Let $f : \mathbb{Z}_6 \to \mathbb{Z}_3$ defined by $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$. It is not hard to verify that f is a homomorphism of $\mathbb{Z}_6$ onto $\mathbb{Z}_3$. $Ker(f) = \{0, [3]\}$ is the subgroup of $\mathbb{Z}_6$ generated by $[3]$, i.e., $\langle [3] \rangle$. (Here $[a]$ is in the notation of Exercise # 4 in §4.3.) FHT implies $\mathbb{Z}_6/\langle [3] \rangle \cong \mathbb{Z}_3$. We note that this example could also have been given as follows: Let $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ defined by $f(i + 6\mathbb{Z}) = i + 3\mathbb{Z}$ for any $i \in \mathbb{Z}$. The reader should verify again that this is a homomorphism, find its kernel and state the conclusion of FHT in this case.* □

7.1.1 Exercises

1. Prove that the map in Example 7.1.3 is a homomorphism.

2. Let G_1, G_2, G_3 be groups. Suppose $f_1 : G_1 \to G_2$ and $f_2 : G_2 \to G_3$ are homomorphisms. Then show $f_2 f_1 : G_1 \to G_3$ is also a homomorphism.

3. Verify that the mapping defined in Example 7.1.9 is a homomorphism. In the second case, i.e., the map $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, show f is well-defined, f is a hom, find $Ker(f)$, and state the conclusion of the FHT for this f.

4. Verify that $f : \mathbb{R} \to \mathbb{C}$ defined by $f(x) = \cos(2\pi x) + i \sin(2\pi x)$ $(= e^{2\pi i x})$ is a homomorphism of the additive group of $\mathbb{R}$ onto the group of all complex numbers of absolute value 1. (Recall if $z = a + bi$, $|z| = \sqrt{a^2 + b^2}$.) What is $Ker(f)$? State the conclusion of the FHT for this map.

7.2 Special Homomorphisms and Isomorphisms

We conclude this chapter with some considerations of special homomorphisms and isomorphisms. First we define the notion of an endomorphism. A homomorphism

$$f : G \to G$$

of a group into itself is called an **endomorphism**. An isomorphism of a group G onto itself is called an **automorphism**. For example, the mapping of the additive group of complex numbers $\mathbb{C}$, given by $z \longmapsto \overline{z}$, the complex conjugate, is an automorphism of $\mathbb{C}$ (see exercise 1 for this section).

Let G be a given group. We denote by $Aut(G)$ the set of all automorphisms of G. This set is a group with respect to the binary operation of composition of mappings: For clearly $1_G \in Aut(G)$ and is the identity element. The associative law is true for mappings with respect to composition and if $f \in Aut(G)$ then f^{-1} exists and $f^{-1} \in Aut(G)$ since

$$\begin{aligned} f^{-1}(ab) &= f^{-1}(ff^{-1}(a)ff^{-1}(b)) \\ &= f^{-1}(f(f^{-1}(a))f(f^{-1}(b))) \\ &= f^{-1}(a)f^{-1}(b), \end{aligned}$$

since composition is represented by juxtaposition. Is this sufficient to show Aut(G) is a group with respect to composition? WHY or WHY NOT? (See exercise 3 for this section.)

Now we consider special kinds of automorphisms of a group G. Let $a \in G$, and consider the mapping $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$. We contend that $\phi_a \in Aut(G)$. We leave it as an exercise to show ϕ_a is 1-1 and onto. We note $\phi_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y)$, and so ϕ_a is an automorphism of G. It is called the **inner automorphism** determined by a.

For future reference, we note here the following result.

Proposition 7.2.1. *Let G be a group, $H \leq G$, and $a \in G$. Then $aHa^{-1} \leq G$.*

Proof: Since the inner automorphism $\phi_a : G \to G$ is a homomorphism, we can apply Theorem 7.1.4 to imply that the image of H under a, i.e., $\phi_a[H] = aHa^{-1}$, is a subgroup of G. In words, Proposition 7.2.1 says that the conjugate of a subgroup is a subgroup. □

All elements of $Aut(G)$ (if there are any) which are not inner automorphisms are called outer automorphisms. Let us denote the set of all inner automorphisms of G by $Inn(G)$. We claim that $Inn(G) \lhd Aut(G)$. To show this, we consider the mapping ψ of G into $Aut(G)$ given by $a \longmapsto \phi_a$, i.e.,

$$\psi(a) = \phi_a. \tag{7.1}$$

It is obvious that ϕ_a is onto $Inn(G)$. Also $\psi(ab)\phi_{ab}$, but

$$\begin{aligned}\phi_a\phi_(x) &= \phi_a(\phi_b(x)) \\ &= \phi_a(bxb^{-1}) \\ &= a(bxb^{-1})a^{-1} \\ &= (ab)xb^{-1}a^{-1} \\ &= (ab)x(ab)^{-1} \\ &\phi_{ab}(x).\end{aligned}$$

Thus $\phi_{ab} = \phi_a\phi_b$ so the mapping ψ preserves the operation, i.e., ψ is a homomorphism. Theorem 7.1.4 implies that the image at $Inn(G) = \psi[G]$ is a subgroup of $Aut(G)$. Now let $f \in Aut(G)$. Then

$$\begin{aligned}f\phi_a f^{-1}(x) &= f(af^{-1}(x)a^{-1}) \\ &= f(a)f(f^{-1}(x)f(a)^{-1}) \\ &= f(a)xf(a)^{-1} \\ &= \phi_{f(a)}(x),\end{aligned}$$

i.e., $f\phi_a f^{-1} = \phi_{f(a)} \in Inn(G)$. Thus $Inn(G) \lhd Aut(G)$.

Finally, let us consider the kernel, $Ker(\psi)$, of the homomorphism given in (7.1). Let $K = Ker(\psi)$. Now K consists of those and only those elements $a \in G$ such that $\phi_a = 1_G$, i.e., $\phi_a(x) = 1_G(x) = x$, for all $x \in G$. In other words,

$$\phi_a(x) = axa^{-1} = x,$$

for all $x \in G$. Thus $K = Z(G)$, the center of G. Thus the FHT (Theorem 7.1.8) implies that

$$Inn(G) \cong G/Z(G).$$

We have therefore established the following result.

Theorem 7.2.2. *The set $Inn(G)$ of all inner automorphisms of a group G is a normal subgroup of the group $Aut(G)$ of all automorphisms of G. Moreover, $Inn(G) \cong G/Z(G)$.*

7.2.1 Exercises

1. Prove that the map $z \longmapsto \overline{z}$, where $z = a + bi$, $\overline{z} = a - ib$ is an automorphism of $\mathbb{C}$ under $+$.

2. In the text, we did not show that $Aut(G)$ was closed with respect to composition, i.e., that composition is a binary operation on $Aut(G)$. Show it. (You may use the result of exercise 2 for Section 7.1.)

3. For an arbitrary group G, let $a \in G$ and define $\phi_a(x) = axa^{-1}$ for all $x \in G$. Show ϕ_a is a 1-1 and onto map of G onto G. Finally show that ϕ_a preserves the group operation. This exercise shows that $\phi_a \in Aut(G)$ (ϕ_a is the inner automorphism determined by a.)

4. Show that if G is a group with trivial center ($Z(G) = \{e\}$), then its group of automorphisms, $Aut(G)$, is also a group with trivial center.

   (HINT: Let $f \in Z(Aut(G))$. For any $x \in G$, let $\phi_x \in Inn(G)$. Then $f\phi_x = \phi_x f$ (Why?). Use this to show that for any $y \in G$, $x^{-1}f(x) \in C_G(f(y))$. Infer the result from this.)

Chapter 8

Solvable Groups, Double Cosets and Isomorphism Theorems

We shall consider in this chapter a number of concepts which play an extremely important role in algebra in general. Here, for the most part, the theorems established will be introductory, and will subsequently be used to establish much deeper theorems. We shall begin with a discussion of a special class of groups called solvable groups. Later, we shall return to such groups, and we shall then give an alternate characterization of them and prove more properties related to solvable groups. This name comes from the fact that solvable groups are used in a subject called Galois Theory (also a part of algebra but not treated here) to determine whether or not a polynomial equation is solvable in terms of taking $n - th$ roots; i.e., to determine whether or not a formula for the roots of a polynomial like the quadratic formula (case $n = 2$) can be found. If such a formula can be found, we say the polynomial equation is solvable by radicals. It turns out that not all polynomial equations of degree ≥ 5 are solvable are by radicals. The reason for this is that the symmetric group Sn is not a solvable group for $n \geq 5$ (cf. Theorem 6.3.2).

We also discuss in the final section the so called correspondence theorem and two of the three isomorphism theorems. These theorems describe relationships between factor groups, normal subgroups, and homomorphisms. The reader should be cautioned that neither the numbering nor the content of these theorems is standard. So, for example, what is called the second isomorphism theorem here may be called the third isomorphism theorem in another text. Also some authors include what we have called the Funda-

mental Homomorphism Theorem (Theorem 7.1.8) as one of the isomorphism theorems. It should also be pointed out that analogs of these theorems are true for almost every type of algebraic system. (Examples where these hold other than groups, which the reader may be familiar with, are vector spaces.)

8.1 Commutators and solvable groups

We begin our discussion with the following basic notion.

Definition 8.1.1. *Let G be a group and let $a, b \in G$. The product $aba^{-1}b^{-1}$ is called the* **commutator** *of a and b. We write $[a, b] = aba^{-1}b^{-1}$.*

Clearly $[a, b] = e$ if and only if a and b commute.

Definition 8.1.2. *Let G' be the subgroup of G which is generated by the set of all commutators of elements of G, i.e., $G' = gp(\{[x, y] \mid x, y \in G\})$. G is called the* **commutator** *(or* **derived***)* **subgroup** *of G.*

If we recall our discussion on the subgroup generated by a subset of a group G, then we know that G' consists of all finite products of commutators and inverses of commutators. (See Proposition 5.1.1.) However, the inverse of a commutator is once again a commutator (see exercise 1 for this section). It then follows that G is precisely the set of all finite products of commutators, i.e., G is the set of all elements of the form

$$h_1 h_2 ... h_n$$

where each h_i is a commutator of elements of G.

The following proposition shows that the commutator subgroup is always normal.

Proposition 8.1.3. *If G is a group, then $G' \lhd G$.*

Proof: If $h = [a, b]$ for $a, b \in G$, and $x \in G$, $xhx^{-1} = [xax^{-1}, xbx^{-1}]$ is again a commutator of elements of G. Now from our previous comments, an arbitrary element of G' has the form $h_1 h_2 ... h_n$, where each h_i is a commutator. Thus $x(h_1 h_2 ... h_n)x^{-1} = (xh_1x^{-1})(xh_2x^{-1})...(xh_nx^{-1})$ and since by the above each xh_ix^{-1} is a commutator $x(h_1 h_2 ... h_n)x^{-1} \in G'$. Using Proposition 6.1.4, we have proven $G \lhd G$. $\square$

We next contend that the factor group G/G' is an abelian group and that actually G' is the smallest normal subgroup that enjoys this property. (Note that if G is a finite group and if $|N| > |G'|$, where $N \lhd G$ such that G/N is abelian, then $|G/G'| > |G/N|$, so we are actually discovering the "largest" abelian homomorphic image of G.)

Theorem 8.1.4. *G/G' is an abelian group. Moreover, if $N \lhd G$ such that G/N is abelian, then $G' \subset N$.*

Proof: In order to establish the first part of the theorem, let aG' and bG' be any two elements of G/G'. Then

$$\begin{aligned}[aG', bG'] &= aG' \cdot bG'(aG')^{-1}(bG')^{-1} \\ &= aG' \cdot bG'a^{-1}G' \cdot b^{-1}G' \\ &= aba^{-1}b^{-1}G' \\ &= G',\end{aligned}$$

since $[a, b] \in G'$. In other words, any two elements of G/G' commute (recall that in the factor group G/G', G' functions as the identity element). Hence G/G' is abelian.

Next let $N \lhd G$. If N does not contain G', then N certainly cannot contain all commutators of elements of G (recall that the group generated by a set is the smallest subgroup containing that set - see §5.1). Thus let $a, b \in G$ be such that $[a, b] \notin N$. Then $[aN, bN] = aba^{-1}b^{-1}N = [a, b]N \neq N$. Hence G/N is non-abelian. Taking the contrapositive completes the proof. □

In general, we know (see exercise 8 for Section 6.1) that a normal subgroup of a normal subgroup need not be normal in the whole group. However, the following theorem shows that in the special case of the commutator subgroup of a normal subgroup, we can state that this is normal in the entire group.

Theorem 8.1.5. *Let $N \lhd G$, a group, and let N' be the commutator subgroup of N. Then $N' \lhd G$.*

Proof: Let $c = [a, b]$ where $a, b \in N$. Then for an arbitrary $x \in G$, we have

$$\begin{aligned}xcx^{-1} &= xaba^{-1}b^{-1}x^{-1} \\ &= (xax^{-1})(xbx^{-1})(xa^{-1}x^{-1})(xb^{-1}x^{-1}) \\ &= (xax^{-1})(xbx^{-1})(xax^{-1})^{-1}(xbx^{-1})^{-1} \\ &= [xax^{-1}, xbx^{-1}].\end{aligned}$$

Since $N \lhd G$, xax^{-1} and $xbx^{-1} \in N$, we have $xcx^{-1} \in N$, where c was an arbitrary commutator of elements of N. It follows directly from this that $N \lhd G$ (WHY?). $\square$

We consider next the following sequence of subgroups of an arbitrary group G:

$$... \subset G''' \subset G'' \subset G' \subset G, \tag{8.1}$$

where G'' is the commutator subgroup of G', G''' is the commutator subgroup of G'', etc.

Definition 8.1.6. *If the above sequence of subgroups of a group G given in (8.1) contains the trivial subgroup, i.e., $\{e\}$, then the group G is called* **solvable**.

If G is abelian, then $G = \{e\}$, and so an abelian group is solvable. The converse is false, e.g., S_3 can be shown to be solvable (see exercise 2 for this section), but of course S_3 is non-abelian. We also observe that A_n for $n \geq 5$ is not solvable. We have $A_n' = A_n$, for $n \geq 5$, since by Theorem 6.3.2 we know that A_n is simple (and non- abelian) for $n \geq 5$. We mention in passing that the Feit-Thompson Theorem alluded to earlier (see the beginning of Section 6.3) states: Any group of odd order is solvable.

8.1.1 Exercises

1. Prove that the inverse of a commutator is a commutator.

2. Let G be a group and G' be its commutator subgroup. Prove: G is abelian if and only if $G' = \{e\}$.

3. Write the element $(1, 2, 3) \in S_3$ as a commutator of elements of S_3.

4. We can define the sequence of subgroups, called the **derived series**, inductively as follows:

   $$G^{(n+1)} \subset G^{(n)} \subset ... \subset G'' \subset G' \subset G, \tag{8.2}$$

   where $G' = G^{(1)}$ is the commutator subgroup of G, and $G^{(i+1)}$ is the commutator subgroup of $G^{(i)}$, for $i > 0$. Prove that every term in the derived series, (8.2) above, is normal in G. (HINT: Theorem 8.1.5.)

5. Find G' if $G = S_3$. Prove that S_3 is solvable. (HINT: A_3.)

6. Prove that S_n is not solvable for all $n \geq 5$. (What do you think about S_4?)

8.2 Double cosets

We turn now to another important decomposition of an arbitrary group G into disjoint complexes. Such decompositions will play an important role in our later considerations of the Sylow Theorems.

Let G be an arbitrary group and let H_1 and H_2 be subgroups of G. For $a, b \in G$, we define

$$a \sim b \quad \text{if and only if} \quad h_1 a h_2 = b \tag{8.3}$$

where $h_1 \in H_1$ and $h_2 \in H_2$. We contend first of all that the relation given in (8.3) is an equivalence relation on G. To see this, we note

1. (Reflexivity): $a \sim a$ since $eae = a$, where e is the identity element and $e \in H_1$ and $e \in H_2$ since $H_1 \leq G$, $H_2 \leq G$.

2. (Symmetry): $a \sim b$ implies there exist $h_1 \in H_1$ and $h_2 \in H_2$ such that $h_1 a h_2 = b$, but then $a = h_1^{-1} b h_2^{-1}$, so $b \sim a$ since $h_1^{-1} \in H_1$ and $h_2^{-1} \in H_2$.

3. (Transitivity): If $a \sim b$ and $b \sim c$, then there exist elements $h_1, h_1' \in H_1$ and $h_2, h_2' \in H_2$ such that

   $$h_1 a h_2 = b \quad \text{and} \quad h_1' a h_2' = c,$$

   whence

   $$h_1' h_1 a h_2' h_2 = c.$$

   Since $h_1 h_1' \in H_1$ and $h_2 h_2' \in H_2$, we have that $a \sim c$.

Thus $\sim$ given by (8.3) is indeed an equivalence relation on G. We next take a look at the equivalence classes.

Definition 8.2.1. *Let G be a group with subgroups H_1 and H_2 (not necessarily distinct). If $a \in G$, the complex $H_1 a H_2$ is called a* **double coset** *with respect to H_1 and H_2. By definition,*

$$H_1 a H_2 = \{h_1 a h_2 \in G \mid h_1 \in H_1, h_2 \in H_2\}.$$

For $a \in G$, the equivalence class $[a]$ of a as we recall, contains all $b \in G$ with $b \sim a$. By the definition given in (8.3), this means $b = h_1 a h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$. Thus $b \in H_1 a H_2$. As the above statements are all "if and only if", we see that $[a] = H_1 a H_2$, the double coset given in Definition 8.2.1. By our general theorem on equivalence relations, Theorem 1.1.4, we know that either

$$H_1 a H_2 = H_1 b H_2 \quad \text{or} \quad H_1 a H_2 \cap H_1 b H_2 = \emptyset$$

and

$$G = \coprod_a H_1 a H_2$$

where the union is taken over certain $a \in G$. The identity element e belongs to the complex $H_1 H_2$.

If $H_2 = \{e\}$, then we simply get the right coset decomposition of G with respect to H_1. If $H_1 = \{e\}$, then we have the left coset decomposition of G with respect to H_2. Thus the double coset decomposition of a group may be viewed as a generalization of the coset (right or left) decomposition of a group. However, the reader should be careful not to generalize all facts related to coset decompositions to the case of double coset decompositions. For example, we saw that any two cosets of a finite group have the same number of elements. We shall presently see that this is not the case with double cosets.

Let us consider the double coset $H_1 a H_2$. Clearly $H_1 a H_2$ contains all right cosets of the form $H_1 a h_2$, where $h_2 \in H_2$ and $H_1 a H_2$ contains all left cosets of the form $h_1 a H_2$ where $h_1 \in H_1$. We claim, as a matter of fact, that $H_1 a H_2$ is a union of right or left cosets of the above form. For suppose that

$$g H_2 \cap H_1 a H_2 \neq \emptyset.$$

Then there exist elements $h_2, h_2' \in H_2$ and $h_1 \in H_1$ such that

$$g h_2' = h_1 a h_2$$

or $g = h_1 a h_2 (h_2')^{-1}$. This implies that

$$g H_2 = h_1 a H_2,$$

and so $g H_2 \subset H_1 a H_2$. Since this shows that any left coset which has anything at all in common with $H_1 a H_2$, must be totally contained in $H_1 a H_2$, we have

$$H_1 a H_2 = \cup_{h_1} h_1 a H_2. \tag{8.4}$$

Similarly, it can be shown that

$$H_1aH_2 = \cup_{h_2} H_1ah_2. \tag{8.5}$$

Next, we wish to ascertain the number of left and right cosets in the double coset. Even though this number can be finite for an infinite double coset, we assume $|G| < \infty$. This is contained in

Theorem 8.2.2. *Let G be a finite group, let $H_1 \leq G$, $H_2 \leq G$, and let $a \in G$. Then*

(a) The number of right cosets of H_1 in H_1aH_2 is $[H_2 : H_2 \cap a^{-1}H_1a]$.

(b) The number of left cosets of H_2 in H_1aH_2 is $[a^{-1}H_1a : H_2 \cap a^{-1}H_1a]$.

Proof: We first note that $a^{-1}H_1a$ is a subgroup by Proposition 7.2.1. Consider the mapping of the double coset H_1aH_2 onto the complex $a^{-1}H_1aH_2$ given by $h_1ah_2 \longmapsto a^{-1}h_1ah_2$. It is easy to show that this map is well-defined, 1-1, and onto (see exercise 2 for this section). Thus $|H_1aH_2| = |a^{-1}H_1aH_2|$. But $a^{-1}H_1aH_2$ is the product of two subgroups $a^{-1}H_1a$ and H_2 so by the product theorem (Theorem 4.3.6),

$$|a^{-1}H_1a \cdot H_2| = \frac{|a^{-1}H_1a||H_2|}{|a^{-1}H_1a \cap H_2|}.$$

Now according to (8.4), the number of left cosets of H_2 in H_1aH_2 is $|H_1aH_2|/|H_2|$. Thus the number of left cosets of H_2 in H_1aH_2 is

$$\frac{|a^{-1}H_1a|}{|a^{-1}H_1a \cap H_2|} = [a^{-1}H_1a : a^{-1}H_1a \cdot H_2].$$

This establishes part (b) of the theorem. A similar argument establishes part (a) (this is left as an exercise). □

Under the same hypotheses as in Theorem 8.2.2, we use the notation $\#(H_1aH_2)$ to be the number of right cosets of H_1 in H_1aH_2 times $|H_1|$ (note from (8.5) that $\#(H_1aH_2) = |H_1aH_2|$). Thus Theorem 8.2.2 implies that

$$\#(H_1aH_2) = \frac{|H_2|}{|a^{-1}H_1a \cap H_2|} \cdot |H_1|.$$

This proves the following result.

Corollary 8.2.3. *Let G be a finite group and let $H_1 \leq G$, $H_2 \leq G$. If $G = \coprod_a H_1 a H_2$ (disjoint), then*

$$|G| = \sum_{j=1}^{n} \frac{|H_1||H_2|}{d_j} \tag{8.6}$$

where $d_j = |a_j^{-1} H_1 a_j \cap H_2|$.

8.2.1 Exercises

1. If $H_1 \leq G$, $H_2 \leq G$, G a group, and $a \in G$. Show that the double coset $H_1 a H_2$ is such that
$$H_1 a H_2 = \cap_{h_2} H_1 a h_2$$
where h_2 ranges over certain elements of H_2.

2. Let $H_1 \leq G$, $H_2 \leq G$, G a group, and $a \in G$. Let $\phi : H_1 a H_2 \to a^{-1} H_1 a H_2$ be defined by $\phi(h_1 a h_2) = a^{-1} h_1 a h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$. Show ϕ is well-defined, 1-1, and onto.

3. Following the proof of part (b) of Theorem 8.2.2, prove part (a), i.e., the number of right cosets of H_1 in $H_1 a H_2$ is $[H_2 : H_2 \cap a^{-1} H_1 a]$.

4. Find the double coset decomposition of S_3 with respect to $H_1 = H_2 = \{(1), (1,2)\}$.

5. Let G be a finite group and $H \leq G$ such that $N_G(H) = N(H) = H$, and any two distinct conjugate subgroups of H have only the identity element in common. Let N be the set of elements of G not contained in H nor in any of its conjugates, together with the identity. Show that $|H| \,|\, (|N| - 1)$.

   HINT: First use the given together with Lagrange's Theorem (in particular equation (4.8)) and Theorem 6.1.1 to show that $|N| = [G : H]$. Next decompose G into double cosets with respect to $N(H)$ and H and use equation (8.6). Now the identity $e \in G$ belongs to some double coset, so we may assume that $a_1 = e$, in the line before equation (8.6). Finally this implies that in (8.6) $d_1 = |H|$, but all the other $d_j = 1$. (Why?) Use the resulting relation to get the desired result.

8.3 Isomorphism theorems

Let G_1 and G_2 be two groups and let $f : G_1 \to G_2$ be a homomorphism of G_1 onto G_2. Furthermore, let $K = Ker(f)$. If $H_1 \leq G_1$, then (see Theorem 7.1.4) $f[H_1] \leq G_2$. If $H_2 \leq G_2$ then it is readily seen that $H = f^{-1}[H_2] \leq G_1$: For if $h_1, h_2 \in H$, then

$$f(h_1 h_2^{-1}) = f(g_1)f(h_2)^{-1} \in H_2,$$

so $h_1 h_2^{-1} \in H$ (see Chapter 2, exercise 2). Now since $e_2 \in H_2$, where e_2 designates the identity of G_2, we have $K = f^{-1}(e_2) \subset H = f^{-1}(H_2)$ and so $f(H) = H_2$, since f is onto and also using exercise 6(b) from Section 1.1. We therefore have shown that any subgroup H_2 of G_2 is of the form

$$H_2 = f(H), \tag{8.7}$$

where $H \leq G$ satisfies the condition that $Ker(f) \subset H$.

Finally let H be any subgroup of G_1 that contains the kernel, K. Then, of course,

$$H \subset H_1 = f^{-1}[f[H]].$$

(See exercise 6(a) of Section 1.1, where an equality is given if f is 1-1, but the above inclusion holds for any f. Why?) However since f is a homomorphism, we can show equality. For if $h_1 \in H_1$, then $f(h_1) \in f[H]$, so $f(h_1) = f(h)$, where $h \in H$. Thus $h_1 = hk$, where $k \in K$ (note $f(h^{-1}h_1) = e_2$), but $K \subset H$; whence $h_1 \in H$, and we have

$$f^{-1}[f[H]] = H. \tag{8.8}$$

With these results at our disposal, we are now in a position to prove the following result.

Theorem 8.3.1. *(Correspondence Theorem) Let $f : G_1 \to G_2$ be a homomorphism of the group G_1 onto the group G_2 with $K = Ker(f)$. Let $\{H_\alpha\}_{\alpha\in\Lambda}$ be the class of all subgroups of G_1 which contain K. The mapping (or correspondence)*

$$\Phi : H_\alpha \to f[H_\alpha]$$

is a 1-1 correspondence between the family $\{H_\alpha\}_{\alpha\in\Lambda}$ and the class of all subgroups of G_2. Moreover, $H_\alpha \lhd G_1$ if and only if $f(H_\alpha) = f[H_\alpha] \lhd G_2$.

Remark 8.3.2. *The condition that f is onto in this theorem is really no restriction because if $f : G_1 \to G_2$ is not onto, we just replace G_2 with $f[G_1]$.*

Proof: Part of the theorem has already been established in our remarks preceding the theorem. In particular, we have noted that the mapping Φ defined in the statement of the theorem is onto (see (8.7); i.e., Φ is the mapping of the family $\{H_\alpha\}_{\alpha\in\Lambda}$ to the family of all subgroups of G_2 given by

$$\Phi(H_\alpha) = f[H_\alpha].$$

We also note that each subgroup H is such that $K = Ker(f) \subset H_\alpha$, for all $\alpha \in \Lambda$. It is also clear that Φ is 1-1, for suppose $\Phi(H_\alpha) = \Phi(H_\beta)$, then $f[H_\alpha] = f[H_\beta]$. But from the remarks preceding the theorem in particular equation (8.8), we get

$$H_\alpha = f^{-1}[f[H_\alpha]] = f^{-1}[f[H_\beta]] = H_\beta.$$

Thus Φ is 1-1.

Finally, if $H_\alpha \subset G_1$ then since f is onto, for arbitrary $g_2 \in G_2$ there exists a $g_1 \in G_1$ such that $g_2 = f(g_1)$. Thus

$$g_2 f[H_\alpha] g_2^{-1} = f(g_1) f[H_\alpha] f(g_1)^{-1} = f[g_1 H_\alpha g_1^{-1}] = f[H_\alpha],$$

and so $f[H_\alpha] \subset G_2$. Conversely, if $f[H_\alpha] \subset G_2$, consider , where $g_1 \in G_1$. Then

$$f[g_1 H_\alpha g_1^{-1}] = f(g_1) f[H_\alpha] f(g_1)^{-1} = f[H_\alpha].$$

But then $\Phi(g_1 H_\alpha g_1^{-1}) = f[g_1 H_\alpha g_1^{-1}] = f[H_\alpha] = \Phi(H_\alpha)$ and since Φ is 1-1, we have $g_1 H_\alpha g_1^{-1} = H_\alpha$ and so $g_1 H_\alpha g_1^{-1} \lhd G_1$. We note that $g_1 H_\alpha g_1^{-1}$ is actually also one of the subgroups of G_1, which contains K because K is normal in G_1; for $K \subset H_\alpha$ implies $K = g_1 K g_1^{-1} \subset g_1 H_\alpha g_1^{-1}$. □

We apply Theorem 8.3.1 to the particular case of the canonical homomorphism (see Example 7.1.2) κ of a group G onto a factor group G/N, where N is, of course, a normal subgroup of G; i.e., $\kappa : G \to G/N$. We *claim* $Ker(\kappa) = N$. Indeed, recall the identity in G/N is N, so that $Ker(\kappa) = \{x \in G \mid \kappa(x) = N\} = \{x \in G \mid xN = N\} = \{x \in G \mid x \in N\} = N$, as claimed. Thus, by Theorem 8.3.1, any subgroup of G/N is of the form $\kappa[H]$ where $H \leq G$ and $N \subset H$. However,

$$\kappa[H] = \{hN \mid h \in H\} = H/N. \tag{8.9}$$

We have, therefore established the following result.

Corollary 8.3.3. *Let G be a group and let $N \lhd G$. Any subgroup of G/N is of the form H/N where H is a subgroup of G containing N. If H_1 and H_2 are two such subgroups of G, then $H_1 \neq H_2$ implies $H_1/N \neq H_2/N$. Moreover $H \lhd G$ if and only if $H/N \lhd G/N$.*

We continue to assume $f : G_1 \to G_2$ is a homomorphism of the group G_1 onto G_2 with kernel K. Let H be a normal subgroup of G that contains K and let $H_2 = f[H]$. Consider the mappings

$$G_1 \xrightarrow{f} G_2 \xrightarrow{\kappa} G_2/H_2,$$

where κ is the canonical map of G_2 onto G_2/H_2. Note $H_2 \lhd G_2$, by Theorem 8.3.1, since $H \lhd G_1$.

The composite map

$$\kappa f : G_1 \to G_2/H_2$$

is, of course, a homomorphism of G_1 onto G_2/H_2. Suppose $a \in G_1$ and $\kappa f(a) = H_2$, i.e., suppose $a \in Ker(\kappa f)$. Then $f(a) \in H_2$ and conversely. Hence, the $Ker(\kappa f)$ is (by equation (8.8)). Applying the FHT (Theorem 7.1.8), we have $G_2/H_2 \cong G_1/H$, where the isomorphism of G_1/H onto G_2/H_2 is given by $aH \longmapsto \kappa f(a) = f(a)H_2$. We summarize this in the following theorem, frequently called the **first isomorphism theorem**.

Theorem 8.3.4. *(First Isomorphism Theorem) Let $f : G_1 \to G_2$ be a homomorphism of the group G_1 onto the group G_2 with $Ker(f) = K$. Let $H \lhd G_1$ such that $K \subset H$. Then $f[H] \lhd G_2$, and*

$$G_1/H \cong f[G_1]/f[H],$$

by the mapping $aH \longmapsto f(a)f[H]$.

Again, we consider the special case of a group G and the canonical map κ onto a factor group G/N. If $H \lhd G$ and $N \subset H$, then

$$\kappa[H] = H_2 = H/N,$$

by equation (8.9). Thus Theorem 8.3.4 gives the following result.

Corollary 8.3.5. *Let G be a group and let H and N be normal subgroups of G such that $N \subset H$. Then*

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

Now assume that H_1 and H_2 are subgroups of a group G, and moreover that $H_2 \lhd G$. Then, in particular, $h_1H_2 = H_2h_1$ for all $h_1 \in H_1$, and so clearly $H_1H_2 = H_2H_1$. This implies by Theorem 4.2.1, that $H_1H_2 \leq G$. As we will have occasion to use this fact in the future, we state it here as the following result.

Proposition 8.3.6. *If $H_1 \leq G$, $H_2 \leq G$ and $H_2 \lhd G$, then $H_1H_2 \leq G$.*

(Of course $H_2 \subset H_1H_2$ and since $H_2 \lhd G$, we have $H_2 \leq H_1H_2$.) Next consider the mapping

$$\phi : H_1 \to H_1H_2/H_2$$

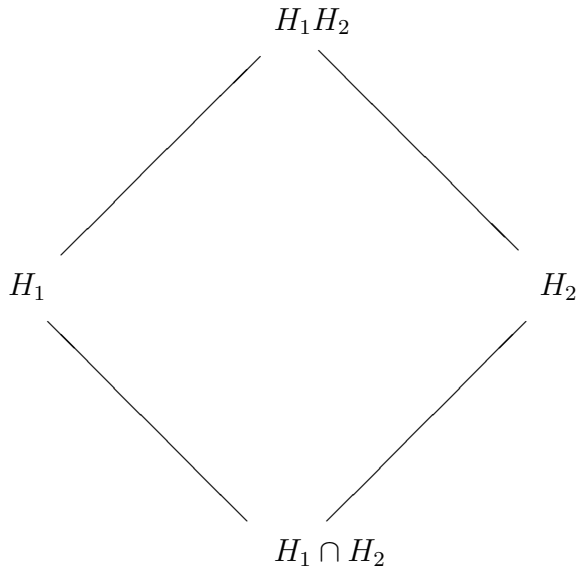
given by $\phi(h_1) = h_1H_2$, where $h_1 \in H_1$. This map is a homomorphism of H_1 into H_1H_2/H_2 (see exercise 1 for this section). We claim tht ϕ is, in addition, onto H_1H_2/H_2. Indeed, for any coset of H_2 in H_1H_2 is of the form $h_1h_2H_2 = h_1H_2$, where $h_1 \in H_1$ and $h_2 \in H_2$. The kernel, $Ker(\phi)$, consists of those $h_1 \in H_1$ such that $\phi(h_1) = h_1H_2 = H_2$, i.e., those elements of $H_1 \cap H_2$ or $Ker(\phi) = H_1 \cap H_2$. Thus applying the FHT (Theorem 7.1.8) to ϕ yields the **second fundamental isomorphism theorem**.

Theorem 8.3.7. *(Second Isomorphism Theorem) If H_1 and H_2 are subgroups of a group G and H_2 is also normal in G, then $H_1 \cap H_2 \lhd H_1$ and*

$$H_1H_2/H_2 \cong H_1/H_1 \cap H_2.$$

The isomorphism is given by the mapping $h_1(H_1 \cap H_2) \cong h_1H_2$, where $h_1 \in H_1$.

The second isomorphism theorem can probably best be remembered by the following mnemonic device:



Label the vertices of the figure as indicated, it being immaterial which side are writes H_1 or H_2 on. One then reads the isomorphism by reading "modulo the opposite sides." Should H_1 also be normal in G, then we obtain, symmetrically, $H_1H_2/H_1 \cong H_2/(H_1 \cap H_2)$, which may be read by reading "modulo" the other pair of opposite sides of the figure.

There is another fundamental theorem of isomorphism (the third isomorphism theorem) due to Zassenhaus, but we postpone a consideration of this theorem until we reach the section to which it is most relevant.

8.3.1 Exercises

1. Prove that if $H_1 \leq G$, $H_2 \leq G$, G a group, with $H_2 \lhd G$ then the map ϕ given by $\phi(h_1) = H_1H_2$, for $h_1 \in H_1$ is a homomorphism from H_1 into H_1H_2/H_2.

2. If $N \lhd G$, G a finite group, and if $[G : N]$ and $|N|$ are relatively prime, then show that N contains every subgroup of G whose order is a divisor of $|N|$.

   (HINT: Let $H \leq G$ such that $|H||N|$. Let $h \in H$ and consider $o(h)$ and $o(gN)$, for gN an element of G/N. Use this to prove $h \in N$.)

3. Let G be a group, H a subgroup of G, let C be a class of conjugate elements, and let $h \in H$ be fixed. Prove: $|Ha \cap C| = |Hah \cap C|$.

   (HINT: Define a map and prove it is 1-1 and onto.)

4. Let $H_1 \leq G$, $H_2 \leq G$, G a group, such that $H_2 \lhd H_1$; also let H be any subgroup of G. Let $H_3 = H_2 \cap H$ and $H_4 = H_1 \cap H$. Prove the following statements.

   (a) $H_3 \lhd H_4$.

   (b) H_4/H_3 is isomorphic to a subgroup of H_1/H_2. *(HINT: Use the second isomorphism theorem "appropriately".*

Chapter 9

Direct Products

In this chapter, we shall consider a process of constructing a new group from a finite number of given groups. Actually, the process (the external direct product) can be extended to the case where an infinite number of groups are given, but we shall not go into these matters here. At the same time, we shall consider the intimately related situation of decomposing a given group in a certain fashion (the internal direct product) into a product (with the usual meaning) of a finite number of subgroups. We shall investigate the relationship between this situation (internal direct product) and the first (external direct product) of our considerations. We shall see that up to an isomorphism the two concepts of direct product are indistinguishable. In the second section, we shall consider applications of this construction.

9.1 External and internal direct product

We proceed now to a precise consideration of the matters described above.

Definition 9.1.1. *Let G_1, G_2, ..., G_n be a finite collection of groups. We form the set $G = G_1 \times G_2 \times ... \times G_n$, the cartesian product of the sets G_1, G_2, ..., G_n. Thus G consists of all n-tuples of the form $(a_1, a_2, ..., a_n)$, where $a_i \in G_i$, $i = 1, 2, ..., n$. We introduce an operation which will make G into a group; viz, for any two n-tuple of G, we define*

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n).$$

The group G so constructed is called the **(external) direct product** *of the given groups. We denote this by $G_1 \times G_2 \times ... \times G_n$ (external).*

It is understood that each product a_ib_i is performed with the operation of G_i. It is now a straight-forward matter to show that, for this operation, the associative law is satisfied. Also the element $(e_1, e_2, ..., e_n)$, where e_i is the identity element of G_i, functions as the identity element of G. Finally, the inverse of the element $(a_1, a_2, ..., a_n)$ is the element $(a_1^{-1}, a_2 1^{-1}, ..., a_n 1^{-1})$ Hence G is a group with respect to the given operation. It is also clear that the following is true.

Proposition 9.1.2. *Let $G = G_1 \times G_2 \times ... \times G_n$.*

(a) If each G_i is finite and $|G_i| = r_i$, then

$$|G| = \prod_{i=1}^{n} r_i.$$

(b) If each G_i is abelian, then G is abelian.

Now we consider the following situation; which will subsequently be shown to be related.

Definition 9.1.3. *Let G be a given group and let $G_1, G_2, ..., G_n$ be normal subgroups of G such that*

$$G = G_1 G_2 ... G_n$$

(usual product of sets in a group) and $G_i \cap G_1 ... G_{i-1} G_{i+1} ... G_n = \{e\}$, for every $i = 1, 2, ..., n$. In this situation, we say that G is decomposed into the **(internal) direct product** *of the subgroups $G_1, G_2, ..., G_n$, and we shall write $G = G_1 \times G_2 \times ... \times G_n$ (internal).*

For the time being, we shall write in parenthesis after an expression of the form $G_1 \times G_2 \times ... \times G_n$ either "external" or "internal" to distinguish which of the two situations defined above actually prevails. After we have seen the inter-connection between these two concepts, it will be clear that we can drop this accompanying label without fear of confusion.

Our first theorem related to direct products is concerned with the latter situation, i.e., where G is the internal direct product of its subgroups, $G_1, G_2, ..., G_n$. We have

Theorem 9.1.4. *$G = G_1 \times G_2 \times ... \times G_n$ (internal) if and only if*

(1) $a_i a_j = a_j a_i$ for any $a_i \in G_i$ and any $a_j \in G_j$ where $i \neq j$, and

(2) Every element of G can be written uniquely in the form $a_1 a_2 ... a_n$ where $a_i \in G_i$.

Proof: Suppose first that $G = G_1 \times G_2 \times ... \times G_n$ (internal), and let $a_i \in G_i$ and $a_j \in G_j$ where $i \neq j$. Then the commutator $[a_i, a_j] = a_i a_j a_i^{-1} a_j^{-1} \in G_j$ since $a_i a_j a_i^{-1} \in G_j$ (since $G_j \lhd G$), and $a_j \in G_j$. However, $a_i^{-1} \in G_i$ and $a_j a_i a_j^{-1} \in G_i$ (since $G_i \lhd G$). Therefore $[a_i, a_j] \in G_i$, but $G_i \cap G_j = \{e\}$ (WHY?). Hence

$$[a_i, a_j] = a_i a_j a_i^{-1} a_j^{-1} = e,$$

which implies that $a_i a_j = a_j a_i$ and proves part (1). Next since $G = G_1 G_2 ... G_n$, any $a \in G$ can be written in the form $a = a_1 a_2 ... a_n$ where $a_i \in G_i$. If also $a = b_1 b_2 ... b_n$ where $b_i \in G_i$, then

$$a = a_1 a_2 ... a_n = b_1 b_2 ... b_n$$

and using the commutativity of elements in different G_i's, we get

$$b_i a_i^{-1} = b_1^{-1} a_1 ... b_{i-1}^{-1} a_{i-1} b_{i+1}^{-1} a_{i+1} ... b_n^{-1} a_n.$$

This in turn implies, since G is the internal direct product of the G_i, that $b_i a_i^{-1} = e$, or that $b_i = a_i$. But this can be done for every $i = 1, 2, ..., n$. This establishes part (2).

Conversely suppose that (1) and (2) hold. We *claim* each $G_i \lhd G$. Indeed, for if $g_i \in G_i$ and $a = a_1 a_2 ... a_n$, $a_j \in G_j$ is an arbitrary element of G, then

$$a g_i a^{-1} = a_1 a_2 ... a_n g_i a_n^{-1} ... a_2^{-1} a_1^{-1} = a_i g_i a_i^{-1}$$

since, by (1), a_j commutes with g_i for all $j > i$ and a_j commutes with g_i for all $j < i$. From (2), we have that $G = G_1 G_2 ... G_n$. Finally we note that a typical element of $G_1 ... G_{i-1} G_{i+1} ... G_n$ is of the form $a_1 a_2 ... a_{i-1} a_{i+1} ... a_n$, where $a_j \in G_j$. Suppose such an element is also in G_i and, hence, is equal to some $a_i \in G_i$:

$$a_i = a_1 a_2 ... a_{i-1} a_{i+1} ... a_n,$$

or

$$e ... e a_i e ... e = a_1 a_2 ... a_{i-1} e a_{i+1} ... a_n,$$

where e is the identity of G. By the uniqueness part of (2), we now have $a_i = e$, so

$$G_i \cap G_1 ... G_{i-1} G_{i+1} ... G_n = \{e\}.$$

We now proceed to establish two theorems which will show that, in the future, we need not distinguish between internal and external direct products.

Theorem 9.1.5. *Let $G = G_1 \times G_2 \times ... \times G_n$ (internal) and let $G_i \cong H_i$, $i = 1, 2, ..., n$. Form $H = H_1 \times H_2 \times ... \times H_n$ (external); then $G \cong H$.*

Proof: Let $f_i H_i \to G_i$ be an isomorphism of H_i onto G_i. We now define a mapping

$$f : H \to G,$$

by

$$f((a_1, a_2, ..., a_n)) = f_1(a_1)f_2(a_2)...f_n(a_n).$$

We *claim* that f is an isomorphism of H onto G.

First we observe that f is onto G: For any element g in G, we know is of the form $g = b_1 b_2 ... b_n$, where $b_i \in G_i$. Therefore, since each f_i is onto, there exist $a_i \in G_i$ so that $b_i = f(a_i)$, and so

$$g = b_1 b_2 ... b_n = f(a_1)f(a_2)...f(a_n) = f(a_1, a_2, ..., a_n),$$

where $(a_1, a_2, ..., a_n) \in H$. (We note that here we have dropped the double parentheses around the n-tuple.) Thus f is onto G.

Second, we note that f is a homomorphism, i.e., f preserves the group operation. For

$$f((a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n)) = f((a_1 b_1, a_2 b_2, ..., a_n b_n)) = f(a_1 b_1)f(a_2 b_2)...f(a_n b_n).$$

Since each f_i is a homomorphism, this is

$$= f(a_1)f(b_1)f(a_2)f(b_2)...f(a_n)f(b_n) = (f(a_1)f(a_2)...f(a_n))(f(b_1)f(b_2)...f(b_n)),$$

since elements from different factors of an internal direct product commute from Theorem 9.1.4 (1). Finally, we have from the definition of f that the above is equal to

$$f(a_1, a_2, ..., a_n)f(b_1, b_2, ..., b_n).$$

Lastly, to prove our claim, we must show that f is 1-1. To see this, suppose that $f(a_1, a_2, ..., a_n) = e$, i.e., $(a_1, a_2, ...a_n) \in Ker(f)$. Then $ee...e = f_1(a_1)f_2(a_2)...f_n(a_n)$, which by the uniqueness of representation, Theorem 9.1.5, implies that $f_i(a_i) = e$, for all i, $1 \leq i \leq n$. Since each f_i is 1-1, Theorem 7.1.6 implies that $a_i = e_i$ for all i, $1 \leq i \leq n$, where e_i is the identity of H_i. Therefore $(a_1, a_2, ..., a_n) = (e_1, e_2, ..., e_n)$ is the identity of H, i.e., $Ker(f)$ is trivial. Thus Theorem 7.1.6 implies that f is 1-1, which proves our claim (that f is an isomorphism). □

We note, in particular, taking $H_i = G_i$, $i = 1, 2, ..., n$, in Theorem 9.1.5 that if $G = G_1 \times G_2 \times ... \times G_n$ (internal), then forming $H = G_1 \times G_2 \times ... \times G_n$ (external) gives a group isomorphic to G.

Theorem 9.1.6. *Let $G = G_1 \times G_2 \times ... \times G_n$ (external); also let $H_i = \{(e_1, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n) \mid a_i \in G_i\}$, for $i = 1, 2, ..., n$. Then the $H_i \lhd G$ and $G = H_1 \times H_2 \times ... \times H_n$ (internal), and $H_i \cong G_i$, $i = 1, 2, ..., n$.*

Proof: Clearly each $H_i \leq G$ (Why?) and the mapping $G_i \to H_i$ given by $a_i \longmapsto (e_1, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n)$ is also clearly an isomorphism of G_i onto H_i. Moreover,

$$(b_1, b_2, ..., b_n)(e_1, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n)(b_1^{-1}, b_2^{-1}, ..., b_n^{-1}) \\ = (e_1, ..., e_{i-1}, b_i a_i b_i^{-1}, e_{i+1}, ..., e_n)$$

which shows $H_i \lhd G$. Now let $(a_1, a_2, ..., a_n)$ be an arbitrary element of G, we can write this in the form

$$(a_1, a_2, ..., a_n) = a_1' a_2' ... a_n',$$

where $a_i' = (e_1, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n) \in H_i$. Hence $G = H_1 H_2 ... H_n$. Finally any element of $H_1 ... H_{i-1} H_{i+1} ... H_n$ is of the form $(a_1, ..., a_{i-1}, e_i, a_{i+1}, ..., a_n)$, where $a_j \in H_j$. Thus it follows immediately that

$$Hi \cap (H_1 ... H_{i-1} H_{i+1} ... H_n) = \{e\},$$

$i = 1, ..., n$, where $e = (e_1, ..., e_n)$ is the identity of G. The result now follows from the definition of the internal direct product. □

From now on, we drop writing in parentheses after an expression $G_1 \times G_2 \times ... \times G_n$ either "external" or "internal". It should be clear from the context what is meant.

9.1.1 Exercises

1. Verify that the "componentwise" multiplication given in Definition 9.1.1 is actually a binary operation on $G_1 \times G_2 \times ... \times G_n$ (external). Also verify that this binary operation is associative.

2. Prove Proposition 9.1.2.

3. Verify the first two statements in the proof of Theorem 9.1.6; i.e.,

   (1) $H_1 \leq G$,

   (2) the map $a_i \longmapsto (e_1, ..., e_{i-1}, a_i, e_{i+1}, ..., e_n)$ is an isomorphism of G_i onto H_i.

4. Let $H_1 \lhd G$, $H_2 \lhd G$ be such that the canonical homomorphism $G \to G/H_2$ when restricted to H_1 gives an isomorphism of H_1 onto G/H_2. Then prove $G = H_1 \times H_2$ (internal).

5. Let G be an abelian group and $H \leq G$ such that G/H is an infinite cyclic group. Then prove that $G \cong H \times G/H$. (HINT: Use exercise 4 above.)

9.2 Applications and further properties

We wish to show, for our first application, that a cyclic group of order n can be written as a direct product of cyclic groups of prime power order.

Theorem 9.2.1. *If G is a cyclic group of order $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, where the p_i are distinct primes and $\alpha_i \geq 1$ are integers, then G is a direct product of cyclic groups of orders $p_i^{\alpha_i}$, $i = 1, 2, ..., k$.*

Proof: We designate by G_i the unique cyclic subgroup of order $p_i^{\alpha_i}$ of G (see Theorem 5.2.1) and let $H = G_1 G_2 ... G_k$. H is, of course a subgroup, since the G_i commute, because G is cyclic (and thus, of course, abelian). Also $G_i \subset H$ for every $i = 1, 2, ..., k$; therefore $p_i^{\alpha_i} | \, |H|$, for every $i = 1, 2, ..., k$. Thus $n = lcm(p_i^{\alpha_i})$ (see Theorem 1.2.11, generalized from 2 factors to k factors) and so $n | \, |H|$. Since $H \leq G$, $|H| \, |G| = n$ and so $n = |H|$. This proves $G = H = G_1 G_2 ... G_k$.

Next, we designate by H_i the cyclic subgroup of G of order $n_i = n/p_i^{\alpha_i}$, $i = 1, 2, ..., k$, and let $W_i = H_i \cap G_i$. Then $W_i \leq H_i$ and also $W_i \leq G_i$. Thus $|W_i| \, |n_i$ and $W_i | p_i^{\alpha_i}$, but $gcd(n_i, p_i^{\alpha_i}) = 1$, so $|W_i| = 1$. Hence $W_i = H_i \cap G_i = \{e\}$. However, $p_i^{\alpha_i} | \, |H_i|$ for all $j \neq i$. Thus $G_j \subset H_i$ for $j \neq i$ since H_i, being cyclic, contains a subgroup of order $p_j^{\alpha_j}$ and that subgroup must be $G_j \leq H_i \leq G$ by uniqueness (see Theorem 5.2.1), so $G_1 ... G_{i-1} G_{i+1} ... G_k \subset H_i$ and therefore

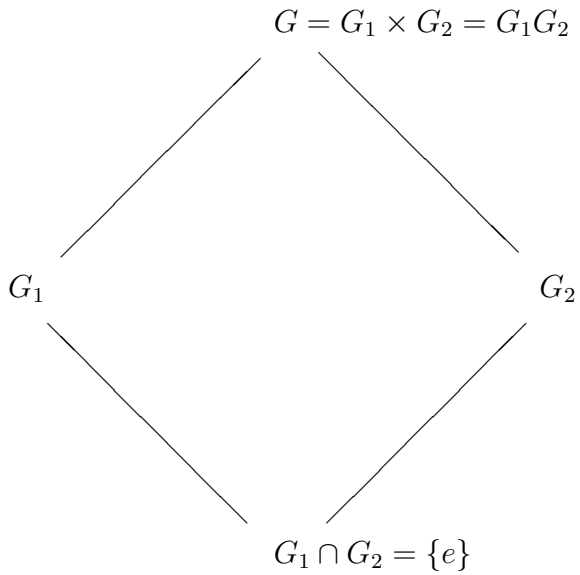
$$(G_1 ... G_{i-1} G_{i+1} ... G_k) \cap G_i = \{e\},$$

for all $i = 1, 2, ..., k$. □

We next prove an important property of direct products.

Theorem 9.2.2. *If $G = G_1 \times G_2$, then $G_2 \cong G/G_1$ and $G_1 \cong G/G_2$.*

Proof: The theorem is an immediate consequence of the second isomorphism theorem (Theorem 8.3.7). Namely, we have



and since G_1 and G_2 are both normal in G, Theorem 8.3.7 gives $G/G_1 \cong G_2/\{e\} \cong G_2$ and $G/G_2 \cong G_1$. $\square$

We have already seen one instance (Theorem 8.1.5) in which a normal subgroup N_1 of a normal subgroup N_2 of a group G is normal in G, i.e., $N_1 \lhd N_2$, $N_2 \lhd G$, and $N_1 \lhd G$. The following theorem gives another important case in which this true.

Theorem 9.2.3. *If H is a direct factor of the group G (i.e., $G = H \times N$, for some $N \leq G$), then every normal subgroup of H is normal in G.*

Proof: Let $W \lhd H$. Now by hypothesis, $G = H \times N$. Thus if g is an arbitrary element of G, then we can write g in the form $g = hn$, where $h \in H$ and $n \in N$. Now

$$gWg^{-1} = (hn)Wn^{-1}h^{-1} = hWh^{-1} = W,$$

where we have used the fact that elements of H and N commute (see Theorem 9.1.4). Since g was an arbitrary element of G, we see indeed that $W \lhd G$. $\square$

We continue with another application of direct products to cyclic groups.

Theorem 9.2.4. *Let C_m and C_n be cyclic groups of orders m and n, respectively. $G = C_m \times C_n$ is cyclic if and only if $gcd(m, n) = 1$.*

Proof: Suppose $gcd(m,n) > 1$. We shall show that G is not cyclic. Let p be a prime such that $p| \, | \, gcd(m,n)$, so $p|m$ and $p|n$. Thus C_m has a cyclic subgroup of order p and C_n has also a cyclic subgroup of order p (see Theorem 5.2.1), but $C_m \cap C_n = \{e\}$. Consequently, G has at least two cyclic subgroups of order p. This implies, by Theorem 5.2.1, that G is not cyclic.

Next suppose that $gcd(m,n) = 1$ and let $C_m = \langle a \rangle$ and $C_n = \langle b \rangle$. Then $ab \in G = C_m \times C_n$ and $o(ab) = mn$, for if we let $t = o(ab)$, then

$$(ab)^{mn} = a^{mn}b^{mn} = e$$

so $t|mn$. Since

$$e = (ab)^{mt} = a^{mt}b^{mt} = b^{mt},$$

so $n|mt$. But $gcd(m,n) = 1$, so $n|t$. Similarly, we can show that $m|t$ and, again, since $gcd(m,n) = 1$, we must have $lcm(m,n) = mn|t$. Thus $mn = t = o(ab)$. However, $|G| = mn$ so $G = \langle ab \rangle$. □

As our last application, we prove that the Euler ϕ-function is multiplicative, i.e., if $gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. Suppose C_m is a cyclic group of order m, and C_n is a cyclic group of order n, where $gcd(m,n) = 1$. Then $C_m \times C_n = C_{mn}$, is a cyclic group of order mn by Theorem 9.2.4. We know from our discussion of cyclic groups in Chapter 5 (in particular see Corollary 5.2.3) that C_m has $\phi(m)$ generators and that C_n has $\phi(n)$ generators. While C_{mn} has $\phi(mn)$ generators. However, it is easy to see (see exercise 2 for this section) that every generator of C_{mn} must be of the form (a,b) where a is a generator of C_m and b is a generator of C_n. Thus we have proven the following result.

Theorem 9.2.5. *If $m, n \in \mathbb{N}$ and $gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. In other words, ϕ is multiplicative.*

9.2.1 Exercises

1. In the proof of Theorem 9.2.4, we showed $n|t$. Show $m|t$ (where these letters have the meaning given there).

2. Let C_m be a cyclic group of order m and C_n be a cyclic group of order n where $gcd(m,n) = 1$. Prove that the generators of $C_{mn} = C_m \times C_n$ are precisely all elements of the form (a,b), where a is a generator of C_m and b is a generator of C_n. (HINT: Theorem 1.2.11.)

3. Let G be a finite abelian group of order $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, where the p_i are distinct primes. Prove that $G = G_1 \times G_2 \times ... \times G_k$, where G_i is the subgroup of G consisting of all elements whose order divides .

   HINT: Mimic the proof of Theorem 9.2.1.

Chapter 10

The Sylow Theorems

We have already observed (see statements after the proof of Theorem 6.2; also see Exercise 4 for Section 6.2) that the converse of Lagrange's theorem is false, i.e., if G is a finite group of order n and if $d|n$, then G need not contain a subgroup of order d. If d is a prime p or a power of a prime p^e, however, then we shall see that G must contain subgroups of that order. In particular, we shall see that if p^d is the highest power of p that divides n, than all subgroups of that order are actually conjugate, and we shall finally get a formula concerning the number of such subgroups. These theorems constitute the Sylow Theorems which, along with a few applications, will be the matter of concern of this chapter.

10.1 Existence of Sylow subgroups; the first Sylow Theorem

Definition 10.1.1. *Let G be a finite group with $|G| = n$ and let p be a prime such that $p^a|n$ but no higher power of p divides n. A subgroup of G of order p^a is called a p-Sylow subgroup.*

It is not at all obvious that a p-Sylow subgroup exists. It is our main concern in this section to show that for each $p|n$ that a p-Sylow subgroup exists. Note that P is a p-Sylow subgroup of G if and only if $G = p^r n$ where $p \not| n$ and $|P| = p^r$.

We first consider and prove a very special case of the end result we wish to obtain.

Theorem 10.1.2. *Let G be a finite abelian group and let p be a prime such that $p|\,||G|$. Then G contains at least one element of order p.*

Proof: The proof will proceed by induction on $|G|$. If $|G| = p$, a prime, then the theorem is clearly true. Thus suppose $|G| = n$, where n is composite and also suppose that the theorem has been proven for all groups whose order $< n$. Suppose p is a prime such that $p|n$. We need to show that G has an element of order p. We *claim* G contains a subgroup not equal to $\{e\}$ or to G itself. This is clear if G is cyclic (see Theorem 5.2.1). If G is not cyclic, let $a \in G$, $a \neq e$, the identity element of G. Then $\langle a\rangle$ is a proper subgroup of G. (Why?) Let H be a proper subgroup of G of maximal order. If $p|\,|H|$, then since $|H| < |G|$, we have by the induction hypothesis that there exists an $h \in H$ such that $o(h) = p$, but clearly $h \in G$, also. This proves our claim when $p|\,|H|$. If, however, $p \not|\,|H|$, then since H is a proper subgroup of G, there exists an element $a \in G - H$. Let K be the cyclic subgroup of G generated by a, i.e., $K = \langle a\rangle$. Now the product HK is a subgroup of G (by Theorem 4.2.1) since G is abelian. Also, $H \subset HK$ properly, i.e., $H \neq HK$, because $a \in HK$ but $a \in H$. However, H was a maximal proper subgroup. Thus it must be that $HK = G$. Then, by Theorem 4.3.6,

$$|G| = \frac{|H||K|}{|H \cap K|} = \frac{|H| \cdot o(a)}{d},$$

where $d = |H \cap \langle a\rangle$. Thus

$$d|G| = |H| \cdot o(a),$$

and since $p|\,|G|$, we must have that $p|\,|H|o(a)$. However, we have assumed $p \not|\,|H$, thus by the Corollary 1.2.10 we have $p|o(a)$. Let $o(a) = m$. Then $m = pk$, where $k \in \mathbb{N}$, and consider the element a^k. By Theorem 5.2.2,

$$o(a^k) = \frac{m}{gcd(m,k)} = m/k = p.$$

□

Thus if G is an abelian group and if $p|n$, then G contains a subgroup of order p; viz., the cyclic subgroup of order p generated by an element $a \in G$ of order p whose existence is guaranteed by Theorem 10.1.2.

We now proceed to the main result of this section, i.e., the first Sylow Theorem.

Theorem 10.1.3. *(Sylow I) Let G be a finite group and let $p \in G$, then G contains a p-Sylow subgroup (i.e., a p-Sylow subgroup exists).*

Proof: As in the preceding theorem, the proof will be given by induction on $|G|$. The theorem is clearly true if $|G| = 2$. Now let $|G| = n = p^a n'$, where $p \not| n'$. By hypothesis, $a > 0$. We next decompose G into conjugacy classes according to the discussion at the beginning of Section 4.1 and use the class equation, i.e., equation (4.8), to obtain

$$G = Z(G) \cup Cl(a_1) \cup Cl(a_2) \cup ... \cup Cl(a_t) \quad \text{(disjoint)} \tag{10.1}$$

where $Cl(a_i)$ designates a conjugacy class. Since the union is disjoint, we can write

$$n = |Z(G)| + k_1 + k_2 + ... + k_t,$$

where $k_j = |Cl(a_j)|$. By Theorem 4.3.4, $k_j = [G : CG(a_j)] = n/n_j$, where $n_j = CG(a_j)$. We return now to equation (10.1) and recall that the conjugacy classes, $Cl(a_j)$, listed (if there are any) are nontrivial, i.e., each $k_j > 1$. Let us suppose that some k_j is such that $p \not| k_j$, i.e., $gcd(k_j, p) = 1$. Since $n_j k_j = n$, we must have $n_j < n$. Moreover, $p^a | n_j$ since $p \not| k_j$. It follows by the induction hypothesis that the subgroup $CG(a_j)$ contains a p-Sylow subgroup and that therefore G contains a p-Sylow subgroup. Thus, in this case, the theorem has been established.

We may, thus, assume that for each j, $j = 1, 2, ..., t$, $p | k_j$. Thus

$$p^a n' = |Z(G)| + pr,$$

whence $p | |Z(G)|$. Since $Z(G)$ is an abelian group, we have by the preceding theorem that $Z(G)$, and therefore, G has an element, a, of order p. Now $\langle a \rangle \lhd G$ since $a \in Z(G)$ and $|\langle a \rangle| = p$. Hence $|G/\langle a \rangle| = p^{a-1} n'$, and so by the induction hypothesis $G/\langle a \rangle$ must contain a p-Sylow subgroup of order p^{a-1}. This p-Sylow subgroup must be of the form $P/\langle a \rangle$, where $P \leq G$ which contains $\langle a \rangle$ by the Corollary 8.3.3. Now

$$|P| = |P\langle a \rangle| \cdot |\langle a \rangle| p^{a-1} \cdot p = p^a,$$

and so P is a p-Sylow subgroup of G. □

On the basis of this theorem, we can now strengthen the result obtained in Theorem 10.1.2.

Theorem 10.1.4. *(Cauchy) If G is a finite group and if p is a prime such that $p|\,|G|$, then G contains at least one element of order p.*

Proof: Let P be a p-Sylow subgroup of G, and let $P = p^a$. If $e \neq a \in P$, then $o(a)|\,|P|$ implies $o(a) = p^b$, where $0 < b \leq a$. But then the cyclic group, $\langle a \rangle$, must have a (unique) subgroup of order p, say $\langle a^t \rangle$, by Theorem 5.2.1. Thus $a^t \in G$ and $o(at) = p$. $\square$

10.1.1 Exercises

1. Let G be a finite group and let $p|\,|G|$. Suppose P is a p-Sylow subgroup of G. Prove that any conjugate of P, gPg^{-1}, is also a p-Sylow subgroup of G.

2. Let G be a finite group and $N \lhd G$ such that $|N|$ is a power of a prime p. Prove that N is contained in every p-Sylow subgroup of G. *(HINT: Use Theorems 4.3.6 and Proposition 8.3.6.)*

3. Let G be a finite group and P be a p-Sylow subgroup of G. Prove that if $x \in N_G(P)$ and $o(x)$ is a power of p, then $x \in P$. *(HINT: Same as for exercise 2.)*

4. Let G be a finite group and P be a p-Sylow subgroup of G. Prove that P is the only p-Sylow subgroup of G contained in $N_G(P)$. *(HINT: Use exercise 3.)*

10.2 The second and third Sylow Theorems

We have seen that p-Sylow subgroup's exist. We now wish to show that any two p-Sylow subgroup's are conjugate. This is the content of the second Sylow Theorem.

Theorem 10.2.1. *(Sylow II) Let G be a finite group and p a prime such that $p|\,|G|$. Then all p-Sylow subgroup's of G are conjugate. In other words, if P_1 and P_2 are any two p-Sylow subgroups of G then there exists an $a \in G$ such that $P_1 = aP_2a^{-1}$.*

Proof: Let P_1 and P_2 be two p-Sylow subgroup's of G, where $|P_1| = |P_2| = p^a$. We now decompose G into double cosets with respect to P_1 and P_2 (see Section 8.2). Thus

$$G = P_1 a_1 P_2 \cup P_1 a_2 P_2 \cup ... \cup P_1 a_t P_2 \quad \text{(disjoint)}$$

and from equation (8.6)

$$|G| = \sum_{j=1}^{t} \frac{|P_1||P_2|}{d_j},$$

where $d_j = |P_2 \cap a_j^{-1} P_1 a_j|$. Hence if $|G| = p^a n'$, where $p \not| n''$, we have

$$p^a n' = \frac{p^a p^a}{d_1} + ... + \frac{p^a p^a}{d_t},$$

or

$$n' = \frac{p^a}{d_1} + ... + \frac{p^a}{d_t}. \tag{10.2}$$

Now $P_2 \cap a_j^{-1} P_1 a_j \leq P_2$, therefore $d_j | p^a$, so $d_j = p^b$, where $0 < b \leq a$. Thus each term on the right hand side of (10.2) is either 1 or a power of p. Since $p \not| n'$, it follows that at least one term on the right hand side of (10.2) must equal 1, say the k^{th} term. This means $d_k = p^a$ so $|P_2 \cap a_k^{-1} P_1 a_k| = p^a$. Whence $P_2 = P_2 \cap a_k^{-1} P_1 a_k \subset a_k^{-1} P_1 a_k$. Since both P_2 and $a_k^{-1} P_1 a_k$ have the same (finite) order and since one is contained in the other, they must be equal: $P_2 = a_k^{-1} P_1 a_k$. Hence the two p-Sylow subgroup's P_1 and P_2 are conjugate. □

We come now to the last of the three Sylow theorems. This one gives us information concerning the number of p-Sylow subgroup's. Let $n_p(G)$ designate the number of p-Sylow subgroup's of G

Theorem 10.2.2. *(Sylow III) Let G be a finite group and p a prime such that $p| |G|$. We have*

$$n_p(G) \equiv 1 (\mathrm{mod}\, p),$$

i.e., $n_p(G)$ is of the form $1 + pv$ where $v \in \mathbb{Z}$. (We may write n_p instead of $n_p(G)$ if it is clear which group G we are working in.)

Proof: Let P be a p-Sylow subgroup of G. Then by the second Sylow Theorem (Theorem 10.2.1) and by Theorem 6.1.1,

$$n_p(G) = [G : N_G(P)] = \frac{|G|}{n},$$

where $n = |N_G(P)|$. (From now on we drop the subscript G and just write $N(P)$ and also just write n_p.) Now $P \subset N(P)$ and $P \lhd N(P)$; $|P|\,|n$, i.e., $p^a|n$, where $p^a = |P|$, so

$$n = p^a n', \qquad \text{where } gcd(n,p) = 1,$$

since P is a p-Sylow subgroup of G and $N(P) \leq G$. We now decompose G into double cosets with respect to P and $N(P)$. Thus

$$G = Pa_1N(P) \cup Pa_2N(P) \cup ... \cup Pa_tN(P), \qquad \text{(disjoint)},$$

and using the numerical relation (8.6) yields

$$|G| = \frac{p^a n}{d_1} + ... + \frac{p^a n}{d_t}, \tag{10.3}$$

where $d_j = |N(P) \cap a_j^{-1}Pa_j|$. Now the identity, e, of G belongs to some double coset, and we may assume that, say $a_1 = e$. In this case, we have

$$Pa_1N(P) = PeN(P) = PN(P) = N(P),$$

hence, the first term on the right hand side of (10.3) becomes $\frac{p^a n}{d_1} = n$. Now cancelling n on both sides of (10.3) and recalling that $|G| = n[G : N(P)] = n \cdot n_p$, gives

$$n_p = 1 + \frac{p^a}{d_2} + ... + \frac{p^a}{d_t}. \tag{10.4}$$

Next we observe that $N(P) \cap a_j^{-1}Pa_j \subset a_j^{-1}Pa_j$ and since $|a_j^{-1}Pa_j| = p^a$, we must have $\frac{p^a}{d_j} = p^{b_j}$, where $0 \leq b_j \leq a$ and $j = 2, ..., t$. If we can show that each such $b_j > 0$, $(2 \leq j \leq t)$, then it will follow from (10.4) that n_p is indeed, of the form $1 + pv$. Hence suppose on the contrary that for some j, say $j = s$ $(2 \leq s \leq t)$, that $p^a = ds$. But

$$N(P) \cap a_s^{-1}Pa_s \subset a_s^{-1}Pa_s$$

and

$$|N(P) \cap a_s^{-1}Pa_s| = d_s = p^a,$$

so $N(P) \cap a_s^{-1}Pa_s = a_s^{-1}Pa_s$. But also $N(P) \cap a_s^{-1}Pa_s \subset N(P)$. Thus both P and $a_s^{-1}Pa_s$ are p-Sylow subgroup's of $N(P)$. Hence by the second Sylow Theorem (Theorem 10.2.1, with $N(P)$ now playing the role of G in that

theorem), they must be conjugate in $N(P)$. But $P \lhd N(P)$, so we must have that $a_s^{-1}Pa_s = P$. This means $a_s \in N(P)$, which implies that

$$Pa_sN(P) = PN(P) = N(P),$$

which contradicts the disjointness of the decomposition. Hence for $j = 2, ..., t$ every $b_j > 0$ and this as already observed, completes the proof. □

The third Sylow Theorem tells us that $n_p(G)$, the number of p-Sylow subgroup's, is of the form $1 + pv$. However, we know as was used in the proof that $n_p(G) = [G : N_G(P)]$ from Theorem 6.1.1. Thus $n_p(G) \mid |G|$. This proves the following fact.

Corollary 10.2.3. *Same hypothesis as in Theorem 10.2.2. Then* $n_p(G) \mid |G|$.

As pointed out above this is really a corollary of the proof of the third Sylow Theorem. The two facts that $n_p(G) \equiv 1 (\mathrm{mod}\, p)$ and $n_p(G) \mid |G|$ are extremely useful. A few of their applications will be seen in the examples of the next section.

For the final theorems of this section, we turn our attention to prime power groups.

Theorem 10.2.4. *Let G be a group of order p^n. Then G contains at least one normal subgroup of order p^m, for each m such that $0 \leq m \leq n$.*

Proof: The theorem is trivial for $n = 1$. We *claim* it is also true for $n = 2$. Indeed, by Theorem 6.3.4, any group of order p^2 is abelian. This together with Theorem 10.1.2 establishes the claim.

We proceed now by induction on n. Thus we assume the theorem is true for all groups G of order p^k where $1 \leq k < n$, where $n > 2$. Let G be a group of order p^n. Also let N be a normal subgroup of order p. N exists since $Z(G)$ is non-trivial (by Theorem 4.3.5) and is, of course, abelian. Thus again by Theorem 10.1.2, $Z(G)$ contains an element, say z, of order p. We can take $N = \langle z \rangle$ and so N is a normal subgroup of G of order p, since every subgroup of the center is normal in G (WHY?). But then G/N is of order p^{n-1}, and therefore, contains (by the induction hypothesis) normal subgroups of orders p^{m-1}, for $0 \leq m - 1 \leq n - 1$. These groups are of the form H/N, where $H \lhd G$ contains N (see the Corollary 8.3.3) and is of order p^m, $1 \leq m \leq n$, because $|H| = |N|[H : N] = |N| \cdot |N/H|$. □

We next introduce the concept of a p-group which generalizes the idea of groups of prime power order.

Definition 10.2.5. *A* p**-group** G *(where* p *is any prime) is a group in which the order of every element is some power of* p*.*

We observe that a p-group does not even have to be finite. But in the finite case, we have the following result.

Theorem 10.2.6. *G is a finite p-group if and only if $|G| = p^n$ for some $n \in \mathbb{N}$.*

Proof: We leave the "if" part as an exercise, i.e., if $|G| = p^n$, then G is a p-group. (See exercise 1 for this section.) Conversely, suppose that G is a finite p-group. We would like to show that $|G| = p^n$. If there were a prime $q \neq p$ such that $q \,|\, |G|$, then by Cauchy's Theorem (Theorem 10.1.4) G would contain at least one element of order q. This contradicts the fact that every element of G has order a power of p, i.e., that G is a p-group. Thus $|G| = p^n$. □

10.2.1 Exercises

1. Prove that if $|G| = p^n$, for some $n \in \mathbb{N}$, and p a prime, then G is a p-group.

2. Let G be a finite group. Prove that any $H \leq G$ such that H is a p-group (Note from Theorem 10.2.6 H is a prime power group, i.e., $|H| = p^n$.) is contained in at least one p-Sylow subgroup (p-Sylow subgroup are maximal p-subgroups in this sense).

   (HINT: Use a double coset decomposition similar to the arguments used in the proofs of the second and third Sylow Theorems, but this time decompose G with respect to H and a p-Sylow subgroup.)

3. Let G be a finite group.

   (a) Show that every subgroup H of G which contains the normalizer of a p-Sylow subgroup is its own normalizer.

   (HINT: Suppose $N_G(P) \subset H$, where P is a p-Sylow subgroup. Now P is a p-Sylow subgroup of H (Why?). Let $x \in N(H)$. We need to show $x \in H$ to be finished (Why?). Note first that xPx^{-1} is also in p-Sylow subgroup of H (Why?). Now use the second Sylow Theorem applied to the above Sylow subgroups of H. From this and the fact that $N_G(P) \subset H$ establish the desired result.)

(b) Use (a) to show that if P is a p-Sylow subgroup then $N(N(P)) = N(P)$.

4. Show that if a group has $1 + p$ Sylow subgroups of order p^a, then any 2 of these subgroups have just p^{a-1} elements in common.

   (HINT: Suppose P_1 and P_2 are any 2 p-Sylow subgroup's. Use an argument with double cosets decomposing the group G into double cosets with respect to P_1 and $N_G(P_2)$ like the argument given for the third Sylow Theorem 10.2.2. Finally, use the second Sylow theorem 10.2.1)

5. Show that if a group G has $1 + p$ Sylow subgroups of order p^a, then G contains p^{a+1} elements whose orders are divisors of p^a.

   (HINT: Use the result of exercise 4 above. Also you may assume that any two of the p-Sylow subgroup's of G intersect in the same subgroup of G.)

10.3 Applications

On the basis of the first Sylow Theorem, Theorem 10.1.3, and Theorem 10.2.4, we see that if G is a finite group and if $p^k | |G|$, then G must contain a subgroup of order p^k. One can actually show that, as in the case of Sylow p-groups, the number of such subgroups is of the form $1 + pt$, but we shall not prove this here.

We shall now consider a number of applications of the Sylow Theorems.

Example 10.3.1. *There is no simple group of order* 84. *Write* $84 = 2^2 \cdot 3 \cdot 7$. *If the* 7*-Sylow subgroup is not normal, then it has* $1 + 7v$ *conjugates where* $v \geq 1$ *and* $(1 + 7v)|2^2 \cdot 3 \cdot 7$. *Clearly* $1 + 7v \neq 7n$, *so the only possibilities are*

$$1 + 7v = 2, 2^2, 3, 2 \cdot 3, 2^2 \cdot 3,$$

all of which are clearly impossible (none of these are $\equiv 1 (\mathrm{mod}\ 7)$*). Hence the* 7*-Sylow subgroup is normal and therefore, any group of order 84 is not simple.*

Example 10.3.2. *There is no simple group of order* 12. *Write* $12 = 2^2 3$. *If the* 3*-Sylow subgroup, which is a cyclic group of order* 3, C_3, *is not normal, it has* $1 + 3v$ *conjugates where* $v \geq 1$ *and* $(1 + 3v)|12$. *Clearly the only possibility is* $v = 1$, *in which case* C_3 *has* 4 *conjugates. These groups have*

only the identity in common, and this accounts for $4 \cdot (3-1) = 8$ *nontrivial elements of* G*. This leaves then* 4 *elements of* G*, which must constitute a* 2*-Sylow subgroup of order* 4*, which of course only has the identity in common with any* 3*-Sylow subgroup. Thus this* 2*-Sylow subgroup must be normal since it can have no distinct conjugate. If the reader goes back to the table for* A_4 *given in Section 6.1, it will be seen that exactly this situation prevails.*

Example 10.3.3. *There is only one group of order* 15 *(up to isomorphism) the cyclic group. Let* $|G| = 15$*. It is clear that both the* 5*-Sylow subgroup,* C_5*, and the* 3*-Sylow subgroup,* C_3*, are normal (Why?). Since* C_5 *is cyclic of order* 5 *and* C_3 *is cyclic of order* 3*,* $C_3 \cap C_5 = \{e\}$ *and* $G = C_3C_5$ *since by Theorem 4.3.6,* $|C_3C_5| = 15$*. Hence* $G = C_3 \times C_5 = C_{15}$*, a cyclic group of order* 15 *by Theorem 9.2.4.*

Further applications along these lines are given in the exercises for this section. Deeper structural applications of the Sylow Theorems can be found in the more advanced literature on group theory (see for example [Sc]).

Theorem 10.3.4. *Any finite abelian group* G *is a direct product of its Sylow subgroups.*

Proof: Let $|G| = \prod_{i=1}^{n} p_i^{a_i}$, where the p_i are distinct primes and $a_i \in \mathbb{N}$. Let P_i be the p_i-Sylow subgroup. P_i is unique by Theorem 10.2.1 (the second Sylow Theorem) and by the fact that G is abelian. Of course each $P_i \lhd G$ and $|P_i| = p_i^{a_i}$. Since $P_i \subset P_1P_2...P_n$ $(i = 1, 2, ..., n)$, we have that $|P_1P_2...P_n|$ is divisible by $p_i^{a_i}$, and therefore $G = P_1...P_n$. Repeated application of Theorem 4.3.6 shows $|P_1P_2| = p_1^{a_1}p_2^{a_2}$, $|P_1P_2P_3| = p_1^{a_1}p_2^{a_2}p_3^{a_3}$, etc. from which it forms immediately that

$$P_i \cap P_1...P_{i-1}P_{i+1}...P_n = \{e\},$$

since the groups being intersected have coprime orders. □

Thus any finite abelian group is a direct product of its p-Sylow subgroup's. There are other finite groups, other than abelian groups, which are the direct products of their Sylow subgroups; such finite groups are called nilpotent. The notion of a nilpotent group can be extended to infinite groups by a consideration of various sequences of subgroups in such a way that for finite groups the notion reduces to the above characterization. However, we shall not go into these matters here.

Suppose finally that G is a finite group and that G is the direct product of its Sylow subgroups, say $|G| = \prod_{i=1}^{n} p_i^{a_i}$, and $G = P_1 \times P_2 \times ... \times P_n$,

where P_i is the p_i-Sylow subgroup of G. Let $d|\,|G|$, then $d = \prod_{i=1}^{n} p_i^{b_i}$, where $0 \leq b_i \leq a_i$ and $1 \leq i \leq n$ (WHY?). Since P_i is a p_i-group of order $p_i^{a_i}$, it must contain a normal subgroup N_i of order $p_i^{b_i}$ by Theorem 10.2.4 for every such b_i. Moreover, every such N_i must actually be normal in G by Theorem 9.2.3. Let $N = N_1 N_2 ... N_n$. Then N is a subgroup of G since each $N_i \lhd G$ (by repeated application of Proposition 8.3.6). Also $N_i \cap (N_1 ... N_{i-1} N_{i+1} ... N_n) = \{e\}$ since $P_i \cap (P_1 ... P_{i-1} P_{i+1} ... P_n) = \{e\}$. (WHY is this true for the P's?) and every $N_i \subset P_i$. Thus

$$N = N_1 \times N_2 \times ... \times N_n$$

and $|N| = \prod_{i=1}^{n} p_i^{b_i} = d$. Therefore we have proven that G possesses a subgroup of order d where d was any positive divisor of $|G|$. As a matter of fact, N is even a normal subgroup of G (WHY?). Specializing to the case of an abelian group, which we know by Theorem 10.3.4 is a direct product of its Sylow subgroups, we obtain the converse of Lagrange's Theorem for such groups.

Theorem 10.3.5. *If G is a finite abelian group of order n, then for each $d|n$, G has a subgroup of order d.*

10.3.1 Exercises

1. Prove that there is no simple group of order 204.

2. Prove that there is no simple group of order 18.

3. Let G be a finite group such that $|G| = pq$, where p and q are distinct primes such that $p \not| (q-1)$ and $q \not| (p-1)$. Then prove that G is cyclic.

   small (HINT: Mimic the proof given in the text that any group of order 15 *is cyclic.)*

4. Find all the 3- and 2-Sylow subgroup's for A_4.

   (HINT: The table for A_4 given in Section 6.1 may be helpful. Also recall something about V_4 in A_4.)

5. In the text, it was shown that if G is a finite abelian group of order n, then for each $d > 0$ such that $d|n$, G has a subgroup of order d. Does this imply that G has an element of order d? WHY or WHY NOT?

   (HINT: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.)

Chapter 11

Solvable Groups and the Jordan-Hölder Theorem

We have previously defined the notion of a solvable group in Section 8.1 (Definition 8.1.6). This was done in terms of a sequence of subgroups of the group G, viz., the commutator subgroups. In this chapter, we shall give an alternate characterization of solvable groups again in terms of sequences of subgroups. We shall be concerned, in particular, with two types of sequences of subgroups: a normal series and a composition series, and the notion of when two such sequences are equivalent, which will lead to the Jordan-Hölder Theorem. These notions will all be made precise in this chapter. We recall as was observed in the introduction to Chapter 8 that the concept of a solvable group is intimately related to the solvability of a polynomial equation by radicals.

11.1 The third isomorphism theorem

In Section 8.3, we considered (Theorems 8.3.4 and 8.3.7) the first and second isomorphism theorems. We come now to what is frequently called the third isomorphism theorem, the proof of which is due to Zassenhaus.

Theorem 11.1.1. *(Third Isomorphism Theorem) Let G be a group with subgroups G_1, G_2, H_1, and H_2. Let $H_1 \lhd G_1$ and $H_2 \lhd G_2$. Then $(G_1 \cap H_2)H_1 \lhd (G_1 \cap G_2)H_1$ and $(G_2 \cap H_1)H_2 \lhd (G_1 \cap G_2)H_2$. Moreover,*

$$(G_1 \cap G_2)H_1/(G_1 \cap H_2)H_1 \cong (G_1 \cap G_2)H_2/(G_2 \cap H_1)H_2.$$

Proof: We first note that $G_1 \cap G_2$, $G_1 \cap H_2$, and H_1 are all subgroups of G_1. Also by hypothesis, $H_1 \lhd G_1$. Thus by Proposition 8.1.3, $(G_1 \cap G_2)H_1$ and $(G_1 \cap H_2)H_1$ are subgroups of G_1. We next *claim* that

$$(G_1 \cap H_2)H_1 \lhd (G_1 \cap G_2)H_1.$$

To see this let $a \in G_1 \cap G_2$, $b \in G_1 \cap H_2$, and $c, d \in H_1$. Then $aba^{-1} \in G_1 \cap H_2$, since $a, b \in G_1$. But now $aba^{-1} \in G_1$ and $b \in H_2$ and $a \in G_2$, which implies that $aba^{-1} \in H_2$ since $H_2 \lhd G_2$. Also $aca^{-1} \in H_1$, since $a \in G_1$, $c \in H_1$, and $H_1 \lhd G_1$. Since a typical element of $(G_1 \cap H_2)H_1$ is of the form bc, where $b \in G_1 \cap H_2$ and $c \in H_1$, we therefore get that

$$a(G_1 \cap H_2)H_1a^{-1} \subset (G_1 \cap H_2)H_1 \tag{11.1}$$

where $a \in G_1 \cap G_2$. Moreover, using the same notation as above,

$$dbd^{-1} = d(bd^{-1}b^{-1})b.$$

Bbut $bd^{-1}b^{-1} \in H_1$, since $d \in H_1$, $b \in G_1$, and $H_1 \lhd G_1$, so

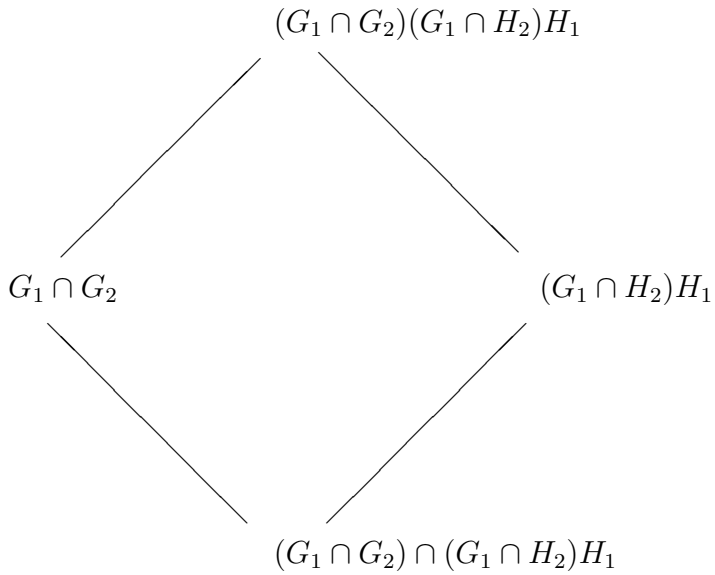
$$dbd^{-1} \in H_1(G_1 \cap H_2).$$

This implies

$$d(G_1 \cap H_2)H_1d^{-1} = d(G_1 \cap H_2)d^{-1}dH_1d^{-1}, \tag{11.2}$$

where we have used the fact that $H_1(G_1 \cap H_2) = (G_1 \cap H_2)H_1$ (which is true since $H_1 \lhd G_1$, by Proposition 8.3.6). Recall the typical element of $(G_1 \cap G_2)H_1$ is of the form ad where $a \in G_1 \cap G_2$ and $d \in H_1$. According to Proposition 6.1.4, this, (11.1) and ((11.2) together imply $(G_1 \cap H_2)H_1 \lhd (G_1 \cap G_2)H_1$. This proves the claim above.

On the basis of the second isomorphism (Theorem 8.3.7), we have



(note that $(G_1 \cap H_2)H_1 \lhd (G_1 \cap G_2)(G_1 \cap H_2)H_2$ since $(G_1 \cap H_2)H_1 \lhd (G_1 \cap G_2)H_1$ and $(G_1 \cap G_2)(G_1 \cap H_2)H_1 = (G_1 \cap G_2)H_1$. Now since $(G_1 \cap H_2)H_1 \lhd (G_1 \cap G_2)(G_1 \cap H_2)H_1$, $(G_1 \cap G_2) \cap (G_1 \cap H_2)H_1 \lhd G_1 \cap G_2$, and

$$(G_1 \cap G_2)/((G_1 \cap G_2) \cap (G_1 \cap H_2)H_1) \cong ((G_1 \cap G_2)H_1)/((G_1 \cap H_2)H_1). \quad (11.3)$$

However, we contend that

$$(G_1 \cap G_2)(G_1 \cap H_2)H_1 = (G_1 \cap H_2)H_1 \cap G_2. \quad (11.4)$$

For clearly

$$(G_1 \cap G_2)(G_1 \cap H_2)H_1 \subset (G_1 \cap H_2)H_1 \cap G_2.$$

While if $w \in (G_1 \cap H_2)H_1 \cap G_2$, then $w \in G_2$ and $w = xy$, where $x \in G_1 \cap H_2$ and $y \in H_1 \subset G_1$. But then $x \in G_1$ and $y \in G_1$, so $w \in G_1 \cap G_2$, and we then get the inclusion the other way. This proves (11.4).

Next we note that any element of $(G_1 \cap H_2)H_1$ is of the form uv, where $u \in G_1 \cap H_2$ and $v \in H_1$. If this element also belongs to G_2, i.e., $uv \in G_2$, then

$$v = u^{-1}(uv) \in G_2;$$

hence $v \in G_2 \cap H_1$. Thus $uv \in (G_1 \cap H_2)(G_2 \cap H_1)$. We have shown that

$$(G_1 \cap H_2)H_1 \cap G_2 \subset (G_1 \cap H_2)(G_2 \cap H_1)$$

Since the reverse inclusion is clear, we have

$$(G_1 \cap H_2)H_1 \cap G_2 = (G_1 \cap H_2)(G_2 \cap H_1)$$

Combining this last result with (11.4) and (11.3) yields

$$(G_1 \cap G_2)/((H_1 \cap G_2)(G_1 \cap H_2)) \cong ((G_1 \cap G_2)H_1)/((G_1 \cap H_2)H_1). \quad (11.5)$$

However, by symmetry, i.e., replacing 1 by 2 and vice versa in (11.5) yields

$$(G_1 \cap G_2)/((H_1 \cap G_2)(G_1 \cap H_2)) \cong ((G_1 \cap G_2)H_2)/((G_2 \cap H_1)H_2). \quad (11.6)$$

and by (11.5) and (11.6), we finally have that

$$(G_1 \cap G_2)H_1/(G_1 \cap H_2)H_1 \cong (G_1 \cap G_2)H_2/(G_2 \cap H_1)H_2.$$

□

We note that the symmetry arguement used in the above proof to get (11.6) could, of course, have been replaced by an argument similar to that given in the first part of the proof. (See exercise 1 for this section.)

11.1.1 Exercises

1. Under the hypothesis of Theorem 11.1.1, use an argument similar to that given in the proof of this theorem to first show that $(H_1 \cap G_2)H_2 \lhd (G_1 \cap G_2)H_2$ and then that equation (11.6) above holds.

11.2 Series of groups; solvable groups revisited

We shall apply the third isomorphism theorem presently, but first we introduce a special sequence of subgroups of a group (usually called **series** of groups). This was alluded to in the introduction to this chapter. Let

$$\{e\} = G_{t+1} \subset G_t \subset ... \subset G_2 \subset G_1 = G \quad (11.7)$$

be a sequence of subgroups of the group G where each G_{i+1} is normal in G_i (but not necessarily in all of G). Such a sequence of subgroups is called a

normal series for G. Associated with a normal series for a group G, is an associated sequence of **factors** (or factor groups); viz

$$G_1/G_2, G_2/G_3, ..., G_t/G_{t+1} = G_t.$$

We observe that a normal series always exists for an arbitrary group G. We could, e.g., take the trivial normal series: $\{e\} \subset G = G_1$. There is also nothing unique about a normal series, e.g., the symmetric group S_4 has the following normal series, among others:

$$\begin{array}{c} \{e\} \subset C_2 \subset V_4 \subset A_4 \subset S_4, \\ \{e\} \subset V_4 \subset A_4 \subset S_4, \\ \{e\} \subset C_2 \subset V_4 \subset S_4, \\ \{e\} \subset V_4 \subset S_4, \\ \{e\} \subset S_4, \end{array} \tag{11.8}$$

where V_4 is the Klein 4-group (see Section 6.3), and, as usual, C_n denotes a cyclic group of order n, here, e.g., take $C_2 = \langle (12)(34) \rangle$. Note that all terms in the fifth series given above for S_4 occur in the fourth and all those in the fourth occur in the third and those in the third occur in the first. A similar situation prevails between the fifth, fourth, second, and first series. This illustrates the following: one normal series is called a **refinement** of another if all the terms of the second occur in the first series. Hence the second series above is a refinement of the fourth series. The third series is also a refinement of the fourth series. However, the second series is not a refinement of the third series.

Finally, two normal series

$$\begin{array}{l} \{e\} = G_{s+1} \subset G_s \subset ... \subset G_2 \subset G_1 = G, \\ \{e\} = H_{t+1} \subset H_t \subset ... \subset H_2 \subset H_1 = H, \end{array} \tag{11.9}$$

are called **equivalent** or (**isomorphic**) if there exists a 1-1 correspondence between the factors of the two series (thus $s = t$) such that the corresponding factors are isomorphic.

Example 11.2.1. *Consider the two series for* $\mathbb{Z}_{15}$,

$$\begin{array}{l} \mathbb{Z}_{15} \supset \langle [5] \rangle \supset \{[0]\}, \\ \mathbb{Z}_{15} \supset \langle [3] \rangle \supset \{[0]\}, \end{array}$$

where [5] *denotes the residue class of* 5 *mod* 15. *These normal series are equivalent: For* $\mathbb{Z}_{15}/\langle[5]\rangle \cong \mathbb{Z}_5$, $\langle[5]\rangle/\{[0]\} \cong \mathbb{Z}_3$, *while the factors of the second series are* $\mathbb{Z}_{15}/\langle[3]\rangle \cong \mathbb{Z}_3$, $\langle[3]\rangle/\{[0]\} \cong \mathbb{Z}_5$ *(where* [3] *denotes the residue class of* 3 *mod* 15*).*

Our first general theorem in this spirit is the following important theorem due to Schreier.

Theorem 11.2.2. *(Schreier) Any two normal series for a group G have equivalent refinements.*

Proof: Consider two normal series for G as in (11.9). Define

$$G_{ij} = (G_i \cap H_j)G_{i+1}, \quad j = 1, 2, ..., t+1,$$
$$H_{ji} = (G_i \cap H_j)H_{j+1}, \quad i = 1, 2, ..., s+1.$$

Then we have

$$G = G_{11} \supset G_{12} \supset ... \supset G_{1,s+1} = G_2$$
$$= G_{21} \supset ... \supset G_{2,s+1} = G_3 \supset ... \supset G_{t,s+1} = \{e\},$$

and

$$G = H_{11} \subset H_{12} \supset ... \supset H_{1,t+1} = H_2$$
$$= H_{21} \supset ... \supset H_{2,t+1} = H_3 \supset ... \supset H_{s,t+1} = \{e\},$$

Now applying the third isomorphism theorem (Theorem 11.1.1) to the groups G_i, H_j, G_{i+1}, H_{j+1}, we have that $G_{i,j+1} = (G_i \cap H_{j+1})G_{i+1} \lhd G_{i,j} = (G_i \cap H_j)G_{i+1}$ and $H_{j,i+1} = (G_{i+1} \cap H_j)H_{j+1} \lhd H_{j,i} = (G_i \cap H_j)H_{j+1}$. Furthermore, also by Theorem 11.1.1,

$$G_{ij}/G_{i,j+1} \cong H_{ji}/H_{j,i+1}.$$

Thus the above two are normal series which are refinements of the two given series and they are equivalent. □

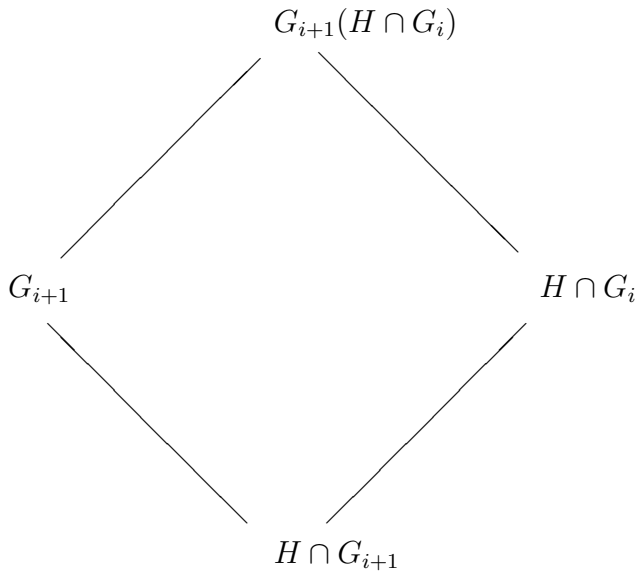
We shall, in the next section, apply Schreier's Theorem 11.2.2 to obtain the important theorem of Jordan-Hölder, but first we wish to give an alternate characterization of solvable groups. Before doing this, we establish the following useful theorem.

Theorem 11.2.3. *If* $\{e\} = G_{t+1} \subset G_t \subset ... \subset G_2 \subset G_1 = G$ *is a normal series for the group G and if* $H \leq G$, *then*

$$H = H \cap G_1 \supset H \cap G_2 \supset ... \supset H \cap G_{t+1} = e$$

is a normal series for H. The factors of the normal series in (11.2.3) are isomorphic to subgroups of the factors of the normal series for G.

Proof: We apply the second isomorphism theorem (Theorem 8.3.7) to the subgroups G_{i+1} and $H \cap G_i$ of the group G_i. Hence, we have



First note that since $G_{i+1} \lhd G_i$, $G_{i+1}(H \cap G_i)$ is a subgroup of G_i, Proposition 8.3.6 implies $G_{i+1} \lhd G_{i+1}(H \cap G_i)$, and also $H \cap G_{i+1} \lhd H \cap G_i$. Second note that $G_{i+1} \cap (H \cap G_i) = H \cap G_{i+1}$ since $G_{i+1} \subset G_i$ and that is how we get the group at the lower vertex of our diagram. Thus Theorem 8.3.7 yields that

$$H \cap G_i / H \cap G_{i+1} \cong G_{i+1}(H \cap G_i)/G_{i+1} \cong G_i/G_{i+1}.$$

□

We now make the following definition (cf. Definition 8.1.6).

Definition 11.2.4. *A group G is said to be* **solvable** *if it has a normal series all of whose factors are abelian groups.*

Since we have already defined a solvable group in Section 8.1, we must show that these two definitions are equivalent. Thus suppose that G is solvable according to Definition 8.1.6. Then

$$G \supset G' \supset G'' \supset ... \supset G^{(t)} = \{e\},$$

where the superscripts designate the higher commutator subgroups (see Section 8.1). This is, of course, a normal series (see comments at the beginning

of Section 8.1 and Theorem 8.1.5) for G. Moreover, $G^{(i)}/G^{(i+1)}$ is abelian by Theorem 8.1.4. Hence G is solvable according to Definition 11.2.4 above.

Suppose now that G is solvable in the sense of Defintion 11.2.4. So that G has a normal series as in (11.7), such that each factor G_i/G_{i+1} is abelian. In particular, $G/G_2 = G_1/G_2$ is abelian. Thus by Theorem 8.1.4, $G_2 \supset G_1' = G'$. Since G_2/G_3 is abelian, we have, again by Theorem 8.1.4, that $G_3 \supset G_2' \supset (G_1')' = G''$. Similarly,

$$G_4 \supset G_3' \supset (G_2')' = G_1''' = G'''.$$

Continuing in this fashion, we finally get that

$$\{e\} = G_{s+1} \supset G^{(s)}.$$

Hence $G^{(s)} = \{e\}$, and G is solvable according to our original definition.

Thus we are at liberty to use whichever characterization of solvabilty is more convenient. In the following theorem, we arbitrarily use the characterization of solvability introduced in this section. We strongly advise the reader to prove the theorem (see exercise 3 for this section) using the initial definition (Definition 8.1.6) without making use of the equivalent characterization we have just established.

Theorem 11.2.5. *Any subgroup and any factor group of a solvable group is solvable.*

Proof: Suppose G is solvable. Then G has a normal series (11.7), such that G_i/G_{i+1} is abelian. Let $H \leq G$. Then form the series (11.2.3). By Theorem 11.2.3, we thus get a normal series, and $(H \cap G_i)/(H \cap G_{i+1})$ is isomorphic to a subgroup of G_i/G_{i+1} and is, therefore, abelian. This completes the first part of the theorem.

Again let G be a solvable group and let (11.7) again denote a normal series for G with abelian factors. It is easy to see that any refinement of the series (11.7) also has abelian factors; e.g., suppose

$$G_1 \supset G_2 \supset H \supset G_3 \supset ....$$

is a refinement of (11.7). Then $H/G_3 \subset G_2/G_3$ and, hence, is abelian. Since $G_2/H \cong (G_2/G_3)/(H/G_3)$, by Corollary 8.3.5, therefore, G_2/H also abelian. Now let $N \lhd G$. Consider the normal series

$$G \supset N \supset \{e\}. \tag{11.10}$$

By Schreier's Theorem (Theroem 11.2.2), (11.7) and (11.10) have equivalent refinements. Let

$$G \supset H_1 \supset H_2 \supset ... \supset H_n \supset N \supset ... \supset \{e\} \tag{11.11}$$

be a refinement of (11.10) equivalent to a refinement of (11.7). By our preceding observations, the factors of (11.11) are abelian. Since $(H_i/N)/(H_{i+1}/N) \cong (G_i/G_{i+1})$, by Corollary 8.3.5,

$$G/N \supset H_1/N \supset H_2/N \supset ... \supset H_n/N \supset N/N = \{e\}$$

is a normal series for G/N with abelian factors. □

Since A_n for $n \geq 5$ was shown to be a simple group (see Theorem 6.3.2),

$$A_n \supset \{e\}$$

is the only normal series for A_n, when $n \geq 5$. But A_n for $n \geq 5$ is, of course, non-abelian, hence is not a solvable group. Consequently, by the preceding Theorem 11.2.5, S_n for $n \geq 5$ is also not a solvable group.

11.2.1 Exercises

1. Prove that any finite p-group is solvable.

   (HINT: Use Theorems 10.2.4 and 10.2.6)

2. Prove that if G is a group that has a normal subgroup N such that both N and G/N are solvable, then G must be solvable.

   (HINT: Construct the appropriate normal series for G using the assumed ones for G/N and N. Also use the Corollary to Theorem 8.3.1 and the Corollary 8.3.5.)

3. Use the original definition of solvability Definition 8.1.6) to establish Theorem 11.2.5 directly.

   (HINT: What is the image of the commutator subgroup under the canonical hom?)

11.3 The Jordan-Hölder Theorem

In order to state the main theorem of this section, we first need two definitions.

Definition 11.3.1. *Let G be a group with $N \lhd G$. Then N is called* **maximal** *in G if $N \subset G$ properly (i.e., $N \neq G$) and there does not exist any normal subgroup where the inclusions are all meant to be proper.*

On the basis of Corollary 8.3.3 another way of characterizing a maximal normal subgroup is as follows: N is a maximal normal subgroup of G if and only if G/N is simple. (See the exercises below.)

We now state our last definition.

Definition 11.3.2. *A* **composition series** *for a group G is a normal series as in (11.7), where all the inclusions are proper and such that G_{i+1} is maximal in G_i (in other words, each factor is simple).*

For example, in the case of the previously given normal series for S_4 in (11.8), only the first $\{e\} \subset C_2 \subset V_4 \subset A_4 \subset S_4$ is a composition series for S_4. A composition series for A_4 would be: $\{e\} \subset C_2 \subset V_4 \subset A_4$. Note that $A_4 \supset V_4 \supset \{e\}$ would not be a composition series for A_4 (Why?). Unlike the case of normal series, it is possible that an arbitrary group does not have a composition series (see exercise 1 for this section) or even if it does have one a subgroup of it may not have one. Of course, a finite group does have a composition series.

We now consider the case in which a group, G, does have a composition series, and we prove the following important theorem.

Theorem 11.3.3. *(Jordan-Hölder): If a group G has a composition series, then any two composition series are equivalent (i.e., the composition factors are unique).*

Proof: Suppose we are given two composition series. Applying Schreier's refinement theorem (Theorem 11.2.2), we get that the two composition series have equivalent refinements. But the only refinement of a composition series is one obtained by introducing repetitions. If in the 1-1 correspondnece between the factors of these refinements, the paired factors equal to $\{e\}$ are disregarded (i.e., if we drop the repetitions), we get clearly that the original composition series are equivalent. $\square$

It was mentioned in the introduction to Chapter 6 that the simple groups are important because "they play a role in finite group theory somewhat analogous to that of the primes in number theory." In particular, an arbitrary finite group, G, can be broken down into simple components. These uniquely determined simple components are, according to the Jordan-Hölder, the factors of a composition series for G.

We close by giving an application of this theorem. In particular, we use the Jordan-Hölder Theorem to prove the uniqueness part of the Fundamental Theorem of Arithmetic. The Fundamental Theorem of Arithmetic states that every positive integer not equal to a prime can be factored uniquely (up to order) into a product of primes.

First, we *claim* that such a factorization exists. Indeed, suppose n is composite (i.e., $n > 1$ and n is not a prime). Then an easy induction shows that n has a prime divisor p and we can write $n = pn_1$, where n_1 is an integer satisfying $n_1 < n$. If n_1 is prime, the claim holds. Otherwise, n_1 has a prime factor p_1, and $n_1 = p_1 n_2$ where $n_2 < n_1$ is an integer. Continuing in this fashion, we must come to an equation $n_{j-1} = p_{j-1} n_j$, where n_j is a prime p_j, since the sequence of decreasing positive integers

$$n > n_1 > n_2 > n_3 > ...$$

cannot continue indefinitely. We now have that $n = pp_1p_2...p_j$ is a product of primes. This proves the existence claim.

On the basis of the Jordan-Hölder Theorem, we can easily show the other part of the Fundamental Theorem of Arithmetic, i.e., apart from order of the factors, the representation of n as product of primes is unique. To do this suppose that

$$n = p_1 p_2 ... p_s,$$

and

$$n = q_1 q_2 ... q_t$$

where the p_i and q_j are primes. Then denoting, as usual, by C_k the cyclic group of order k, we have

$$C_n \supset C_{p_2...p_s} \supset C_{p_3...p_s} \supset ... \supset C_{p_s} \supset \{e\},$$

and

$$C_n \supset C_{q_2...q_t} \supset C_{q_3...q_t} \supset ... \supset C_{q_t} \supset \{e\},$$

as two composition series for C_n. But the Jordan-Hölder Theorem implies these must be equivalent; hence we must have $s = t$ and by suitably arranging $p_i = q_i, 1 \leq i \leq s$. Thus we have established the unique factorization theorem for positive integers as an application of the Jordan-Hölder Theroem.

11.3.1 Exercises

1. Prove that any infinite abelian group G does not have a composition series.

   (HINT: Suppose it does and come to a contradiction. Also use the result of exercise 4 for Section 6.3.)

2. Prove that a finite group is solvable if and only if the factors of a composition series are cyclic groups having prime orders.

3. Prove that if G is a group which has a composition series, then any normal subgroup of G and any factor group of G also have composition series with factors isomorphic to composition factors of G.

   (HINT: Mimic the proof of Theorem 11.2.5.)

4. Prove that N is a maximal normal subgroup of G if and only if G/N is simple.

5. Optional Problem Identify the last statement in this section. State where it came from, what it means, and its significance.

Bibliography

[FT] Feit, W. and Thompson, J.G., "Solvability of groups of odd order," Pacific Journal of Mathematics 3 (1963), 775-1029.

[G] Gorenstein, D., "The Enormous Theorem," Scientific American 253(6), 1985, 104-115.

[L] Ledermann, W., **Introduction to the Theory of Finite Groups**, Oliver and Boyd, 1967.

[R] Reid, J.D., "On finite groups and finite fields," The American Mathematical Monthly 98(6), 1991, 549-551.

[Sc] Scott, W., **Group Theory**, Prentice-Hall, 1964.

[St] Stoll, R.R., **Introduction to Set Theory and Logic**, W.H. Freeman, 1963.

Index