Elementary Group Theory

Timothy J. Hodges

Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221-0025

CHAPTER 1

Groups and Homomorphisms

1.1. Definition of a group

Consider the set G of bijections on a set S, (you can take $S = \{1, 2, 3\}$ if you want to be more concrete). From basic set theory we know that composition of functions gives this set some additional structure. What do we know about the set G together with this operation?

(1) We know that the operation is associative.
(2) We know that the identity map $I(s) = s$ is a bijection which acts an identity element for composition of functions. That is, for any other bijection $f\colon S \to S$, $f \cdot I = f$ and $I \cdot f = f$.
(3) We know that the inverse of a bijection is also a bijection. So every element of G has an inverse under composition.

We model our definition of group on this situation. But first lets think about the idea of an operation on a set. By this we mean a way of combining two elements to get a new one, so this is essentially a function $\phi : G \times G \to G$. While this is a logical notation mathematically speaking, its not practical, because we usually want to write an operation in the form $g * h$. So we compromise and consider $*$ as a function $*\colon G \times G \to G$, but we make the convention that $*(g, h) = g * h$. Such an operation is called a binary operation (because it combines *two* elements of the set to get a new one).

Definition 1.1.1. A *group* is a set G together with a binary operation $*\colon G \times G \to G$ such that:

(1) $\exists e \in G$ such that $\forall g \in G$, $e * g = g$ and $g * e = g$
(2) $\forall g \in G$, $\exists h \in G$ such that $g * h = e$ and $h * g = e$
(3) $\forall g, h, k \in G$, $(g * h) * k = g * (h * k)$.

For this concept to be one of the most fundamental in mathematics, there should be some interesting examples. Here are a few that the reader should be familiar with

Example 1.1.2. The basic number systems are groups under addition: the integers, $\mathbb{Z}$; the rational numbers, $\mathbb{Q}$; the real numbers, $\mathbb{R}$; the complex numbers, $\mathbb{C}$. We know addition is associative; the identity element is 0; and the inverse of a number x is just its negative $-x$. Of course the natural numbers are not a group because they don't contain the inverses of any elements (except 0).

Example 1.1.3. The set of *non-zero* real numbers $\mathbb{R}^*$ forms a group under multiplication for similar reasons. So do $\mathbb{Q}^*$ and $\mathbb{C}^*$. Note that $\mathbb{R}$ is not a group under multiplication since the element 0 does not have a multiplicative inverse. In a sense this is about as close one can get to satisfying the group axioms: the

operation is associative; there exists an identity element for the operation; and all elements but one have a multiplicative inverse.

EXAMPLE 1.1.4. Consider the set of non-singular $n \times n$ matrices whose entries are real numbers. From linear algebra we know that matrix multiplication is associative; that the identity matrix is nonsingular (and is an identity element for multiplication in the sense above); and that the inverse of a nonsingular matrix exists and is non-singular. Thus this the set of non-singular $n \times n$ matrices is a group under multiplication, which we denote $\mathrm{GL}_n(\mathbb{R})$. Similarly we can define $\mathrm{GL}_n(\mathbb{Q})$ and $\mathrm{GL}_n(\mathbb{C})$.

EXAMPLE 1.1.5. Let T be a set. The set $\mathcal{A}(T)$ of bijections from T to T is a group under composition of functions. We know from elementary set theory that composition of functions is associative; the identity map is clearly an element of $\mathcal{A}(T)$ that acts as an identity element for composition of functions; finally we know that any bijection has an inverse which is also a bijection so that all elements have inverses. The group $\mathcal{A}(T)$ is also called the group of permutations of T. If T is a finite set with n elements, then $\mathcal{A}(T)$ has $n!$ elements.

EXAMPLE 1.1.6. In the case where $T = \{1, 2, \ldots, n\}$, we denote this group by S_n. Lets look in detail at S_3. Denote by (123) the cyclic permutation that sends 1 to 2, 2 to 3 and 3 to 1. Similarly denote by (12) the permutation that interchanges 1 and 2 and fixes 3. Then in this notation, S_3 consists of six elements:

$$S_3 = \{e, (12), (23), (13), (123), (132)\}.$$

We shall use the convention that these permutations are composed from right to left. Thus (12)(23) means first perform (23) then perform (12). Hence (12)(23) = (123). The reader should construct the complete multiplication table for S_3.

DEFINITION 1.1.7. A group is said to be *abelian* if $gh = hg$ for all $g, h \in G$.

Obviously the first two sets of examples are abelian groups but the second two are not.

DEFINITION 1.1.8. The *order* of a group is its cardinality in the set-theoretic sense. We denote the order of G by $|G|$.

For instance $|S_n| = n!$.

1.2. Products of groups

Given any pair of groups, H and G, their Cartesian product $H \times G$ naturally forms a group. At this stage, this is not a particularly interesting or exciting fact (and the reader can skip this section for a while if she prefers). It does present an opportunity to give a proof of how to verify the group axioms.

THEOREM 1.2.1. *Let $(H, \circ)$ and $(G, *)$ be groups. Define an operation on the Cartesian product $H \times G$ by*

$$(h_1, g_1) \cdot (h_2, g_2) = (h_1 \circ h_2, g_1 * g_2).$$

Then $(H \times G, \cdot)$ is a group.

PROOF. (1) Let e be an identity element for H and f an identity element for G. Then for any $(h, g) \in H \times G$,

$$(e, f) \cdot (h, g) = (e \circ h, f * g) = (h, g).$$

and

$$(h, g) \cdot (e, f) = (h \circ e, g * f) = (h, g).$$

Hence (e, f) acts an identity element for $H \times G$.

(2) Let $(h, g) \in H \times G$. Then we know that there exist $h' \in H$ such that $h \circ h' = e$ and $h' \circ h = e$. Similarly there exists a $g' \in G$ such that $g * g' = f$ and $g' * g = f$. Hence

$$(h, g) \cdot (h', g') = (h \circ h', g * g') = (e, f) \quad \text{and} \quad (h', g') \cdot (h, g) = (h' \circ h, g' * g) = (e, f)$$

as required.

(3) Let $h_1, h_2, h_3 \in H$, and let $g_1, g_2, g_3 \in G$. Then using the associative law from H and G, we see that

$$\begin{aligned}((h_1, g_1) \cdot (h_2, g_2)) \cdot (h_3, g_3) &= (h_1 \circ h_2, g_1 * g_2) \cdot (h_3, g_3) \\ &= ((h_1 \circ h_2) \circ h_3), (g_1 * g_2) * g_3) \\ &= ((h_1 \circ (h_2 \circ h_3), (g_1 * (g_2 * g_3) \\ &= (h_1, g_1) \cdot (h_2 \circ h_3, g_2 * g_3) \\ &= (h_1, g_1) \cdot ((h_2, g_2) \cdot (h_3, g_3))\end{aligned}$$

Hence the associative law holds in $(H \times G, \cdot)$. □

1.3. Basic properties

The axioms are chosen for their minimality. Some immediate questions are opened up immediately. The axioms guarantee an identity element - can there be more than one? The axioms also guarantee that inverses of elements exist but say nothing about uniqueness here either. We begin with a little book-keeping. From now on we will drop the $*$ and denote the operation by juxtaposition. That is, we'll now write ab for $a * b$. We'll bring the $*$ back for clarity whenever it is needed.

LEMMA 1.3.1. *Let G be a group.*

(1) *There is a unique identity element.*
(2) *The inverse of an element is unique.*

PROOF. Let e and f be two identity elements. Then for all $g \in G$, $eg = g$ and $gf = g$. In particular, taking $g = f$ in the first case yields $ef = f$ and taking $g = e$ in the second yields $ef = e$. So $e = f$. We can summarize this argument as $f = ef = e$.

Now let h and k be two inverses of an element $g \in G$. Then $gh = e$ and $hg = e$; and $gk = e$ and $kg = e$. Hence

$$k = ke = k(gh) = (kg)h = eh = h.$$

□

Thus we may speak of *the* identity element of a group (and we sometimes write e_G to signify the identity element of the group G). We may also talk of *the* inverse of an element. It therefore makes sense to use the notation g^{-1} to denote the inverse of g (note that had we not proved the result about uniqueness of the inverse, this

notation would have been meaningless - this is why this notation does not occur in the axioms).

The axiomss also guarantee cancellation of elements in the following sense. Since we use this fact frequently, we present it as a lemma, even though the proof is essentially trivial.

LEMMA 1.3.2. *Let G be a group and $a, b, c \in G$. Then*

$$ab = ac \implies b = c \qquad \text{and} \qquad ac = bc \implies a = b$$

PROOF. Multiply on the left by a^{-1} and on the right by c^{-1} respectively. □

There is also an important issue connected with the definition of associativity. The axiom deals with two possible products of three elements. What about four elements? There are five different ways of multiplying four elements together:

$$a(b(cd), \quad a((bc)d), \quad (a(bc))d, \quad ((ab)c)d, \quad (ab)(cd)$$

The reader should be able to see that all five are equal using repeated application of the associative law. using induction we can show that this is true for arbitrarily long products.

THEOREM 1.3.3. *Let $a_1, \dots, a_n$ be a collection of n elements from a group G. Then all possible products of these elements in this order are equal.*

PROOF. It suffices to show that an arbitrary product is equal to the fixed "right to left" product $a_1(a_2(\dots a_n)\dots))$. We can do this by induction on n. The case $n = 3$ is the associative law and serves as the base of the induction. Take an arbitrary product of length n, lets call it p, and assume the result is true for products of $n-1$ or fewer terms. We can write $p = rs$ where r is a product of $a_1, \dots a_i$ for some $i \geq 1$ and s is a product of $a_{i+1}, \dots a_n$. By the inductive hypothesis, $r = a_1 r'$ where r' is the product of $a_2, \dots, a_i$. So $p = (a_1 r')s = a_1(rs)$ and rs is the unique product of $a_2, \dots, a_n$. So $rs = a_2(a_3(\dots))$ and $p = a_1(a_2(\dots a_n)\dots))$ as required. □

1.4. Exponents and the order of an element

We now proceed to define exponents exactly as if the operation was ordinary multiplication. We define exponents inductively by

$$g^0 = e, \qquad g^{n+1} = g^n g$$

We can then define negative exponents by

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

As one might expect the laws of exponents hold. Unfortunately, the proofs involve many different cases and are not much fun.

LEMMA 1.4.1. *Let G be a group, let $g \in G$ and let $n, m \in \mathbb{Z}$. Then*

(1) $g^n g^m = g^{n+m}$
(2) $(g^n)^m = g^{nm}$
(3) $g^{-n} = (g^n)^{-1}$

DEFINITION 1.4.2. Let g be an element of a group G. The order of g, denoted $o(g)$, is the smallest positive integer n such that $g^n = e$. If no such n exists, then we say that g has infinite order.

Thus $o(g) = n \implies g^n = e$. However the converse is false: $g^n = e \not\Rightarrow o(g) = n$ (assuming that $g^n = e \implies o(g) = n$ is one of the most common beginner's mistakes in group theory). Of course the counterexamples are completely trivial. Inside the multiplicative group of real numbers, $\mathbb{R}^*$, we have that $(-1)^8 = 1$, but $o(g) = 2$.

EXAMPLE 1.4.3. Consider the group of complex sixth roots of unity, $G = \{z \in \mathbb{C} \mid z^6 = 1\}$. If $\omega = (-1 + \sqrt{3}i)/2$ (a non-trivial cube root of 1), then

$$G = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$$

In this group there are two elements of order 6 ($-\omega$ and $-\omega^2$), two elements of order 3 (ω and ω^2), one element of order two (-1) and one element of order 1.

PROPOSITION 1.4.4. *Let G be a group and let $g \in G$ be an element of order $n \in \mathbb{N}$. Then*

(1) *$g^t = e$ if and only if $n|t$*
(2) *$g^s = g^t$ if and only if $s \equiv t \pmod{n}$.*

PROOF. (1) Use the division algorithm to write $t = nd + r$ where $0 \leq r < n$. The $g^t = g^{dn+r} = (g^n)^d g^r = g^r$. Since $r < n$, it follows from the definition of order that $g^t = e$ if and only if $r = 0$; that is, $g^t = e$ if and only if $n|t$.

(2) $g^s = g^t \iff g^{s-t} = e \iff n|(s-t) \iff s \equiv t \pmod{n}$. □

1.5. Subgroups and cyclic groups

DEFINITION 1.5.1. Let $(G, *)$ be a group. A nonempty subset H of G is called a subgroup if it is closed under the operation $*$ and H together with the operation restricted to H forms a group.

For instance, if $G = \mathbb{C}^*$, then the set of sixth roots of unity considered above is a subgroup of G. If $G = S_3$, then the subset $H = \{e, (12)\}$ is a subgroup of G.

PROPOSITION 1.5.2. *A non-empty subset H of a group G is a subgroup if and only if:*

(1) *H is closed: $\forall h, h' \in H$, $hh' \in H$.*
(2) *$\forall h \in H$, $h^{-1} \in H$*

PROOF. ($\implies$) Assume that H is a subgroup. Part (1) is immediate from the definition of a group. Before proving part (2), we must check that the identity element e_H of the subgroup H must be e_G. Pick some $h \in H$. Then

$$he_H = h = he_G$$

So by cancelation, $e_G = e_H \in H$. This assures us that there is no ambiguity in the notation h^{-1} - the inverse in H is the same as the inverse in G. Thus part (2) follows again from the axioms of a group.

For the converse, assume that a nonempty subset H of G satisfies the two given properties. Then the operation in G restricts to a binary operation on H which is associative, because it is associative on the larger set G. Since H is nonempty. we may pick an $h \in H$. By the second condition $h^{-1} \in H$, and by the first condition $e = hh^{-1} \in H$. Hence H is a subgroup. □

COROLLARY 1.5.3. *A non-empty subset H of a group G is a subgroup if and only if $\forall h, k \in H$, $hk^{-1} \in H$.*

PROOF. Suppose that H is a subgroup and that $h, k \in H$. Then $k^{-1} \in H$ by part (2) above. hence $hk^{-1} \in H$ by part (1).

Conversely suppose that the condition holds. Let $h \in H$. Then $e = hh^{-1} \in H$. Hence also $eh^{-1} = h^{-1} \in H$. This proves condition (2) of the theorem. Now let $h, k \in H$. Then we have shown that $k^{-1} \in H$. Hence by hypothesis H contains $h(k^{-1})^{-1} = hk$. This proves condition (2). Hence by Proposition 1.5.2 H is a subgroup. □

EXAMPLE 1.5.4. For any integer n, the subset $n\mathbb{Z} = \{m \in \mathbb{Z} \mid n||m\}$ is a subgroup of $\mathbb{Z}$. For instance if $n = 2$, then $2\mathbb{Z}$ is just the subgroup of even integers.

EXAMPLE 1.5.5. Let $G = \mathrm{GL}_n(\mathbb{R})$ and let $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}$. Let $A, B \in \mathrm{SL}_n(\mathbb{R})$. Then by the multiplicativity of the determinant,

$$\det(AB^{-1}) = \det(A)\det(B)^{-1} = 1$$

Hence by the corollary, $\mathrm{SL}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

EXAMPLE 1.5.6. For any group G, we define the *center* of G to be the set $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$. The elements of $Z(G)$ are the elements of G that commute with every element of G. We say that such an element is *central*. We leave it as an exercise for the student to check that $Z(G)$ is a subgroup of G.

COROLLARY 1.5.7. *Let G be a group and let H be a finite nonempty subset of G. Then H is a subgroup if and only if H is closed.*

PROOF. Let $n = |G|$. Suppose that H is closed. Let $h \in H$ and consider the set $L = \{hk \mid k \in H\}$. Because of cancelation, if $k \neq k'$, then $hk \neq hk'$. Hence we have that $L \subset H$ and $|L| = |H|$. So $L = H$. Thus there exists a $k \in H$ such that $hk = e$. So $k = h^{-1}$ and we have established that H contains the inverse of all its elements. By Proposition 1.5.2, H must be a group.

The converse is clear. □

PROPOSITION 1.5.8. *Let G be a group and let $g \in G$. The set $H = \{g^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.*

PROOF. The two properties of Proposition 1.5.2 follow directly from the rules of exponents given in Lemma 1.4.1. □

DEFINITION 1.5.9. Let G be a group and let $g \in G$. The set $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ is called the *cyclic subgroup generated by g*.

DEFINITION 1.5.10. Let G be a group. If there exists a $g \in G$ such that $G = \langle g \rangle$, then G is said to be a cyclic group.

The next result assembles some elementary results about the set of all subgroups of a group.

PROPOSITION 1.5.11. *Let G be a group.*

(1) *The set $\{e\}$ is a subgroup of G.*
(2) *G is a subgroup of G.*
(3) *If H and K are subgroups of G, then so is $H \cap K$.*
(4) *If H and K are subgroups of G and G is abelian, then the set $HK = \{ab \mid a \in H, b \in K\}$ is a subgroup of G.*

PROOF. The proofs are either trivial or easy exercises for the reader. □

The subgroup $\{e\}$ is called the *trivial* subgroup. A subgroup H such that $H \subsetneq G$ is called a *proper* subgroup.

DEFINITION 1.5.12. Let I be a subset of a group G. The subgroup generated by I is defined to be the intersection of all the subgroups of G containing I. It is denoted by $\langle I \rangle$.

It can be shown fairly easily that $\langle I \rangle$ consists of the set of "words" in the elements of I and their inverses. That is, if $\tilde{I} = \{a^{-1} \mid a \in I\}$, then

$$\langle I \rangle = \{a_1 a_2 \dots a_n \mid n \in \mathbb{N}, \quad a_i \in I \cup \tilde{I}\}.$$

Thus in particular, if I is a singleton set, say $I = \{g\}$, then the definition of $\langle \{g\} \rangle$ coincides with the definition of $\langle g \rangle$ above.

1.6. Subgroups of S_4

In order to illustrate further the concept of subgroups and to generate a few more examples of small but interesting groups, we look briefly at subgroups of S_4. Notice that S_4 has 24 elements which fall into a number of different types, which we'll list by order. First obviously there is the identity element e. The there are the six *transpositions* (of order 2):

$$(12), \quad (13), \quad (14), \quad (23), \quad (24), \quad (34)$$

Then there are three elements which are products of disjoint transpositions, and also have order 2:

$$(12)(34), \quad (13)(24), \quad (14)(23)$$

There are eight 3-cycles which can be grouped into mutually inverse pairs

$$(123), \quad (132), \quad (124), \quad (142), \quad (134), \quad (143), \quad (234), \quad (243)$$

Finally there are six 4-cycles:

$$(1234), \quad (1243), \quad (1324), \quad (1342), \quad (1423), \quad (1432)$$

Thus S_4 has 8 cyclic subgroups of order 2, four cyclic subgroups of order 3, and 3 cyclic subgroups of order 4. An example of the latter is the subgroup:

$$\{e,\ (1234),\ (13)(24),\ (1432)\}$$

Somewhat surprisingly, the three products of disjoint transpositions generate a subgroup of order 4, sometimes called the Klein 4 group. Note that this group is not cyclic because all its non-trivial elements have order 2:

$$\{e,\ (12)(34),\ (13)(24),\ (14)(23)\}$$

With a little more effort one can prove that set

$$\{e, (1234), (1432), (12)(34), (13)(24), (14)(23), (13), (24)\}$$

is a group using Corollary 1.5.7 above. This is an interesting group because it can be identified with the group of symmetries of the square. Consider a square with the vertices numbered clockwise 1 to 4. then for each symmetry identify what permutation of the vertices is produced by applying the symmetry (thus for instance clockwise rotation by 90 degrees yields (1234) and reflection through the 2 - 4 diagonal yields (13). This group is known as the dihedral group. Finally if we look at all the elements of S_4 that can be written as the product of two

transpositions, we again get a subgroup, this time of order 12. This group is known as the alternating group:

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

Again we could prove this directly by showing that it is closed. We will see a more sophisticated and more general proof later.

1.7. Cosets and Lagrange's theorem

DEFINITION 1.7.1. Let G be a group and let H be a subgroup. The left cosets of H in G are the subsets of the form:

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

EXAMPLE 1.7.2. Lets consider a couple of cases inside $G = S_3$. First take $H = \{e, (12)\}$. Then by direct calculation one can see that

$$H = eH = (12)H, \quad (23)H = \{(23), (132)\} = (132)H,$$
$$(13)H = \{(13), (123)\} = (123)H$$

On the other hand if $K = \{e, (123), (132)\}$, then

$$K = eK = (123)K = (132)K, \qquad (12)K = \{(12), (23), (13)\}$$

One notices immediately that all the cosets for a fixed subgroup have the same size and that G is the disjoint union of the different cosets (i.e., the cosets form a partition of G). Both these facts are true in general and they form these observations together provide a proof of Lagrange's Theorem which states that the order of a subgroup divides the order of the group.

EXAMPLE 1.7.3. Let $G = \mathrm{GL}_n(\mathbb{R})$ and let $H = \mathrm{SL}_n(\mathbb{R})$. Let $a \in \mathrm{GL}_n(\mathbb{R})$ be a matrix with $\det a = d$. Then the coset aH is precisely the set of matrices with determinant d.

THEOREM 1.7.4. *Define a relation on G by $g \sim h$ if and only if $g^{-1}h \in H$. Then*

1. *The relation $\sim$ is an equivalence relation on G.*
2. *The equivalence classes for $\sim$ are precisely the left cosets of H in G. That is, $g \sim k$ if and only if $k \in gH$.*
3. *$|gH| = |H|$ for all $g \in G$.*

PROOF. (1) Reflexivity: We know that $e \in H$. So $g^{-1}g \in H$ and hence $g \sim g$ for all $g \in G$. Symmetry: Suppose that $g \sim h$. Then $g^{-1}h \in H$. But then $(g^{-1}h)^{-1} \in H$ also. Since $(g^{-1}h)^{-1} = h^{-1}g$ we find that $h^{-1}g \in H$ and hence that $h \sim g$. Thus $g \sim h \implies h \sim g$. Transitivity: Suppose that $g \sim h$ and $h \sim k$. Then $g^{-1}h \in H$ and $h^{-1}k \in H$. since H is closeed under multiplication, $g^{-1}k = g^{-1}hh^{-1}k \in H$. So $g \sim h$ and $h \sim k$ implies $g \sim k$, as required.

(2) Let $g \in G$. Then

$$\begin{aligned} g \sim k &\iff g^{-1}k \in H \\ &\iff \exists h \in H \text{ such that } g^{-1}k = h \\ &\iff \exists h \in H \text{ such that } k = gh \\ &\iff k \in gH \end{aligned}$$

Thus the equivalence class of g with respect to the relation $\sim$ is the left coset gH.

(3) Let $g \in G$ and define a map $\lambda_g \colon H \to gH$ by $\lambda_g(h) = gh$. Then it is easily checked that λ_g is a bijection. □

DEFINITION 1.7.5. Let G be a group and let H be a subgroup. We denote the number of left cosets of H in G by $[G : H]$.

COROLLARY 1.7.6 (Lagrange's Theorem). *Let G be a finite group and let H be a subgroup. Then $|G| = [G : H]|H|$. In particular $|H|$ divides $|G|$.*

COROLLARY 1.7.7. *Let G be a group whose order is prime. Then G is cyclic and G has no non-trivial proper subgroups.*

PROOF. Since $|G| = p > 1$, it contains an element not equal to the identity, say g. But then $\langle g \rangle$ contains at least two elements (g and e). But $|\langle g \rangle|$ is then a number bigger than 2 and dividing p. Hence $\langle g \rangle = G$ and G is cyclic. □

COROLLARY 1.7.8. *Let G be a group and let $g \in G$. Then $o(g)$ divides $|G|$.*

PROOF. Since $o(g) = |\langle g \rangle|$, the result follows directly from Lagrange's theorem. □

1.8. Homomorphisms, Isomorphisms and Normal Subgroups

DEFINITION 1.8.1. A homomorphism from a group G to a group H is a function $\phi \colon G \to H$ such that

$$\phi(ab) = \phi(a)\phi(b), \qquad \text{for all } a, b \in G$$

EXAMPLE 1.8.2. One of the most natural examples of a homomorphism is the determinat map. Define $D \colon GL_n(\mathbb{R}) \to \mathbb{R}^*$ by $D(A) = \det A$. Since the determinant is multiplicative in the sense that $\det AB = \det A \det B$, this map is a homomorphism of groups.

PROPOSITION 1.8.3. *Let $\phi \colon G \to H$ and $\psi : H \to K$ be homomorphisms of groups. Then $\psi\phi \colon G \to K$ is also a homomorphism.*

PROOF. Let $a, b \in G$. Then

$$\psi\phi(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = \psi\phi(a)\psi\phi(b).$$

□

The *kernel* of a homomorphism is the inverse image of the identity element. That is, if $\phi \colon G \to H$ is a homomorphism,

$$\ker \phi = \{g \in G \mid \phi(g) = e_H\}$$

The kernel of a homomorphism turns out to play a far more important role in the subject than one might at first expect.

LEMMA 1.8.4. *Let $\phi \colon G \to H$ be a homomorphism of groups. Then*

(1) $\ker \phi$ *is a subgroup of* G
(2) *For all* $g \in G$ *and* $k \in \ker \phi$, $gkg^{-1} \in \ker \phi$.
(3) $\phi(G)$ *is a subgroup of* H

PROOF. An easy exercise □

Subgroups satisfying the second property turn out to be particularly important. they are called normal subgroups.

DEFINITION 1.8.5. A subgroup N of a group G is said to be normal if, for all $n \in N$ and $g \in G$, $gng^{-1} \in N$.

Thus the kernel of any homomorphism is a normal subgroup. We shall see shortly that all normal subgroups arise in this way. The kernel turns out to be an extremely important object. The following result is one reason why.

PROPOSITION 1.8.6. *Let $\phi\colon G \to H$ be a homomorphism of groups. Then ϕ is injective if and only if* $\ker\phi = \{e\}$.

PROOF. Suppose that ϕ is injective. The $|\ker\phi| = 1$, so $\ker\phi$ must be the trivial group. Conversely assume that $\ker\phi = \{e\}$. Let $g, g' \in G$ and suppose that $\phi(g) = \phi(g') = h$. Then

$$\phi(g'g^{-1}) = \phi(g')\phi(g)^{-1} = hh^{-1} = e$$

Hence $g'g^{-1} \in \ker\phi = \{e\}$. Thus $g'g^{-1}) = e$, so $g = g'$. Hence ϕ is injective. □

Now we come to the problem of deciding when two groups are the "same". To do this we have to define an equivalence relation on the set of all groups.

DEFINITION 1.8.7. An isomorphism from a group G to a group H is a bijective homomorphism $\phi\colon G \to H$

EXAMPLE 1.8.8. Let

$$H = \{\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \mid r \in \mathbb{R}\}$$

and let $\phi\colon \mathbb{R} \to H$ be the map

$$\phi(r) = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}.$$

It is easily verified that ϕ is an isomorphism form the additive group of real numbers to the matrix group H.

PROPOSITION 1.8.9. *Let G, H and K be groups.*

(1) *The identity map $I\colon G \to G$ is an isomorphism.*
(2) *If $\phi\colon G \to H$ is an isomorphism, then $\phi^{-1}\colon H \to G$ is also an isomorphism.*
(3) *If $\phi\colon G \to H$ and $\psi : H \to K$ are isomomorphisms of groups. Then $\psi\phi\colon G \to K$ is also a isomorphism.*

PROOF. the first part is trivial. The third part follows from the facts that: (a) the compositions of two homomorphisms is a homomorphism and (b) the compositions of two bijections is a bijection.

Let $\phi\colon G \to H$ be an isomorphism. Since ϕ is a bijection we know that ϕ^{-1} exists and is a bijection. Let $c, d \in H$. We want to show that $\phi^{-1}(cd) = \phi^{-1}(c)\phi^{-1}(d)$. Since ϕ is a bijection, we can choose $a, b \in G$ such that $c = \phi(a)$ and $d = \phi(b)$ (hence $a = \phi^{-1}(c)$ and $b = \phi^{-1}(d)$). Since ϕ is a homomorphism,

$$cd = \phi(a)\phi(b) = \phi(ab)$$

Hence,

$$\phi^{-1}(cd) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(c)\phi^{-1}(d)$$

as required. □

We say that two groups G and H are isomorphic if there exists an isomorphism $\phi\colon G \to H$. In this case we write $G \cong H$. Proposition 1.8.9 states that this relation is reflexive, symmetric and transitive. We restate this as a corollary for additional clarity.

COROLLARY 1.8.10. *Let G, H and K be groups.*

(1) $G \cong G$
(2) *If $G \cong H$, then $H \cong G$.*
(3) *If $G \cong H$ and $H \cong K$, then $H \cong K$.*

1.9. Quotient Groups

Recall the definition of a normal subgroup that was given in the previous section: A subgroup N of a group G is said to be *normal* if, for all $n \in N$ and $g \in G$, $gng^{-1} \in N$. Normal subgroup have an enormous number of special properties not shared by general subgroups. The most important property is that the set of left cosets froms a group in an extremely natural way yielding a vast generalization of the concept of modular arithmetic (that is, addition modulo a positive integer).

DEFINITION 1.9.1. let G be a group and let H be a subgroup then the set of left cosets of H in G is denoted G/H and is called the *left coset space.*

Let us introduce some general notation for the product of two subsets of a group. let $S, T \subset G$. Then we define

$$ST = \{st \mid s \in S \text{ and } t \in T\}$$

It is easy to see that for any three subsets, $(ST)U = S(TU)$; thus this product is an associative binary operation on the set of subsets of G. If S is a singleton set, say $S = \{s\}$, we shall write sT for $\{s\}T$ as we did for cosets.

EXAMPLE 1.9.2. Let $G = \mathrm{GL}_n(\mathbb{R})$ and $H = \mathrm{SL}_n(\mathbb{R})$. We observed above that the cosets of H are the sets of matrices of a given determinant. That is, if $H_t = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = t\}$,then

$$G/H = \{H_t \mid t \in \mathbb{R}\}$$

Thus G/H is the set whose elements are the sets H_t. The multiplicativity of the determinant shows that $H_sH_t \subset H_{st}$. A little extra thouhgt showa that any matrix of determinant st can be factored as the product of a matrix of determinant s times a matrix of determinant t. Hence we have that $H_sH_t = H_{st}$. Hence multiplication of subsets is an associative binary operation on G/H and its easy to see that it actually defines a group structure on G/H which is isomorphic to $\mathbb{R}^*$.

In this and the following section we show that this example is a special case of a very general phenomenon.

We begin by rephrasing the definition of normality.

LEMMA 1.9.3. *Let N be a subgroup of a group G. Then the following are equivalent:*

(1) *N is a normal subgroup;*
(2) *For all $g \in G$, $gNg^{-1} = N$*
(3) *For all $g \in G$, $gN = Ng$*

Thus if we have two left cosets, say aN and bN we can multiply them together using the associative operation and we obtain another left coset:

$$(aN)(bN) = a(Nb)N = a(bN)N = ab(NN) = abN.$$

(The above steps are all mechanical except for the fact that $NN = N$, which is left as an exercise.)

THEOREM 1.9.4. *Let N be a subgroup of a group G. Multiplication of cosets defines a group operation on the coset space G/N.*

PROOF. We have already observed that the operation $(aN)(bN) = abN$ is an associative binary operation on G/N. It is clear that the group $N = eN$ itself is an identity for this operation. If aN is a left coset then

$$(aN)(a^{-1}N) = aa^{-1}N = eN$$

so inverses exist. Thus we have verified the three axioms of a group. □

EXAMPLE 1.9.5. Suppose that $G = \mathbb{Z}$ and that N is the subgroup $n\mathbb{Z}$. Then $G/N = \mathbb{Z}/n\mathbb{Z}$ is the group of congruence classes of integers modulo n under addition modulo n.

1.10. The isomorphism theorems

THEOREM 1.10.1 (The First Isomorphism Theorem). *Let G be a group and let $\phi\colon G \to H$ be a homomorphism. then $G/\ker\phi \cong \phi(G)$.*

PROOF. Let $K = \ker\phi$. Define a map $\psi\colon G/K \to \phi(G)$ by $\psi(gK) = \phi(g)$. We must first verify that this map is well-defined: that is, if $gK = g'K$, then $\phi(g) = \phi(g')$. But if $gK = g'K$, then $g' = gk$ for some $k \in K$ and so $\phi(g') = \phi(gk) = \phi(g)\phi(k) = \phi(g)e = \phi(g)$.

Suppose that $\psi(gK) = e_H$, then $\phi(g) = e_H$ and $g \in K$; hence $gK = K = e_{G/K}$, and so ψ is injective.

Let $h \in \phi(G)$. Then $h\phi(g)$ for some $g \in G$. Hence $h = \psi(gK)$, proving that ψ is surjective.

Finally if $gK, g'K \in G/K$, then $\psi(gKg'K) = \psi(gg'K) = \phi(gg') = \phi(g)\phi(g') = \psi(gK)\psi(g'K)$. So ψ is a homomorphism. □

LEMMA 1.10.2. *Let G be a group, let K be a normal subgroup of G and let H be a subgroup of G. Then*

(1) *$HK = KH$ and this is a subgroup of G*
(2) *$H \cap K$ is a normal subgroup of H*

PROOF. Exercise □

THEOREM 1.10.3 (The Second Isomorphism Theorem). *Let G be a group, let K be a normal subgroup of G and let H be a subgroup of G. Then $HK/K \cong H/(H \cap K)$.*

PROOF. Define a map $\phi\colon H \to HK/K$ by $\phi(h) = hK$. Then ϕ is clearly a homomorphism because $\phi(hh') = hh'K = hKh'K = \phi(h)\phi(h')$. Now $\phi(h) = e_{HK/K} \iff \phi(h) = K \iff hK = K \iff h \in K$. So $\ker\phi = H \cap K$. Finally ϕ is clearly surjective since an arbitrary element of HK/K is of the form hkK for some $h \in H$, $k \in K$. Since $kK = K$, $hkK = hK$ and we see that every element

of HK/K is of the form hK for some $h \in H$, as required. The result then follows from the first isomorphism theorem. □

THEOREM 1.10.4 (The Third Isomorphism Theorem). *Let G be a group, let H, K be normal subgroups of G with $H \subset K$. Then K/H is a normal subgroup of G/H and*

$$(G/H)/(K/H) \cong G/K.$$

PROOF. Define $\phi : G/H \to G/K$ by $\phi(gH) = gK$. One shows that ϕ is a well-defined homomorphism with $\ker \phi = K/H$. the result then follows again from the first isomorphism theorem. The details are left as an exercise for the reader. □

THEOREM 1.10.5 (The Fourth Isomorphism Theorem). *Let G be a group and let N be a normal subgroup of G. Then there is a one-to-one correspondence between subgroups of G containing N and subgroups of G/N given by $K \leftrightarrow K/N$. The correspondence also is a one-to-one correspondence between normal subgroups of G containing N and normal subgroups of G/N.*

PROOF. Exercise □

1.11. Classification

Given that we now have a reasonable notion of when two groups are isomorphic, we can ask the natural question: how many different groups of a given order are there? Of course as one gets up to $n = 1,356,490$, this question becomes impossibly difficult and of little interest (except in very special situations). However it as interesting beginner's exercise and helps to put the above concepts into perspective.

Lets first clarify one point which the reader may have intuitively realized.

LEMMA 1.11.1. *All cyclic groups of a fixed order are isomorphic.*

PROOF. Let G be a group of order n. Let α be a generator for G. Define a map $\phi\colon \mathbb{Z} \to G$ by $\phi(n) = \alpha^n$. Then ϕ s a group homomorphism by the laws of exponents. By Proposition 1.4.4 the kernel is $n\mathbb{Z}$ and by the first isomorphism theorem, $G \cong \mathbb{Z}_n$. By transitivity of isomorphism all groups of order n are isomorphic to each other. □

We'll use the notation C_n to denote "the" cyclic group of order n written multiplicatively.

When looking at groups of order 6, one immediately comes up with the examples $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$. In order to determine whether two such groups are isomorphic, one needs a way of showing that a group is isomorphic to a product of two subgroups.

THEOREM 1.11.2. *Let H and K be normal subgroups of a group G. Suppose that $H \cap K = \{e\}$ and $HK = G$. Then $G \cong H \times K$.*

PROOF. Note first that if $h \in H$ and $k \in K$, then $hkh^{-1}k^{-1} \in H \cap K$ (since $hkh^{-1} \in K$ and $kh^{-1}k^{-1} \in H$ by the normailty of H and K). So $hkh^{-1}k^{-1} = e$ and $hk = kh$. now define a mpa $\psi : H \times K \to G$ by $\psi((h,k)) = hk$. Then

$$\psi((h_1,k_1)(h_2,k_2)) = \psi((h_1h_2, k_1k_2)) = h_1h_2, k_1k_2 = h_1k_1h_2k_2 = \psi((h_1,k_1))\phi((h_2,k_2))$$

so ψ is a homomorphism. Since $HK = G$ by assumption, it is surjective. Now suppose that $\psi((h,k)) = e$. Then $hk = e$, so $k = h^{-1} \in H \cap K$. Thus $(h,k) = (e,e)$ and so the kernel of ψ is trivial. So ψ is an isomorphism. □

Corollary 1.11.3. *Suppose that a and b are relatively prime positive integers. Then $C_{ab} \cong C_a \times C_b$.*

Proof. Let α be a generator for G. Then $o(\alpha^a) = b$ and $o(\alpha^b) = a$ (exercise). Hence $H = \langle \alpha^a \rangle$ and $K = \langle \alpha^b \rangle$ are subgroups of order b and a respectively. Since a and b are relatively prime, the intersection $H \cap K$ must be trivial (exercise). Finally since they are relatively prime, there exist s and t such that $as + bt = 1$. Let d be any integer. Then $d = asd + btd$ and $\alpha^d = (\alpha^a)^{sd}(\alpha^b)^{td}$. Hence $C_{ab} = HK$. Applying the theorem yields $C_{ab} = H \times K$. But $H \cong C_b$ and $K \cong C_a$, and the corollary follows. □

The above give two very simple ways of proving that a pair of groups are isomorphic. We also need some general methods of showing easily that two groups are not isomorphic. A property of a group is said to be invariant under isomorphism if whenever a group G has the property and $G \cong H$, then H also has this property. the following properties are isomorphism invariants:

- The order of the group.
- The number of elements of any given order
- The order of the center fof the group.

Now lets begin to look at the possible isomorphism types of a given order n for small n. The first few cases are easy.

- $n = 2$: Since 2 is prime, all groups are cyclic and hence isomorhic to C_2.
- $n = 3$: Just C_3
- $n = 4$: If G has an element of order 4 it is cyclic. Otherwise all its elements have order 2, it is abelian and by Theorem 1.11.2 it is isomorphic to $C_2 \times C_2$.
- $n = 5$: Just C_5.

The case $n = 6$ gives the opportunity for some interesting analysis. If G is cyclic, it is isomorphic to $C_6 \cong C_2 \times C_3$. Suppose that G is abelian. If it had elements of order both 2 and 3, then 1.11.3 would imply that $G \cong C_2 \times C_3$. If it contained only elements of order 2 it would contain a subgroup isomorphic to $C_2 \times C_2$, which is impossible by Lagrange's Theorem. If it had all elements of order 3, it would contain two ditsingt subgroups H and K of order three. But then $HK \cong H \times K$, which is impossible since the latter has order 9. So there are no non-cyclic abelian groups of order 6. Now suppose that G is not abelian. It cannot have all elements of order 2 (exercise), so it must have an element of order 3. It cannot have 5 elements of order 3 because this would yield a pair of cyclic subgroups of order 3 with intersection of order 2. Hence there must be at least one element of order 2. If there were only one such element, it would be central (because if $o(t) = 2$, then $o(gtg^{-1}) = 2$). But as we can see below, a nonabelian group of order 6 cannot have a non-trivial center. thus the group must have 2 elements of order 3 (which necessarily generate a normal subgroup) and three elements of order 2. We see that a non-abelian group of order 6 looks very like S_3. To prove it is isomorphic, we will wait till we have developed further the concept of a group action.

The next interesting case is $n = 8$. Here we have 3 obvious abelian groups: $C_8, C_4 \times C_2$ and $C_2 \times C_2 \times C_2$. By looking at the number of elments of different orders, we see that they are pairwise non-isomorphic. We know one non-abelian group of order 8, the dihedral group D_4. Another group of order 8 is the quaternion

group which can be realised as the following subgroup of $\mathrm{GL}_n(\mathbb{C})$

$$Q = \{\pm I, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\}$$

Again one can verify by looking at orders of elements that Q and D_4 are non-isomorphic. It can be shown that these are all the groups of order 8 up to isomorphism.

1.12. Linear Groups

We have met above the general linear group and the special linear group. Many other interesting groups appear in linear algebra and geometry.

1.12.1. Orthogonal groups. The *orthogonal* group is the group

$$O_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^\top A = I\}$$

It is easily verified that $O_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. Note that since $\det A^\top = \det A$, we must have $(\det A)^2 = 1$; moreover it is easily seen by example that both values can occur for any n. The determinant map $\det\colon O_n(\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism with image $\{1, -1\}$ and kernel

$$SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R}).$$

Hence by the first isomorphism theorem,

$$O_n(\mathbb{R})/SO_n(\mathbb{R}) \cong \mathbb{Z}_2.$$

1.12.2. Symplectic groups. Let J be the $2n \times 2n$ matrix:

$$J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

We define the symplectic group $Sp_{2n}(\mathbb{R})$ by

$$Sp_{2n}(\mathbb{R}) = \{A \in \mathrm{GL}_{2n}(\mathbb{R}) \mid A^\top J A = J\}.$$

1.12.3. Lorentz group. Another interesting group arises as the symmetries of space-time. Note that the definition of the symplectic group in terms of the matrix J would define a subgroup of $\mathrm{GL}_n(\mathbb{R})$ for any matrix J. Define

$$J = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

and set

$$L = \{A \in \mathrm{GL}_4(\mathbb{R}) \mid A^\top J A = J\}$$

1.12.4. Unitary groups. When working over the complex numbers, the natural bilinear form is now the Hermitian form $\langle x, y\rangle = \bar{x}^\top y$ where the bar denotes the complex conjugate. the symmetries of Hermitian space are the unitary matrices

$$U_n = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid \bar{A}^\top A = I\}$$

Again we can look at the determinant map $\det\colon U_n \to \mathbb{R}^*$. If $A \in U_n$ and $\det A = z$, then it follows from the multiplicativity of the determinant that $||z|| = \bar{z}z = 1$. Hence the image of the determinant is contained inside the unit circle S^1 of complex numbers of modulus one. Again one can find suitable matrices A of any such determinant, so that the image of det is the whole of S^1. We define

$$SU_n = U_n \cap SL_n(\mathbb{C})$$

Thus the kernel of det is SU_n and the first isomorphism gives

$$U_n/SU_n \cong S^1$$

CHAPTER 2

Groups Actions

2.1. Group Actions

Definition 2.1.1. Let G be a group and T a set. An action of G on T is a function $\sigma\colon G \times T \to T$ such that, denoting $\sigma(g,t)$ by $g \cdot t$,

(1) For all $g, h \in G$, $t \in T$, $g \cdot (h \cdot t) = (gh) \cdot t$.
(2) For all $t \in T$, $e_G \cdot t = t$.

Given such an action σ we may define maps $\sigma_g : T \to T$ for all $g \in G$ by $\sigma_g(t) = g \cdot t$

Theorem 2.1.2. *Let σ be an action of a group G on a set T. For $g \in G$ define $\sigma_g : T \to T$ by $\sigma_g(t) = g \cdot t$. Then*

(1) *$\sigma_g \in \mathcal{A}(T)$ for all $g \in G$*
(2) *the map $\tilde{\sigma}\colon G \to \mathcal{A}(T)$ given by $\tilde{\sigma}(g) = \sigma_g$ is a homomorphism of groups.*

Conversely, given any group homomorphism $\tau\colon G \to \mathcal{A}(T)$, the map $\hat{\tau}\colon G \times T \to T$ given by $\hat{\tau}(g,t) = \tau(g)(t)$ is a group action.

Proof. First observe that for any $g, h \in G$ and $t \in T$

$$\sigma_g \cdot \sigma_h(t) = \sigma_g(\sigma_h(t)) = g \cdot (h \cdot t)) = (gh) \cdot t = \sigma_{gh}(t)$$

so $(\sigma_g \cdot \sigma_h) = \sigma_{gh}$. This proves that $\sigma_g \cdot \sigma_{g^{-1}} = I_T = \sigma_{g^{-1}} \cdot \sigma_g$. Hence $\sigma_g \in \mathcal{A}(T)$. Obviously the same result now implies that σ is a homomorphism. The proof of the converse is similar. □

Example 2.1.3. The classic example of a group action is the action of a matrix group on the corresponding vector space. For instance, take $G = \mathrm{GL}_n(\mathbb{R})$ and $T = \mathbb{R}^n$. It is clear that the usual matrix multiplication satisfies the axioms above.

Example 2.1.4. The group operation defines an action of G on itself by left multiplication. Let $\lambda_g \in \mathcal{A}(G)$ be the associated permutation of G given by $\lambda_g(h) = gh$ and let $\lambda : G \to \mathcal{A}(G)$ be the map $\lambda(g) = \lambda_g$. The homomorphism λ is called the *left regular representation* of G.

Example 2.1.5. A group can also act on itself by *conjugation*: $g \cdot h = ghg^{-1}$.

Theorem 2.1.6 (Cayley's theorem). *Any finite group is isomorphic to a subgroup of S_n.*

Proof. Let G be a finite group. Consider the left regular representation $\lambda\colon G \to \mathcal{A}(G)$. If $g \in \ker \lambda$, then λ_g is the trivial permutation; that is $gh = \lambda_g(h) = h$ for all $h \in G$. But this implies that $g = e$ by cancelation. Thus $\ker \lambda = \{e\}$ and λ is injective. By the First Isomorphism theorem, g is isomorphic to its image which is a subgroup of $\mathcal{A}(G)$. Since $\mathcal{A}(G) \cong S_{|G|}$, the theorem follows. □

Definition 2.1.7. Let G be a group acting on a set T. Let $Y \subset T$. Define

$$\mathrm{Stab}_G(T) = \{g \in G \mid g \cdot Y = Y\}$$

For instance, let T be the real plane and G the group of rigid motions of the plane. let Y be a figure in the plane (such as a hexagon or the letter H). Then $\mathrm{Stab}_G(Y)$ is the usual symmetry group of the figure Y.

2.2. The Counting Formula

Definition 2.2.1. Let G be a group acting on a set T. Let $t \in T$.

(1) The stabilizer of t in G is defined to be $\mathrm{Stab}_G(t) = \{g \in G \mid g \cdot t = t\}$
(2) The orbit of t under G is defined to be $\mathcal{O}(t) = \{g \cdot t \mid g \in G\}$.

Theorem 2.2.2 (The Counting Formula). *Let G be a group acting on a set T. Let $t \in T$.*

(1) *$Stab_G(t)$ is a subgroup of G*
(2) *If G is a finite group, then $|G| = |Stab_G(t)||\mathcal{O}(t)|$*

Notice that the G-orbits inside T form a partition of T (that is, T is the disjoint union of the orbits. Recall that in this case the orbits must arise from an equivalence relation on T. We can recreate the partition of T by defining this relation.

Let G be a group acting on a set T. define a relation $\sim$ on T by $s \sim t$ if and only if there exists a $g \in G$ such that $t = gs$. It is a routine exercise to verify that this defines an equivalence relation. The equivalence class of $t \in T$ is clearly just the orbit $\mathcal{O}(t)$.

Example 2.2.3. Consider the group D_8 of symmetries of the octagon. Each element of D_8 induces a permutation of the set V of vertices of the octagon. Let v be one such vertex. The stabilizer of v is the set of all symmetries that fix v. clearly this is just the identity and the reflection through v and the opposite vertex. On the other hand the orbit $\mathcal{O}(v)$ is just the set of different vertices to which v can be sent by a symmetry. Since the octagon is regular, this is just the set of all 8 vertices. Thus $|D_8| = 16$. Naturally the same argument shows that the set of symmetries D_n of a regular n-gon has order $2n$.

Example 2.2.4. More interesting examples involve the symmetries of the regular solids. Consider for example the dodecahedron and let D be its group of symmetries. Recall that the dodecahedron has 20 vertices, 30 edges and 12 pentagonal faces. Three faces meet at each vertex. Again fix a vertex v. the stabilizer of v is he set of symmetries that fix v. These consist of the cyclic group of order three of rotations and the three reflections through the edges meeting at the vertex. So $\mathrm{Stab}_D(v) \cong S_3$ and has order 6. On the other hand the orbit of v is just the set of 20 vertices. So $|D| = 20 \times 6 = 120$. the reader will probably easily agree that this is an easier method of finding the order of D than trying to identify all 120 symmetries.

Another way to approach the problem is to notice that the group D acts on the set of faces. If we fix a particular face f, then $\mathrm{Stab}_D(f) \cong D_5$, the group of symmetries of the pentagon, which has order 10. Since the orbit of f has size 12 we again get 120 for the order of the group.

EXAMPLE 2.2.5. We can also derive the usual formula for combinations using the counting formula. Recall that the number of ways of choosing a set of k elements from a set of n elements is given by the binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

We can derive this formula in the following way. Let $T = \{1, 2, \ldots, n\}$ and let $\mathcal{P}(T)$ be the *power set* of T - the set of all subsets. The clearly S_n acts on $\mathcal{P}(T)$ in the natural way and the set of subsets of size k is precisely the orbit of the element $\{1, 2, \ldots, k\} \in \mathcal{P}(T)$. An element of S_n will be in the stabilizer if it separately permutes the sets $\{1, 2, \ldots, k\}$ and $\{k, k+1, \ldots, n\}$. Thus

$$\mathrm{Stab}_{S_n}(\{1, 2, \ldots, k\}) = \mathcal{A}(\{1, 2, \ldots, k\}) \times \mathcal{A}(\{k, k+1, \ldots, n\}) \cong S_k \times S_{n-k}$$

hence the counting formula states that

$$n! = |S_k \times S_{n-k}||\mathcal{O}(\{1, 2, \ldots, k\})| = k!(n-k)! \binom{n}{k}$$

which of course gives us the usual formula for "combinations".

2.3. Action of a group on itself - the class equation

Now we study in more detail the action of a group on itself via conjugation: $g \cdot h = ghg^{-1}$. In this case the stabilizer of an element h is called the set:

$$\begin{aligned} C_G(h) &= \{g \in G \mid ghg^{-1} = h\} \\ &= \{g \in G \mid gh = hg\} \end{aligned}$$

called the centralizer of H; it is the set of elements of G that commute with h. Note that $C_G(h)$ contains the center $Z(G)$ and the subgroup $\langle h \rangle$, so that if $h \neq e$ then $C_G(h)$ is a non-trivial subgroup. Note also that $C_G(h) = G$ if and only if $h \in Z(G)$.

Similarly the orbit of H is called the conjugacy class of h and is the set of elements of G which are conjugate to h:

$$\mathcal{C}(h) = \{ghg^{-1} \mid g \in G\}$$

Interpreting the counting formula in this context yields:

COROLLARY 2.3.1. *Let G be a group and $h \in G$. Then*

$$|\mathcal{C}(g)| = |G|/|C_G(h)| = [G\colon C_G(h)]$$

In particular, the cardinality of a conjugacy class must divide the order of the group. Of course, the conjugacy class $C_G(h)$ must contain h. We say the conjugacy class is trivial if $C_G(h) = \{h\}$. It is easy to see that $C_G(h) = \{h\}$ if and only if $h \in \mathcal{Z}(G)$.

THEOREM 2.3.2 (The class equation). *Let G be a finite group and let $g_1, \ldots, g_t$ be representatives of the non-trivial conjugacy classes of G. Then*

$$|G| = |\mathcal{Z}(G)| + \sum_{i=1}^{t} [G\colon C_G(g_i)].$$

PROOF. Since "being conjugate to" is an equivalence relation, the conjugacy classes of G partition G. For elements in the center, the conjugacy classes are all trivial. Thus these can be lumped together to yield the partition

$$G = \mathcal{Z}(G) \cup \bigcup_{i=1}^{t} \mathcal{C}(g_i)$$

hence

$$|G| = |\mathcal{Z}(G)| + \sum_{i=1}^{t} |\mathcal{C}(g_i)|$$

and the theorem follows from the corollary above. □

The reader should pause to take in the significance of this theorem. the summands on the right all divide $|G|$ and at most one (the first) can be equal to 1.

EXAMPLE 2.3.3. Consider the case when $G = S_3$. The conjugacy classes are $\{e\}$, $\{(12), (13), (23)\}$ and $\{123, (132)\}$, so the class equation is $6 = 1 + 3 + 2$.

Suppose that $|G| = 9$, then the class equation could only be $9 = 3 + 3 + 3$ or $9 = 9$ (the last case of course is the class equation of an abelian group. We see below that the first case can't happen.

COROLLARY 2.3.4. *Let p be a prime and let G be a finite group of order p^t for some positive integer t. Then $\mathcal{Z}(G) \neq \{e\}$.*

PROOF. All the summands of the form $|\mathcal{C}(g_i)|$ on the right hand side are divisors of p^n (and not equal to 1). Therefore they are divisible by p. Since the left hand side is divisible by p, the remaining summand, $|\mathcal{Z}(G)|$ must also be divisible by p. Hence $\mathcal{Z}(G) \neq \{e\}$. □

COROLLARY 2.3.5. *Let p be a prime and let G be a finite group of order p^2. Then G is abelian.*

PROOF. Exercise. □

Note that the example of S_3 shows that a group of order pq with $p \neq q$ does not need to be abelian.

2.4. Sylow's Theorem

Sylow's theorem represents one of the high points of elementary group theory, combining simple ideas to prove a complex and surprising result.

The theorem consists of three parts, the first of which is a partial converse to Lagrange's Theorem. Recall that Lagrange's Theorem states that if G is a finite group of order n and if H is a subgroup of order k, then $k|n$. We turn this around to ask whether for any k dividing n whether there exists a subgroup of order k. In general the answer to this question is "No". Sylow's Theorem answers this question when k is a largest possible power of a prime.

Let G be a group of order $n = p^e m$ where $\gcd(p, m) = 1$. In its simplest from Sylow's Theorem has three parts:

- There exists subgroups of G of order p^e.
- All such subgroups are conjugate.
- The number of such subgroups divides m and is congruent to 1 modulo p.

To prove Sylow's Theorem we shall make use of some further group actions on sets connected to G.

Let $\mathbb{S}$ be the set of subgroups of G. We know that if H is a subgroup, then so is any conjugate gHg^{-1}. hence G acts on $\mathbb{S}$ by conjugation. That is, we define an action of G on $\mathbb{S}$ by:

$$\text{For any } g \in G, \qquad g \cdot H = gHg^{-1}$$

Then the stabilizer of a subgroup under this action is the normalizer of the subgroup,

$$\mathrm{Stab}_G H = \{g \in G \mid gHg^{-1} = H\} = \mathcal{N}_G(H)$$

The orbit is just the set of subgroups conjugate to H, so part (2) above can be restated as saying the subgroups of order p^e from a single orbit under this action.

Definition 2.4.1. Let G be a finite group and let p be a prime dividing $|G|$. Suppose that p^e is the highest power of p dividing n. A subgroup of G of order p^e is called a *Sylow p-subgroup* of G.

Lemma 2.4.2. *Let G be a finite abelian group of order n and let p be a prime dividing n. Then G contains a subgroup of order p.*

Proof. We work by (complete) induction on $n = |G|$. The case where $n = 2$ is trivial.

Now suppose that the result is true for all abelian groups of order less than n. Clearly it suffices to find an element of G of order p. We may certainly pick a non-trivial element $g \in G$. Let $o(g) = m$. If $p \mid m$, then we may write $m = pm'$ and $o(g^{m'}) = p$.

On the other hand suppose that $p \not| m$. Let $N = \langle g \rangle$. Then N is a (normal) subgroup of order m and the quotient group G/N has order n/m, which is smaller than n but still divisible by p (since $p \not| m$.By induction G/N contains an element of order p, say hN. This means that $h^p N = (hN)^p = N$ and hence that $h^p \in N$. Since $h \notin N$, this implies that $\langle h^p \rangle$ is strictly contained in $\langle h \rangle$ and hence that $o(h^p) < o(h)$. But we know that

$$o(h^p) = \frac{o(h)}{\gcd(p, o(h))}$$

This implies that $\gcd(p, o(h)) \neq 1$ and hence, since p is prime that $p|o(h)$. Returning to the argument above, this yields an element in G of order p. □

Theorem 2.4.3. *Let G be a finite group of order n. Sylow p-subgroups exist for all p dividing n.*

Proof. We prove the result by complete induction on $n = |G|$. Clearly the result is true when $n = 2$. Assume that the result is true for all groups of order $k < n$.

Let p be a prime dividing n. Suppose first that $p \not| \mathcal{Z}(G)$. Looking at the class equation we see that p cannot divide all the remaining terms on the right. So there must exist a $g \in G$ such that $[G\colon C_G(g)]$ is not divisible by p. But in this case $|C_G(g)| = p^e m'$ where $\gcd(p, m') = 1$ and $m' < m$. By induction $C_G(g)$ has a subgroup H of order p^e and H is clearly a Sylow p-subgroup of G.

Now assume that $p|\mathcal{Z}(G)$. By the lemma, $\mathcal{Z}(G)$ contains a subgroup N of order p. Since N is contained in the center of G it is a normal subgroup of G. By induction G/N contains a Sylow p-subgroup, K, which has order p^{e-1}. let

$\phi\colon G \to G/N$ be the natural surjection and let $H = \phi^{-1}(K)$. Then $K \cong H/N$ by the first isomorphism theorem, so $|H| = p.p^{e-1} = p^e$. Hence H is a Sylow p-subgroup of G. □

The next lemma touches on one of the crucial properties of Sylow subgroups: no element of one Sylow p-subgroup can normalize non-trivially another one. That is if P and P' are two Sylow p-subgroups and $x \in P$ satisfies $xP'x^{-1} = P'$, then $x \in P'$.

LEMMA 2.4.4. *Let P and P' be two Sylow p-subgroups. Then $P \cap \mathcal{N}_G(P') = P \cap P'$.*

PROOF. Let $N = \mathcal{N}_G(P')$ and let $Q = P \cap N$. Then applying the second isomorphism theorem to N and the subgroups Q and P', yields

$$\frac{QP'}{P'} \cong \frac{Q}{Q \cap P'}$$

This implies that the order of QP'/P' is of the form p^f for some non-negative integer f and that $|QP'| = |QP'/P'||P'| = p^{e+f}$ contradicting Lagrange's Theorem unless $f = 0$. hence $Q \subset P'$ as required. □

THEOREM 2.4.5. *Let G be a finite group of order n and let p be a prime dividing n.*

(1) *All Sylow p-subgroups are conjugate to each other.*
(2) *Let n_p be the number of Sylow p-subgroups of G. Then*

$$n_p | m \qquad \textit{and} \qquad n_p \equiv 1 \pmod{p}.$$

PROOF. Let P be a Sylow p-subgroup. Let $\mathcal{P} = \{gPg^{-1} \mid g \in G\}$ be the set of conjugates of P; lets denote theses conjugates by $P_1, \ldots, P_s$, so that $\mathcal{P} = \{P = P_1, \ldots, P_s\}$. Then P itself acts on $\mathcal{P}$ by conjugation. An orbit will be a singleton set $\{P_i\}$ if and only if $P \subset \mathcal{N}_G(P_i)$. But this can only happen if $P = P_i$ by the lemma. hence $\{P\}$ is the only trivial orbit; all the other orbits must have more than one element and hence, because $|P| = p^e$, the size of these orbits is divisible by p. This proves that the number of conjugates of P is congruent to 1 modulo p.

Now let P' be any other Sylow p-subgroup. Again we let P' act on $\mathcal{P}$ and consider the orbit decomposition. the size of the orbits must be a power of p. Thus at least one orbit must be trivial; otherwise we would conclude that $p||\mathcal{P}$, contradicting the conclusion of the previous paragraph. Suppose this orbit is $\{P_i\}$. Then $P' \subset \mathcal{N}_G(P_i)$. By the lemma, this implies that $P = P_i$. Hence every Sylow p-subgroup is conjugate to P, proving (1). Thus n_p equal to the number of conjugates of P; hence $n_p \equiv 1 \pmod{p}$. Finally, applying the Counting Theorem to the action of G on subgroups, we see that $n_p = [G\colon \mathcal{N}_G(P)]$. But $[G\colon \mathcal{N}_G(P)][\mathcal{N}_G(P)\colon P] = [G\colon P] = m$, so $n_p|m$. □

EXAMPLE 2.4.6. As an easy illustrative example, consider the group D_5 of symmetries of the regular pentagon. Recall that D_5 has order $10 = 2.5$ and its elements are the identity, four non-trivial rotations and five reflections. The theorem states that the number of Sylow 5-subgroups must divide 2 and be congruent to 1 modulo 5. Thus there is a single normal subgroup of order 5; of course this is the group consisting of the identity and the four non-trivial rotations. On the other hand the theorem states that in a group of order 10 the number of Sylow

2-subgroups must divide 5 and be congruent to 1 modulo 2. Hence it must be 1 or 5. Clearly in the case of D_5, the answer is 5 and these groups are the 5 cyclic groups of order 2 generated by the reflections.

As a first application we see that "most" groups of order pq are abelian (of course S_3 is an example that shows that this is not always true).

THEOREM 2.4.7. *Let G be a group of order pq where p and q are primes and $p < q$. If p does not divide $q - 1$, then G is abelian.*

PROOF. Consider the number n_q of Sylow q-subgroups. Then $n_q | p$ and $n_q \equiv 1 \pmod{q}$. hence $n_q = 1$ and there is only one Sylow q-subgroup, say H, which must then be normal.

Now consider the number n_p of Sylow p-subgroups. Then $n_p | q$ and $n_p \equiv 1 \pmod{p}$. If $n_p = q$, this would imply that $p|(q-1)$, which is not possible. hence $n_p = 1$ also. Let the unique Sylow p-subgroup be K. By Lagrange's Theorem, $H \cap K = \{e\}$. Now HK must be a subgroup that is properly bigger than K, so its order is greater than q and by Lagrange's Theorem divides pq. Hence $HK = G$. Thus by Lemma 1.11.2, $G \cong H \times K \cong C_q \times C_p$ and in particular, G is abelian. □

If there is only Sylow sp-sugroup for some p, then we know that this subgroup must be normal. Thus the Sylow theorems provide us with a method of proving that a grop has a proper non-trivial normal subgroup. This turns out to be an extremely important question. Groups that do not have proper non-trivial normal subgroups are called simple groups and form the fundamental building blocks of finite group theory as we shall see in the next chapter.

DEFINITION 2.4.8. A group is said to be *simple* if it has no non-trivial proper normal subgroups.

Cyclic groups of prime order are simle because they have no non-trivial proper subgroups at all. Conversely, an abelian simple group muct be cyclic of prime order (why?). At this stage it is not at all obvious whether it is possible for a groups to have non-trivial proper subgroups yet still be simple (because none of them are normal). We shall answer this question in the next section. Our next result says that if there are any such groups, they have to have at least 60 elements. Its proof is one of the most satisfying exercises in elemetary group theory, so I won't spoil the fun by providing the proof.

THEOREM 2.4.9. *There are no non-abelian simple groups of order less than sixty.*

PROOF. Exercise. □

2.5. The Alternating Groups

Continuing with our theme of group actions, we consider a canonical action of the symmetric group S_n on the vector space $\mathbb{R}^n$. this allows us easily to identify the *alternating group*, the subgroups of S_n consisting of permutations that can be represented as a product of an even number of transpositions. the alternating groups are among the most important families of finite groups and their structure plays a key role in explaining the non-existence of a formula for the solutions of a quintic equations.

PROPOSITION 2.5.1. *let $\sigma \in S_n$ and let $\sum \lambda_i e_i \in \mathbb{R}^n$, where $\lambda_i \in \mathbb{R}$. Define $\pi_\sigma \colon \mathbb{R}^n \to \mathbb{R}^n$ by*

$$\pi_\sigma \left(\sum \lambda_i e_i \right) = \sum \lambda_i e_{\sigma(i)}$$

Then π_σ is an invertible linear transformation and $\pi_\sigma \pi_{\sigma'} = \pi_{\sigma\sigma'}$.

Let $\pi \colon S_n \to \mathrm{GL}_n(\mathbb{R})$ be the map $\pi(\sigma) = \pi_\sigma$. Then π defines an action of S_n on $\mathbb{R}^n$. Note that since $\pi_\sigma(e_i) = e_{\sigma(i)}$, π_σ is the matrix with a 1 in the $(\sigma(i), i)$-th position and zeros everywhere else. These matrices are known as *permutation matrices*.

EXAMPLE 2.5.2. Consider explicitly the case when $n = 3$. Then

$$\pi((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \pi((13)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \pi((23)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

and

$$\pi((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \pi((132)) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Notice that the determinant of any permutation matrix is ± 1 since there is exactly one term in the usual expansion of the determinant that is non-zero for such matrices and this term is ± 1. The composition $sgn = \det \circ \pi \colon S_n \to \{\pm 1\}$ is a homorphism and is known as the sign representation.

DEFINITION 2.5.3. The kernel of the map sgn is called the *alternating group* and is denoted by A_n.

Note that A_n must have $n!/2$ elements by the first isomorphism theorem since S_n has $n!$ elements and $S_n/A_n \cong C_2$.

EXAMPLE 2.5.4. The alternating group A_4 is the subgroup consisting of all three cycles and products of disjoint transpositions:

$$\{e, (123), (132), (134), (143), (124), (142), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

Sylow's theorem predicts that the number of Sylow 3-subgroups must be 1 or 4; clearly in this case the answer is 4, the eight 3-cycles splitting into 4 mutually inverse pairs. On the other hand the number of Sylow 2-subgroups should be either 1 or 3; clearly the answer here is 1. The group $V = \{e, (12)(34), (13)(24), (14)(23)\}$ is the unique Sylow 2-subgroup.

We now look more closely at the group A_5 and prove that it is simple. Up to this point we know that the cyclic groups of prime order are simple but we know of no other examples. We also know that no non-abelian group of order less than 60 can be simple. Thus A_5 is the smallest non-abelian simple group. Its simplicity is intimately connected with the Abel-Ruffini theorem that there is no algebraic formula for the roots of a quintic polynomial.

The group A_5 has 60 elements, too many to write out explicitly. One can however look at the number of elements of different types. In addition to the identity element we see, using some straightforward counting arguments, that we have:

- 20 3-cycles such as (123).

- 24 5-cycles such as (12345).
- 15 products of two disjoint 2-cycles such as (12)(34).

Now the orders of elements of A_5 that are possible from Lagrange's Theorem are the divisors of 60, namely $1, 2, 3, 4, 5, 6, 10, 12, 15, 20$ and 30. But only $1, 2, 3$ and 5 actually occur. *This is an important illustration of the fact that k divides $|G|$ does not necessarily imply that there exist an element of order k.*

Lets look at the Sylow subgroups. Note that $60 = 2^2.3.5$. The Sylow 3-subgroups have order 3, so they must be cyclic. The number of them should be congruent to 1 modulo 3 and must divide 20, so the options are 1, 4 and 10. Since each of the 3-cycles above generates a cyclic subgroup of order 3 which contains it and one other 3-cycle, its clear that there are 10 such Sylow 3-subgroups. Similarly the Sylow 5-subgroups are cyclic of order 5, and the number of them must divide 12 and be congruent to 1 module 5. So its clear that there must be 6 Sylow 5-subgroups. Finally the Sylow 2-subgroups are of order 4 and the number of them is congruent to 1 modulo 4 and divides 15. The possibilities are 1 or 5. But there are 5 subgroups similar to the Klein group $\{e, (12)(34), (13)(24), (14)(23)\}$. so the answer is obviously five.

Now lets review the class equation for A_5. Recall that the class equation comes from the partition of G into conjugacy classes. The equation itself describes the order of G as the sum of (a) the order of the center, which is the union of the trivial conjugacy classes; and (b) the orders of the non-trivial conjugacy classes.

First recall the following basic fact about conjugation inside S_n.

LEMMA 2.5.5. *Let $\pi \in S_n$ and let $(a_1 a_2 \dots a_t)$ be a t-cycle. Then*

$$\pi(a_1 a_2 \dots a_t)\pi^{-1} = (\pi(a_1)\pi(a_2)\dots\pi(a_t))$$

hence all t-cycles are conjugate in S_n.

Thus the three cycles in S_5 form a single conjugacy class. Of course its not completely clear that they are still conjugate inside the subgroup A_5. Recall that $|G| = |\mathcal{C}(g)|.|C_G(h)|$. Since $|\mathcal{C}_{S_5}((123))| = 20$, the size of the centralizer of (123) must be 6. But the centralizer contains (123) and (45) and together these generate the group of order 6, so we must have:

$$C_{S_5}((123)) = \{e, (123), (132), (45), (123)(45), (132)(45)\}$$

But then

$$C_{S_5}((123)) = C_{S_5}((123)) \cap A_5 = \{e, (123), (132)\}$$

Hence, the order of the conjugacy class of (123) in A_5 must be $60/3 = 12$ and therefore all of the 3-cycles are still conjugate in A_5.

A similar argument can be applied to the 5-cycles but with a different result. the 24 5-cycles are conjugate in S_5. therefore $|C_{S_5}((12345))| = 120/24 = 5$; hence $C_{S_5}((12345)) = \langle(12345)\rangle$. Thus,

$$C_{A_5}((12345)) = C_{S_5}((12345)) \cap A_5 = \langle(12345)\rangle$$

Hence, the order of the conjugacy class of (12345) in A_5 must be $60/5 = 12$. Thus inside A_5 the 5-cycles fall into two distinct conjugacy classes of size 12.

A similar argument applied to the products of disjoint transpositions yields a single conjugacy class of size 15. hence the class equation of A_5 reads:

$$60 = 1 + 12 + 12 + 15 + 20$$

Interestingly, the simplicity of A_5 is an easy consequence of this.

THEOREM 2.5.6. *The group A_5 is simple*

PROOF. The key observation is that any normal subgroup must be a union of conjugacy classes; for the definition of normality can be interpreted as the statement that a group is normal if and only if contains all conjugates of any of its elements. Thus if K is a proper non-trivial normal subgroup, its order must be a "subsum' of the right hand side of the class equation that includes the first term. The only possibilities less than 30 are:

$$13, 16, 21, 25, 28$$

and clearly none of these numbers divide 60. Hence no proper non-trivial normal subgroup exists. □

More generally, on can prove that the alternating group A_n is simple for all $n \geq 5$. The proof can be found in most abstract algebra introductory texts.

CHAPTER 3

Composition series and solvable groups

3.1. Composition series

One of the fundamental theorems in number theory is the unique factroization theorem which states that every number can be expressed in a unique way as a product of primes. Interestingly an analogous result holds for groups. If $N \triangleleft G$, then we can think of N and G/N as being "factors" of G. We can then try and "factorize" N and G/N. If G is finite this process must stop and at this point we have reduced down to simple groups, which play the role of primes in group theory.

Definition 3.1.1. A *normal series* for a group G is a finite sequence of subgroups, $G_0 = \{e\} \subset G_1 \subset G_2 \subset \ldots G_t = G$ such that $G_i \triangleleft G_{i+1}$. The *length* of the series is defined to be t.

Definition 3.1.2. A *composition series* is a normal series in which all the factor groups are simple

Example 3.1.3. Let G be S_4. Recall the definition of the Klein 4-group V and let $C = \{e, (12)(34)\}$. Then

$$\{e\} \triangleleft C \triangleleft V \triangleleft A_4 \triangleleft S_4$$

is a composition series for S_4. Note that the definition of normal series does *not* require that the terms of the series be normal in the group G. In the case above V and A_4 are normal in G but C is not.

The unique factorization theorem for integers has two parts. One is the existence part which states that every integer can be factored as a product of primes. The second is the uniqueness part which states that there there is only one way of factoring a number into a product of primes. The analogous result for groups has two similar parts: (1) composition series always exist for finite groups; and (2) the set of composition factors is the same for any composition series.

Proposition 3.1.4. *Any finite group has a composition series.*

Proof. We use induction on $n = |G|$. The case $n = 1$ is trivial. Consider the set of all proper normal subgroups of $|G|$ and pick one, say N, whose order is as large as possible. By the fourth isomorphism theorem G/N is simple. Now $|N| < n$, so by induction, N has a composition series,

$$N_0 = \{e\} \triangleleft N_1 \triangleleft N_2 \triangleleft \ldots \triangleleft N_s = N$$

Then clearly $N_0 \triangleleft N_1 \triangleleft N_2 \triangleleft \ldots \triangleleft N_s \triangleleft G$ is a normal series for G. $\square$

3.2. The Jordan Holder Theorem

Suppose that G is a finite abelian group of order n and let $G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_t = G$ be a composition series for G. Then the composition factors must all be abelian simple groups; that is, they are isomorphic to a cyclic group of prime order, say $G_i/G_{i-1} \cong C_{p_i}$. By Lagrange's Theorem, $n = p_1 \ldots p_t$. Thus while there may be many different composition series for G, the length of any composition series is equal to t, the number of primes in the prime factorization of n; and the collection of composition factors is the same in the sense that the types of composition factors that occur and the number of times they occur is invariant. For instance, if $G = \langle \alpha \rangle$ is an abelian group of order 60 then

$$\{e\} \triangleleft \langle \alpha^{12} \rangle \triangleleft \langle \alpha^{6} \rangle \triangleleft \langle \alpha^{2} \rangle \triangleleft G$$

and

$$\{e\} \triangleleft \langle \alpha^{20} \rangle \triangleleft \langle \alpha^{10} \rangle \triangleleft \langle \alpha^{5} \rangle \triangleleft G$$

are both composition series with composition factors C_5, C_2, C_3, C_2 and C_3, C_2, C_2, C_5 respectively. We can thus think of a composition series in some way as a "prime factorization" for a finite group. The Jordan Holder Theorem is then the analog of the unique factorization theorem for integers. Its states that composition series are unique in the sense that they have the same length and that the set of composition factors occuring, counted with multiplicity is the same for any such series.

Definition 3.2.1. Let G be a group and let $G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_s = G$ and $H_0 = \{e\} \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_t = G$ be two normal series for G. We say that the series are *equivalent* if $s = t$ and there exists a bijection between the sets of factor groups for which corresponding factors are isomorphic.

Theorem 3.2.2 (Jordan-Holder). *Any two composition series of a finite group are equivalent.*

Proof. We shall prove the theorem by induction on the s length of the shorter series. Clearly if $s = 1$, then G is simple, so the result is clearly true. Now assume that $G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_s = G$ and $H_0 = \{e\} \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_t = G$ are two composition series with $s \leq t$. If $G_{s-1} = H_{t-1}$ then the result from the induction hypothesis applied to G_{s-1}. Otherwise $G_{s-1}H_{t-1}$ is a normal subgroup of G strictly bigger than G_{s-1}. Since G/G_{s-1} is simple, the fourth isomorphism theorem tells us that $G_{s-1}H_{t-1} = G$. Therefore,

$$\frac{G_{s-1}}{G_{s-1} \cap H_{t-1}} \cong \frac{G_{s-1}H_{t-1}}{H_{t-1}} = \frac{G}{H_{t-1}}$$

and

$$\frac{H_{t-1}}{G_{s-1} \cap H_{t-1}} \cong \frac{G_{s-1}H_{t-1}}{G_{s-1}} = \frac{G}{G_{s-1}}$$

Now let

$$\{e\} \triangleleft K_1 \triangleleft K_2 \triangleleft \ldots \triangleleft K_u = G_{s-1} \cap H_{t-1}$$

be a composition series for $G_{s-1} \cap H_{t-1}$. Then

$$\{e\} \triangleleft K_1 \triangleleft K_2 \triangleleft \ldots \triangleleft K_u \triangleleft G_{s-1}$$

is a composition series for G_{s-1}, as is

$$\{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_{s-1}$$

Thus, by induction, $u = s-2$ and the two series are equivalent. A similar argument shows that

$$\{e\} \triangleleft K_1 \triangleleft K_2 \triangleleft \ldots \triangleleft K_u \triangleleft H_{t-1}$$

is equivalent to

$$\{e\} \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_{t-1}$$

and $u = t-2$. Hence $s = t$ and by combining all the above information we see that the two original series are equivalent. □

3.3. Solvable groups

If G is an abelian group, its composition factors must also be abelian. However, the converse is far from true, as the examples of S_3 and S_4 illustrate. It is quite possible for a non-abelian group to have abelian composition factors. Thes kind of groups turn out to be extremely important.

Definition 3.3.1. A group G is said to be solvable if it has a normal series

$$G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_t = G$$

for which the factors G_i/G_{i-1} are abelian.

This definition works for both finite and infinite groups. For finite groups one can equivalently define a solvable group to be one whose composition factors are all abelian. The symmetric groups S_3 and S_4 are solvable but S_5 is not (since its composition factors are A_5 and C_2). More generally, the fact that there are no non-abelian simple groups of order less than 60 implies that all groups of order less than 60 are solvable and that A_5 is the smallest group that is not solvable.

The following result about solvable grops is of fundamental importance.

Theorem 3.3.2. *Let G be a group and H a normal subgroup. Then G is solvable if and only if both H and G/H are solvable.*

Proof. Suppose that G is solvable. Then there exists a normal series

$$G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_t = G$$

for which the factors G_i/G_{i-1} are abelian. Let $H_i = G_i \cap H$. Then for any $k \in H_{i-1}$ and $h \in H_i$, then $hkh^{-1} \in G_{i-1} \cap H = H_{i-1}$, so the H_i form a normal series for H. Moreover, using the second isomorphism theorem,

$$\frac{H_i}{H_{i-1}} = \frac{G_1 \cap H}{G_{i-1} \cap H} = \frac{G_i \cap H}{G_{i-1} \cap (G_i \cap H)} \cong \frac{G_{i-1}(G_i \cap H)}{G_{i-1}} \subset \frac{G_i}{G_{i-1}}$$

Hence H_i/H_{i-1} is abelian, and H is solvable. Similarly, let $K_i = G_iH/H$. Then $K_0 = \{e\} \triangleleft K_1 \triangleleft K_2 \triangleleft \ldots \triangleleft K_t = G/H$ is a normal series for G/H. Using both the second and third isomorphism theorems we see that

$$\frac{K_i}{K_{i-1}} = \frac{G_iH/H}{G_{i-1}H/H} \cong \frac{G_iH}{G_{i-1}H} = \frac{G_i(G_{i-1}H)}{G_{i-1}H} \cong \frac{G_i}{G_{i-1}H \cap G_i} \cong \frac{G_i/G_{i-1}}{G_{i-1}H \cap G_i/G_{i-1}}$$

Thus K_i/K_{i-1} is a homomorphic image of G_i/G_{i-1} and hence is abelian. Thus G/H is solvable.

The converse we leave as an exercise. □