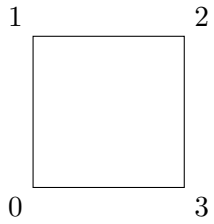
Math 328: Introduction to Group Theory
University of Alberta, Fall 2021

Adam Topaz

Last updated: December 6, 2021

1 Introduction

In a few words, groups are a formal way to capture symmetry in mathemtics. For example, we might be interested in the symmetries of the square:



Imagine that you can pick up this square, move it around in space, and place it back on the desk so that the corners and edges line up with the original shape. We can encode such a symmetry by keeping track of where the corners go, with the only restriction being that the adjacency is preserved. There are a total of eight such symmetries. See if you can write them all down! How many prerserve the orientation?

Alteranatively, we might be interested in the symmetries of the roots of a polynomial equation. For example, the equation

$$X^2 - 2 = 0$$

has two solutions $X = \sqrt{2}$ and $X = -\sqrt{2}$. If we consider the collection of real numbers which can be written as successive sums and products of rational numbers along with $\sqrt{2}$, any such number can be written in a unique way as

$$a + b \cdot \sqrt{2}, \quad a, b \in \mathbb{Q}.$$

We can then study the symmetries of this collection of numbers which preserve the arithmetic operations (addition, multiplication, negation, 0 and 1). Some experimentation will lead to the property that any such symmetry is determined by the image of $\sqrt{2}$, and this image must again be a root of X^2-2. In other words, the only nontrivial symmetry is the one which sends $\sqrt{2}$ to $-\sqrt{2}$. What happens if we replace X^2-2 with X^3-2?

Another example we might consider is the collection of symmetries of $\mathbb{R}^2$ which preserve the linear structure, the orientation, and volumes. In concrete terms, these are the linear endomorphisms of $\mathbb{R}^2$ whose determinant is 1:

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{R},\ a\cdot d - b\cdot c = 1 \right\}.$$

The key property all of these examples have in common, is that the symmetries involved can be *composed* to produce a new symmetry. For example, in the third example, the product of two 2×2 matrices whose determinant is 1 is again a matrix whose determinant is 1.

2 Definitions

2.1 Basics

Let's start with the definition of a group.

Definition 2.2. A *group* is a set G endowed with a binary operation

$$(-\cdot -) : G\times G \to G$$

satisfying the folloowing axioms:

1. For all $a,b,c \in G$, one has $(a\cdot b)\cdot c = a\cdot(b\cdot c)$, i.e. $(-\cdot -)$ is associative.
2. There exists an element $e\in G$, called the *identity* or *neutral element*, such that for all $a\in G$, one has $a\cdot e = e\cdot a = a$. We will often denote such an element using the symbol 1.
3. For each $a\in G$, there exists an element $a^{-1}\in G$, called the *inverse* of g, such that one has $g\cdot g^{-1} = g^{-1}\cdot g = e$, with e an identity element as above.

A group G is called *abelian* provided that for all $g,h\in G$, one has $g\cdot h = h\cdot g$.

This is the most common definition that appears in the literature. One point to note is that to specify a group, one first specifies the set G and the operation $(- \cdot -)$ as data, then one must prove that the three axioms hold true. It's possible to consider the identity and inversion as data as well, due to the following lemma.

Lemma 2.3. *Let G be a group. The following hold:*

1. *The identity element is unique.*
2. *For each $a \in G$, the inverse a^{-1} is uniquely determined by a.*

Proof. If e and e' are both neutral elements in G, then

$$e = e \cdot e' = e'.$$

If b, b' are both inverses for $a \in G$, then

$$b = b \cdot e = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'. \qquad \square$$

Then $\cdot$ is used for the binary operation of a group, the neutral element will usually be denoted by 1, and inversion denoted by $g \mapsto g^{-1}$. When we want to explicitly specify the binary operation $\cdot$ of a group G, we will write, for example, $(G, \cdot)$. In some situations, we will use the notation $+$ for the binary operation, in which case the neutral element will be denoted by 0 and inversion will be denoted by negation $x \mapsto -x$.

Example 2.4. There are various familial exampels of groups. For instance, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are all (additive) groups. The set of positive reals $\mathbb{R}_{>0}$ is a group with respect to multiplication of real numbers. The set of invertible $n \times n$ matrices over $\mathbb{R}$ is a group under matrix multiplication.

Here are a few additional important properties that hold true in any group.

Lemma 2.5. *Let G be a group. The following hold:*

1. *One has $(a^{-1})^{-1} = a$ for all $a \in G$.*
2. *One has $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ for all $a, b \in G$.*
3. *For any sequence of elements $a_1, \ldots, a_n \in G$, the value $a_1 \cdot a_2 \cdots a_n$ is independent of how this expression is parenthesized.*

2.6 Solving equations

Let G be a group and let $a, b \in G$ be given. Suppose we wish to "solve" for x and y in the following expressions:

$$a \cdot x = b, \quad y \cdot a = b.$$

The standard approach is to multiply on the correct side by a^{-1} to "cancel" the a on the left, leaving with an expression of the form $x =?$ or $y =?$. For the first equation, multiply on the left by a^{-1} to obtain

$$x = 1 \cdot x = a^{-1} \cdot a \cdot x = a^{-1} \cdot b.$$

Similarly, multiply the second equation on the right by a^{-1} to obtain

$$y = y \cdot 1 = y \cdot a \cdot a^{-1} = b \cdot a^{-1}.$$

These solutions turn out to be unique, due to the following.

Lemma 2.7. *Let $a, b, u, v \in G$ be given. One has $a \cdot u = a \cdot v$ iff $u = v$. One has $u \cdot b = v \cdot b$ iff $u = v$. Thus, the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions $x = a^{-1} \cdot b$ and $y = b \cdot a^{-1}$.*

Exercise 2.8. Suppose that G is a group and $a, b \in G$ are given. Prove that $a = b^{-1}$ iff $a \cdot b = 1$ iff $b \cdot a = 1$.

2.9 Multiplication tables

Definition 2.10. If G is a finite group enumerated as $G = \{g_1, \ldots, g_n\}$, then the *multiplication table* associated to G (and the enumeration of G) is the $n \times n$ table whose (i, j)-th term is the product $g_i \cdot g_j$.

The multiplication table of a group is one explicit way to describe the binary operation of the group G, hence the group structure itself. We will often regard two multiplication tables as *equivalent* if they only differ by relabeling the elements of G.

For example, we can classify all groups G such that $\#G = 3$, using a multiplication table up-to relabeling, as follows. First, let us enumerate G as $G = \{a, b, c\}$. One of these elements must be $1 \in G$, so we may as well say $1 = a$ (again, we ignore differences in labeling). Thus $G = \{1, b, c\}$. We can thus start to fill in the multiplication table as follows:

	1	b	c
1	1	b	c
b	b		
c	c		

Suppose that $b \cdot b = 1$. In this case, if $b \cdot c = 1$ then $c = b \cdot b \cdot c = b$, which cannot happen, hence $b \cdot c \in \{b, c\}$. If $b \cdot c = b$ then $c = 1$ and if $b \cdot c = c$ then $b = 1$, neither of which can happen. We deduce that $b \cdot b \neq 1$. If $b \cdot b = b$ then $b = 1$ which cannot happen, hence it must be the case that $b \cdot b = c$. We obtain:

	1	b	c
1	1	b	c
b	b	c	
c	c		

Note also that $b \cdot c \notin \{b, c\}$ arguing similarly as above, hence $b \cdot c = 1$.

	1	b	c
1	1	b	c
b	b	c	1
c	c		

We can argue similarly (or by symmetry) to fill in the last row as follows.

	1	b	c
1	1	b	c
b	b	c	1
c	c	1	b

We have thus found that there is a *unique* multiplication table for a group of order 3, up-to relabelling the elements of G.

2.11 Exponentiation and orders

Suppose that G is a group, $g \in G$ and $n \in \mathbb{N}$ are given. We define g^n inductively as follows:

$$g^0 = 1, \quad g^{n+1} = g^n \cdot g.$$

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

Lemma 2.12. *In the above context, suppose that $a, b \in \mathbb{Z}$ are two integers. Then one has $g^{a+b} = g^a \cdot g^b$ and $(g^a)^b = g^{a \cdot b}$.*

Proof. Use induction and associativity. Details are left as an exercise. □

Definition 2.13. Let G be a group and $g \in G$ an element. The *order* of G is the smallest positive integer n such that $g^n = 1$, provided such a positive integer exists, and ∞ otherwise. We denote the order of g by $\mathrm{ord}(g)$.

We will also use the word "order" to describe the *size* of the underlying set of a group G. In other words, if G is a group, then the *order of* G is defined as the *size* $\#G$. Later on, we will be able to say something about the relationship between the order of an element $g \in G$, as defined above, and the order of the group G itself.

Example 2.14. An element g has order 1 if and only if $g = 1$. Every nonidentity element of $\mathbb{Z}$ has infinite order. The element $\exp(2 \cdot \pi \cdot i/n)$ has order n in $(\mathbb{C}^\times, \cdot)$, where $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$ denotes the group of nonzero complex numbers with respect to multiplication.

In the following subsections, we discuss a few important classes of examples which will appear throughout the course.

2.15 Permutation groups

Let A be any set. The collection

$$\mathrm{Per}(A) := \{f : A \to A \mid f \text{ is bijective}\}$$

is a group under function composition. Indeed, the composition of two bijections is a bijection to this operation is well-defined, any bijection has a (functional) inverse, and the identity function is a bijection. As is usual in group theory, we will use the notation $\sigma \cdot \tau$ as opposed to $\sigma \circ \tau$ for the composition of two elements of $\mathrm{Per}(A)$.

For a positive integer n, we write $S_n := \mathrm{Per}(\{1, \ldots, n\})$. As $A := \{1, \ldots, n\}$ is finite, a function $f : A \to A$ is bijective if and only if it's injective, and it's easy to see that there are $n!$ such functions. Thus $\#S_n = n!$.

Elements in S_n can be represented in several ways. For example, we can specify the behaviour of $\sigma \in S_n$ by describing it's action on the elements $1, 2, \ldots, n$, summarized in a table as follows:

1	2	$\cdots$	n
$\sigma(1)$	$\sigma(2)$	$\cdots$	$\sigma(n)$

For example, if $\sigma \in S_4$ is represented with the following table

1	2	3	4
2	3	1	4

and τ with the following:

1	2	3	4
3	2	4	1

Then $\sigma \cdot \tau$ has the following presentation

1	2	3	4
1	3	4	2

A more concise way to represent elements of S_n is in terms of a *cycle decomposition*. A *cycle* is a string of distinct integers $(a_1, \ldots, a_m)$ with $a_1, \ldots, a_m \in \{1, \ldots, n\}$ which represents the cyclic permutation sending a_1 to a_2, a_2 to a_3, etc. with a_m being sent to a_1, and all other elements of $\{1, \ldots, n\}$ being fixed. Explicitly $\sigma := (a_1, \ldots, a_m)$ is the permutation defined by

$$\sigma(t) = \begin{cases} a_{i+1} & t = a_i,\ 1 \leq i < m \\ a_1 & t = a_m \\ t & \text{otherwise.} \end{cases}$$

Note that a cycle of length 1 is the identity function.

Any permutation $\sigma \in S_n$ can be expressed in terms of a *cycle decomposition*. Here is an algorithm to compute this cycle decomposition:

1. To begin a new cycle, choose the smallest element a of $\{1, \ldots, n\}$ which has not yet appeared in a previous cycle. At the start of the algorithm, take $a = 1$. Start a new cycle as follows: "(a".

2. Determine $b := \sigma(a)$. If $b = a$, close the cycle with a parenthesis without writing b down, and return to step 1. If $b \neq a$, write b next to a in the cycle: "(a b".

3. Determine $c := \sigma(b)$. If $c = a$, close the cycle with a right parenthesis and return to step 1. If $c \neq a$, write c to the right of b and repear this step using c as the new value of b until the cycle closes.

The algorithm terminates when all of the numbers from $\{1, 2, \ldots, n\}$ have appearerd in some cycle. As a final step, remove all cycles of length 1 from the cycle decomposition of σ (as they are just the identity function).

This algorithm produces a decomposition of σ into a product of *disjoint* cycles (meaning that every integer $i \in \{1, \ldots, n\}$ appears in at most one cycle products by the algorithm). We will see later on that such a presentation is essentially unique (up to permutations of the cycles and cyclic permutations within the cycles).

Here are some properties about cycle decompositions:

1. If two cycles $\sigma := (a_1, \ldots, a_m)$ and $\tau := (b_1, \ldots, b_k)$ are disjoint, meaning that $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_k\}$ are disjoint sets, then one has $\sigma \cdot \tau = \tau \cdot \sigma$.

2. A *transposition* is a cycle of the form $\sigma := (i, j)$ with $i \neq j$. Any cycle can be expressed as a product of transpositions as follows:

$$(a_1, \ldots, a_m) = (a_1 a_m) \cdot (a_1 a_{m-1}) \cdots (a_1 a_3) \cdot (a_1 a_2).$$

Lemma 2.16. *The group S_n is abelian if and only if $n = 1$ or $n = 2$.*

Proof. Clearly S_1 and S_2 are abelian. Conversely, if $n \geq 3$, consider $(12), (13) \in S_n$ and compute

$$(12)(13) = (132)$$

while

$$(13)(12) = (123).$$

Since (132) and (123) act differently on 1, they are distinct, hence S_n is not abelian. □

2.17 Modular arithmetic

Throughout this subsection, n denotes a positive integer.

Theorem 2.18 (The division algorithm)**.** *Let a be any integer. Then there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that*

$$a = n \cdot q + r.$$

Proof. Let r be the minimum of the (nonempty) set

$$S := \{a - n \cdot k \mid k \in \mathbb{Z}\} \cap \mathbb{N}.$$

Then $r = a - n \cdot q$ for some $q \in \mathbb{Z}$ and $0 \leq r$ by definition. If $n \leq r$, then $r - b = a - n \cdot (q + 1)$ is also nonnegative, which would contradict the minimality of r, hence $r < n$.

As for uniqueness, suppose $n \cdot q + r = n \cdot q' + r'$, with $0 \leq r, r' < n$. Then n divised $r - r'$ since $r - r' = n \cdot (q - q')$, while

$$-n < r - r' < n.$$

The only integer satisfying these properties is 0, hence $r = r'$. Also, $q = q'$ since $n \cdot (q - q') = r - r' = 0$ and $0 < n$. □

Lemma 2.19. *Let a, b be two integers. The following are equivalent:*

1. *n divides $a - b$.*

2. *If* $a = n \cdot q + r$ *and* $b = n \cdot q' + r'$ *with* $0 \leq r, r' < n$, *then* $r = r'$.

Proof. The implication (2) $\Rightarrow$ (1) is trivial. Conversely, suppose n divides $a - b$ hence n divides $n \cdot (q - q') + (r - r')$. It follows that $r - r'$ is divisible by n as well, while

$$-n < r - r' < n.$$

As in the proof of Theorem 2.18, this implies $r = r'$. □

Definition 2.20. Given $a, b \in \mathbb{Z}$, we say that a *is congruent to* b *modulo* n provided that the equivalent conditions of Lemma 2.19 hold true. In this case, we shall write $a \equiv b\ (n)$ or $a \equiv b \bmod n$.

Exercise 2.21. The relation asserting that a is congruent to b modulo n is an equivalence relation.

Definition 2.22. We define $\mathbb{Z}/n$ to be the quotient of $\mathbb{Z}$ by the equivalence relation given by congruence modulo n. The element of $\mathbb{Z}/n$ represented by $a \in \mathbb{Z}$ will be denoted by $a \bmod n$.

Exercise 2.23. The map

$$\{0, 1, \ldots, n-1\} \to \mathbb{Z}/n$$

given by $r \mapsto r \bmod n$ is a *bijection.*

Theorem 2.24. *The rule* $(a \bmod n,\ b \bmod n) \mapsto (a + b) \bmod n$ *yields a well-defined binary operation*

$$\mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n$$

with respect to which $\mathbb{Z}/n$ *obtained an abelian group structure. With respect to this group structure the neutral element of* $\mathbb{Z}/n$ *is* $0 \bmod n$ *and the inverse of* $a \bmod n$ *is* $(-a) \bmod n$. *We denote the operation in* $\mathbb{Z}/n$ *additively.*

Proof. To see this operation is well-defined, we need to check that it does not depend on choice of representatives. Namely, suppose $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$. Then $n|(a - a')$ and $n|(b - b')$ hence $n|((a + b) - (a' + b'))$ so that indeed $(a + b) \equiv (a' + b') \bmod n$. The fact that this yields a group structure, and the other assertions of the theorem, are left as an exercise. In fact, we will see later on that this is a special case of a more general construction in group theory. □

2.25 Dihedral groups

Let n be an integer with $3 \leq n$, and consider the *regular n-gon* X. A *symmetry* of X is a rigid motion of X which is obtained by taking a copy of X, moving it around in space, and placing it back on the original X so that it covers X exactly. In more formal terms, label the vertices of X as $\{1, 2, \ldots, n\}$. A symmetry of X is then a permutation σ of $\{1, 2, \ldots, n\}$ preserving the adjacency of the vertices of X.

The collection of all symmetries of the regular n-gon is denoted by D_{2n}. This collection has $2n$ elements: n rotations and n reflections. The identity permutation is contained in D_{2n}, and, given any two $\sigma, \tau \in D_{2n}$, the composition $\sigma \circ \tau$ and σ^{-1} are both contained in D_{2n}. Thus D_{2n} is again a group.

Here is one way to represent the elements of D_{2n}. Let r denote the rotation of the regular n-gon by $360/n$ degrees, and let s denote a reflection about some axis defining a symmetry of the regular n-gon. Note that rs is again a reflection (about a different axis) hence $(rs)^2 = 1$ so that

$$rs = sr^{-1}.$$

The following elements are all distinct:

$$1, r, r^2, \ldots, r^{n-1}.$$

And, multiplying by s on the right, we see that the following are also distinct:

$$s, rs, r^2s, \ldots, r^{n-1}s,$$

which must therefore be the n distinct reflections. Thus, all together we have

$$D_{2n} = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\},$$

with the multiplication operations uniquely determined by the following rules:

$$r^n = 1, \quad rs = sr^{-1} = sr^{n-1}.$$

In formal terms, D_{2n} can be described using *generators and relations* (more on this later):

$$D_{2n} = \langle\ r, s \mid r^n = s^2 = (rs)^2 = 1\ \rangle.$$

Here are a couple of alternative presentations:

$$D_{2n} = \langle\ r, s \mid r^n = s^2 = 1,\ r \cdot s = s \cdot r^{n-1}\ \rangle.$$

$$D_{2n} = \langle\ r, s \mid r^n = s^2 = 1,\ s \cdot r = r^{n-1} \cdot s\ \rangle.$$

Exercise 2.26. Prove that the three above presentations are indeed presentations of D_{2n}.

2.27 The quaternion group

The quaternion group is the set

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

where the multiplication is determined by the following rules:

1. One has $(-1)^2 = 1$, $i^2 = j^2 = k^2 = -1$.
2. One has $(-1) \cdot i = -i$, $(-1) \cdot j = -j$, $(-1) \cdot k = -k$.
3. For all $a \in Q_8$, one has $(-1) \cdot a = a \cdot (-1)$.
4. One has $i \cdot j = k = -j \cdot i$.

This is a non-abelian group of order 8.

2.28 Products of groups

Suppose that G_i, $i \in I$ is a collection of groups. The cartesian product

$$\prod_i G_i = \{(g_i)_i \mid g_i \in G_i\}$$

can be endowed with the structure of a group where

$$(g_i)_i \cdot (h_i)_i = (g_i \cdot h_i)_i.$$

The identity is $(1_i)_i$, where $1_i \in G_i$ is the identity element of G_i, and the inverse of $(g_i)_i$ is simply $(g_i^{-1})_i$.

Exercise 2.29. Verify all unproven assertions in this subsection.

2.30 Matrix Groups

Linear algebra provides us with several families of groups. For example, the *general linear group* (over the reals) is the set

$$\mathrm{GL}_n(\mathbb{R})$$

of $n \times n$ real-valued invertible matrices. The identity matrix is invertible, the product of two invertible matrices is invertible, and the inverse of an invertible matrix provides the multiplicative inverse. Thus $\mathrm{GL}_n(\mathbb{R})$ is a group with respect to matrix multiplication. We define $\mathrm{GL}_n(\mathbb{C})$ similarly as the set of invertible $n \times n$ matrices with complex entries, which is again a group with respect to matrix multiplication.

Here are some examples of groups whose operation is given by matrix multiplication:

1. The set $\mathrm{SL}_n(k)$ of $n \times n$ matrices with entries in k whose determinant is 1, where $k = \mathbb{R}$ or $k = \mathbb{C}$ (or any commutative ring).

2. The set of upper triangular invertible matrices with entries in k where, again, $k = \mathbb{R}$ or $k = \mathbb{C}$ (or any commutative ring).

There are several otherr important examples in this context, some of which will be discussed later on in this course.

Exercise 2.31. Prove that the sets in items (1) and (2) above are indeed groups with respect to matrix multiplication.

2.32 Homomorphisms

Definition 2.33. Let G and H be groups. A *homomorphism* from G to H is a function $\varphi : G \to H$ such that for all $x, y \in G$, one has $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$. Note that the product appearing on the left hand side of the equation (before φ is applied) is the operation of G, while the one on the right-hand side (after φ is applied) is the one in H.

Lemma 2.34. *Let G, H and K be three groups, $\varphi : G \to H$ and $\psi : H \to K$ homomorphisms. Then $\psi \circ \varphi$ is a homomorphism as well.*

Proof. Exercise. □

Lemma 2.35. *Let G, H be two groups and $\varphi : G \to H$ a homomorphism. Let $g \in G$ and $a \in \mathbb{Z}$ be given. Then $\varphi(g^a) = \varphi(g)^a$. In particular, $\varphi(1) = 1$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$.*

Proof. Exercise. □

Example 2.36. The identity function $\mathbf{1}_G : G \to G$ is a homomorphism.

Example 2.37. Let $g \in G$ be an element of a group. If g has finite order n, then the map

$$\varphi : \mathbb{Z}/n \to G$$

defined by $\varphi(a \bmod n) = g^a$ is a well-defined *injective* homomorphism. If g has infinite order, then the map

$$\varphi : \mathbb{Z} \to G$$

defined by $\varphi(a) = g^a$ is an injective homomorphism.

2.38 Automorphisms

Definition 2.39. Let G and H be two groups. An *isomorphism* is a homomorphism $\varphi : G \to H$ such that there exists a homomorphism $\psi : H \to G$ satisfying $\varphi \circ \psi = \mathbf{1}_H$ and $\psi \circ \varphi = \mathbf{1}_G$. An *automorphism* of G is an isomorphism from G to itself.

Lemma 2.40. *A homomorphism $\varphi : G \to H$ is an isomorphism if and only if it is a bijection.*

Proof. Exercise. □

2.41 Group actions

Definition 2.42. An *action* of a group G on a set X is a function

$$G \times X \to X,$$

denoed $(g, x) \mapsto g \cdot x$, satisfying:

1. One has $1 \cdot x = x$ for all $x \in X$.
2. One has $(g \cdot h) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$.

Note that the left-most dot in the last equation is multiplication in G, the next left-most is the action of an element on X, while the two dots on the right hand side of the equation are the notation for the action of elements of G on elements of X.

Example 2.43. The symmetric group S_n acts on $\{1, 2, \ldots, n\}$ in the obvious way: $\sigma \cdot i = \sigma(i)$ for $i \in \{1, \ldots, n\}$ and $\sigma \in S_n$. Similarly, D_{2n} acts on $\{1, 2, \ldots, n\}$ by identifying $\{1, 2, \ldots, n\}$ with the set of vertices of the regular n-gon.

Lemma 2.44. *Suppose that G acts on X. Then the map*

$$\rho : G \to \mathrm{Per}(X)$$

given by $\rho(g)(x) = g \cdot x$ is a group homomorphism. Conversely, if

$$\rho : G \to \mathrm{Per}(X)$$

is a group homomorphism, then G acts on X via $g \cdot x = \rho(g)(x)$.

Proof. Exercise. □

3 Subgroups

We have introduced group homomorphisms as a way to relate different groups. Naturally, one can ask about homomorphisms that satisfy additional conditions. For example, we have already seen that a bijective homomorphism is an *isomorphism*, which can be considered as merely a *relabelling* of the elements of the group in the sense that two isomorphic groups behave identically from the perspective of group theory. But what about injective homomorphisms and surjective homomorphisms? In this section, we introduce and study the notion of a *subgroup*, which will essentially give us a concrete way to describe *injective* homomorphisms.

3.1 The definition and some examples

Definition 3.2. Let G be a group. A *subgroup* of G is a subset H of G satisfying:

1. One has $1 \in H$.
2. For all $g, h \in H$, the product $g \cdot h \in G$ is an element of H.
3. For all $g \in H$, the inverse $g^{-1} \in G$ is an element of H.

We use the notation $H \leq G$ to say that H is a subgroup of G.

Lemma 3.3. *Let H be a subgroup of a group G, and consider the binary operation*

$$(g, h) \mapsto g \cdot h$$

on H where $g \cdot h$ is the product of g, h when considered as elements of G. With this operation, H is itself a group.

Proof. Exercise. □

Example 3.4. Here are a few examples of subgroups.

1. One has $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, all groups with respect to addition.
2. If G is any group, then $\{1\} \leq G$ and $G \leq G$.
3. $\{1, r, \ldots, r^n\} \leq D_{2n}$ and $\{1, s\} \leq D_{2n}$.
4. $D_{2n} \leq S_n$ if we identify elements of D_{2n} with the associated permutation of the vertices of the regular n-gon.

5. If $H \leq G$ and $G \leq K$ then $H \leq K$.

Example 3.5. Some non-examples:

1. $\mathbb{Q}^\times = \{\alpha \in \mathbb{Q} \mid \alpha \neq 0\}$ is a multiplicative group and $\mathbb{Q}$ is an additive group. We have $\mathbb{Q}^\times \subset \mathbb{Q}$ but $\mathbb{Q}^\times$ is not a subgroup of $\mathbb{Q}$.

2. $\mathbb{N} \subset \mathbb{Z}$ is not a subgroup.

3. $\mathbb{Z} \smallsetminus \{0\} \subset \mathbb{Z}$ is not a subgroup.

4. $\{1, r\} \subset D_{2n}$ is not a subgroup for $n \geq 3$.

Lemma 3.6. *A subset H of G is a subgroup if and only if the following hold:*

1. *The set H is nonempty.*

2. *For all $x, y \in H$, one has $x \cdot y^{-1} \in H$.*

Proof. If H is a subgroup then the conditions hold as $1 \in H$ and H is closed under multiplication and inversion. Conversely, assume the two conditions. As H is nonempty, there is some element $h \in H$. Thus by 2 we have $h \cdot h^{-1} = 1 \in H$. If $g \in H$ then as $1 \in H$ one has $1 \cdot g^{-1} = g^{=1} \in H$ again by 2. If $g, h \in H$ then $h^{-1} \in H$ hence $g \cdot h = g \cdot (h^{-1})^{-1} \in H$ again by 2. □

Lemma 3.7. *A* finite *subset H of a group G is a subgroup if and only if it is nonempty and closed under multiplication.*

Proof. If H is a subgroup then $1 \in H$ and H is clsoed under multiplication. Conversely, let $h \in H$ be any element. Then the set $\{h^n \mid n \in \mathbb{Z},\ n \geq 1\}$ is finite, hence there exist some positive integers $a < b$ with $h^a = h^b$. Put $n := b - a$ hence $x^n = 1$, so $1 \in H$, and it follows that every element of H has finite order. Also, $h^{-1} = h^{n-1} \in H$ so that H is closed under inverses. This shows that H is indeed a subgroup. □

Lemma 3.8. *Let H_i, $i \in I$ be any collection of subgroups of G. The intersection $\bigcap_i H_i$ is again a subgroup of G.*

Proof. Exercise. □

3.9 Images and Kernels

Definition 3.10. Let $\varphi : G \to H$ be a homomorphism of groups. Define

1. $\mathrm{im}(\varphi) = \{h \in H \mid \exists g \in G,\ \varphi(g) = h\}$.
2. $\ker(\varphi) = \{g \in G \mid \varphi(g) = 1\}$.

Lemma 3.11. *In the above context,* $\mathrm{im}(\varphi)$ *is a subgroup of* H *and* $\ker(\varphi)$ *is a subgroup of* G*.*

Proof. For the image, note that $\varphi(1) = 1$ hence $1 \in \mathrm{im}(\varphi)$. Also, $\varphi(g^{-1}) = \varphi(g)^{-1}$ and $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ hence $\mathrm{im}(\varphi)$ is closed under multiplication and inversion. For the kernel, the fact that $\varphi(1) = 1$ shows that $1 \in \ker(\varphi)$. If $\varphi(g) = 1$ then $\varphi(g^{-1}) = \varphi(g)^{-1} = 1^{-1} = 1$ hence $g \in \ker(\varphi)$. If $\varphi(g) = \varphi(h) = 1$ then $\varphi(g \cdot h) = \varphi(g) \cdot \varphi(h) = 1 \cdot 1 = 1$ hence $g \cdot h \in \ker(\varphi)$ as well. This shows that $\ker(\varphi)$ is a subgroup. □

Lemma 3.12. *Let* $\varphi : G \to H$ *be a homomorphism of groups. Then* φ *is surjective if and only if* $\mathrm{im}(\varphi) = G$*.*

Proof. Clear. □

Lemma 3.13. *Let* $\varphi : G \to H$ *be a homomorphism of groups. Then* φ *is injective if and only if* $\ker(\varphi) = \{1\}$*.*

Proof. If φ is injective, then clearly $\ker(\varphi) = \{1\}$ as $\varphi(1) = 1$. Conversely, suppose $\ker(\varphi) = \{1\}$ and assume that $\varphi(a) = \varphi(b)$. Then $\varphi(a \cdot b^{-1}) = 1$ hence $a \cdot b^{-1} \in \ker(\varphi) = \{1\}$. Thus $a \cdot b^{-1} = 1$, hence $a = b$. □

3.14 Centralizers, Normalizers, Stabilizers

In this section we introduce some additional important families of subgroups. Throughout this subsection, G denotes a group and A a *subset* of G.

Definition 3.15. The *centralizer* of A in G is defined as

$$C_G(A) := \{g \in G \mid \forall a \in A,\ g \cdot a \cdot g^{-1} = a\}.$$

If $A = \{a\}$ is a singleton, we write $C_G(a)$ instead of $C_G(\{a\})$.

Lemma 3.16. $C_G(A)$ *is a subgroup of* G*.*

Proof. Since $1 \cdot a \cdot 1^{-1} = a$ for all a, we have $1 \in C_G(A)$. If $g \in C_G(A)$ and $a \in A$ then $g \cdot a \cdot g^{-a} = a$. Multiply on the left by g^{-1} and on thhe right by g to deduce that $a = g^{-1} \cdot a \cdot g = g^{-1} \cdot a \cdot (g^{-1})^{-1}$. As a was arbitrary, $g^{-1} \in C_G(A)$. If $g, h \in C_G(A)$, and $a \in A$ is given then

$$(gh) \cdot a \cdot (gh)^{-1} = g \cdot (h \cdot a \cdot h^{-1}) \cdot g^{-1} = g \cdot a \cdot g^{-1} = a.$$

Thus $g \cdot h \in C_G(A)$. □

Definition 3.17. The *center* of a group G is defined as

$$Z(G) := C_G(G).$$

In other words, $Z(G) = \{g \in G \mid \forall a \in G,\ g \cdot a = a \cdot g\}$. The lemma above shows that $Z(G)$ is a subgroup of G.

Definition 3.18. The *normalizer* of A is defined as

$$N_G(A) := \{g \in G \mid g \cdot A \cdot g^{-1} = A\}.$$

Here $g \cdot A \cdot g^{-1} := \{g \cdot a \cdot g^{-1} \mid a \in A\}$.

Lemma 3.19. *$N_G(A)$ is a subgroup of G and $C_G(A) \leq N_G(A)$.*

Suppose now that G acts on a set X.

Definition 3.20. Let $x \in X$ be given. The *stabilizer* of x in G is the set

$$G_x := \{g \in G \mid g \cdot x = x\}.$$

Lemma 3.21. *In the above context, G_x is a subgroup of G.*

Proof. Clearly $1 \in G_x$ and G_x is closed under multiplication. If $g \in G_x$ then

$$x = (g^{-1} \cdot g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x,$$

hence $g^{-1} \in G_x$ as well. □

Definition 3.22. The *kernel* of the action of G on X is the set

$$G_X := \{g \in G \mid \forall x \in X,\ g \cdot x = x\}.$$

Lemma 3.23. *G_X is a subgroup of G.*

Proof. G_X is the intersection $\bigcap_{x \in x} G_x$, and the intersection of an arbitrary family of subgroups is a subgroup. □

Exercise 3.24. G_X is the kernel of the permutation representation

$$\rho : G \to \mathrm{Per}(X)$$

associated to the G-action on X.

3.25 Cyclic groups and subgroups

Definition 3.26. A group H is called *cyclic* if it can be generated by a single element, i.e. if there exists some element $g \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$.

We shall write $H = \langle x \rangle$ to denote the fact that H is generated by $x \in H$, which means that $H = \{x^n \mid n \in \mathbb{Z}\}$. A cyclic group can have more than one generator. For example, if $H = \langle x \rangle$ then $H = \langle x^{-1} \rangle$ as well. We will soon classify all generators of a cyclic group.

Example 3.27.
1. The subgroup $\{1, r, \ldots, r^{n-1}\}$ of D_{2n} is cyclic and generated by r. This is the subgroup of rotations in D_{2n}.
2. The additive group $\mathbb{Z}$ is cyclic, generated by 1.
3. If H is cyclic and $\varphi : H \to G$ is a homomorphism, then the image of φ is a cyclic subgroup of G.

Lemma 3.28. *Let $H = \langle x \rangle$ be cyclic. If x has finite order n, then the map*

$$\varphi : \mathbb{Z}/n \to H, \quad a \bmod n \mapsto g^a$$

is an isomorphism. If x has infinite order, then the map

$$\varphi : \mathbb{Z} \to H, \quad a \mapsto g^a$$

is an isomorphism. In particular, $\#H = \operatorname{ord}(x)$.

Proof. It was shown on homework 1 that these maps are well-defined and injective, while it is easy to see that they are homomorphisms. They are also surjective as H is cyclic, hence they are isomorphisms. □

Lemma 3.29. *Let G be any group and $g \in G$ an element. Let $m, n \in \mathbb{Z}$ be such that $g^m = g^n = 1$. Then $g^{\gcd(m,n)} = 1$.*

Proof. By the Euclidean algorithm, it follows that there exist $a, b \in \mathbb{Z}$ such that $d := \gcd(m, n) = a \cdot m + n \cdot b$. Thus $g^d = (g^m)^a \cdot (g^n)^b = 1$. □

Lemma 3.30. *Suppose $g \in G$ is an element of finite order and that m is an integer. Then $\operatorname{ord}(g)$ divides m if and only if $g^m = 1$.*

Proof. If $\operatorname{ord}(g) | m$ then clearly $g^m = 1$ since $m = k \cdot \operatorname{ord}(g)$ for some k hence $g^m = (g^{\operatorname{ord}(g)})^k = 1$. Conversely, suppose that $g^m = 1$ hence, setting $d := \gcd(m, \operatorname{ord}(g))$, we have $g^d = 1$. But since $0 < d \leq \operatorname{ord}(g)$, it follows from the definition of ord that $d = \operatorname{ord}(g)$. Thus $\operatorname{ord}(g) | m$. □

Theorem 3.31. *Let G_1 and G_2 be two cyclic groups. Then $G_1 \cong G_2$ if and only if G_1 and G_2 have the same order. In fact, if g_i is a generater of the cyclic group G_i and $\#G_1 = \#G_2$, then the map defined by*

$$g_1^k \mapsto g_2^k, \quad k \in \mathbb{Z}$$

is an isomorphism $G_1 \cong G_2$.

Proof. Two isomorphic groups always have the same order, so we focus on the converse. The order g_i agrees with the order of G_i by the lemma above so g_1 and g_2 have the same order. If this order is infinite, then the map described above is the composition of two isomorphisms:

$$G_1 \xrightarrow{g_1^k \mapsto k} \mathbb{Z} \xrightarrow{k \mapsto g_2^k} G_2.$$

If the order is finite, say n, then the map above is the composition of the isomorphisms:

$$G_1 \xrightarrow{g_1^k \mapsto k \bmod n} \mathbb{Z}/n \xrightarrow{k \bmod n \mapsto g_2^k} G_2.$$

This completes the proof. □

Let us now discuss the orders of elements in a cyclic group.

Lemma 3.32. *Let G be a group, and $g \in G$ any element. Let a be a nonzero integer.*

1. *If g has infinite order, then so does g^a.*
2. *If g has finite order n, then g^a has order $n/\gcd(a, n)$.*

Proof. Suppose g has infinite order. If a is positive, then $(g^a)^k = g^{ak} \neq 1$ for any positive k (why?), hence g^a has infinite order as well. If a is negative, simply replace g by g^{-1} and recall that g^{-1} has infinite order as well (details left as an exercise).

If g has finite order n, put $d := \gcd(a, n)$. This is a positive integer, and we can write $a = r \cdot d$ and $n = s \cdot d$ for some $r, s \in \mathbb{Z}$. Recall that r and s are *coprime*. Put $h := g^a$. Note that $h^s = g^{a \cdot s} = g^{r \cdot d \cdot s} = (g^n)^r = 1^r = 1$. It follows that the order of h divides s. On the other hand, if $e := \mathrm{ord}(h)$ then

$$1 = h^e = g^{a \cdot e}$$

so that $n = s \cdot d$ divides $a \cdot e = r \cdot d \cdot e$. It follows that s divides $r \cdot e$, but since r and s are coprime, we deduce s divides e. In other words, s and e are positive integers which divide eachother, and they must therefore be the same. □

Theorem 3.33. *Suppose that G is a cyclic group with generator g, and let $a \in \mathbb{Z}$ be given.*

1. *Suppose G has infinite order. Then $G = \langle g^a \rangle$ if and only if $a = \pm 1$.*
2. *Suppose G has finite order n. Then $G = \langle g^a \rangle$ if and only if one has $\gcd(a, n) = 1$.*

Proof. In case (1), if $a = \pm 1$ then clearly $G = \langle g^a \rangle$ (why?). Conversely, if $G = \langle g^a \rangle$ then $g = g^{a \cdot k}$ for some $k \in \mathbb{Z}$, and since g has infinite order it follows that $1 = a \cdot k$ (why) hence a must divide 1, so that $a = \pm 1$.

In case (2), we see that g^a generates a subgroup of order $n/\gcd(a, n)$ by the previous lemma, and this is the whole group G (which has order n) if and only if $n = n/\gcd(a, n)$ or equivalently $\gcd(a, n) = 1$. □

Definition 3.34. Let n be a positive integer. The integer $\varphi(n)$ is the number of integers $a \in \{0, 1, \ldots, n-1\}$ satisfying $\gcd(a, n) = 1$.

Corollary 3.35. *If G is a cyclic group of finite order n and g is a generator of G, then G has $\varphi(n)$ generators given by g^a for $a \in \{0, 1, \ldots, n-1\}$ satisfying* $\gcd(a, n) = 1$.

Finally, let us determine all subgroups of a cyclic group.

Theorem 3.36. *Let G be a cyclic group with generator g.*

1. *Every subgroup of G is cyclic. In fact, if $H \leq G$, then either $H = \langle 1 \rangle = \{1\}$ or $H = \langle g^k \rangle$ where k is the smallest positive integer such that $g^k \in H$.*
2. *If G has infinite order, then for any disctinct nonnegative integerrs a and b, one has $\langle g^a \rangle \neq \langle g^b \rangle$, and for any integer k, one has $\langle g^k \rangle = \langle g^{|k|} \rangle$. In particular, the subgroups of G are in bijection with natural numbers.*
3. *If G has finite order n, then for each positive integer a dividing n, there is a unique subgroup $H \leq G$ of order a, and $H = \langle g^d \rangle$ where $d = n/a$. Furthermore, for every integer k, one has $\langle g^k \rangle = \langle g^{\gcd(k,n)} \rangle$. In particular, the subgroups of G are in bijection with the positive divisors of n.*

Proof. Assertion (1): We may as well assume that H is nontrivial (as the trivial subgroup is always cyclic). If H is nontrivial, then there exists some

integer $a \neq 0$ such that $g^a \in H$. We may assume without loss of generality that a is positive (replace g by its inverse otherwise). Let

$$S = \{b \in \mathbb{N} \mid b \neq 0,\ g^b \in H\}.$$

This is a subset of the natural numbers which is nonempty by the above, hence has a minimal element d. Note that $\langle g^d \rangle \subset H$ since H is a subgroup.

Now suppose that $h \in H$ is any element, and note that $h = g^a$ for some integer a. Consider $a = q \cdot d + r$ for some $0 \leq e < d$. Then

$$g^r = g^{a - q \cdot d} = g^a \cdot (g^a)^{-q} \in H.$$

As d is minimal, it follows that $r = 0$, hence $a = q \cdot d$. Thus $g^a = (g^d)^q \in \langle g^d \rangle$. It follows that $H = \langle g^d \rangle$.

Assertion (3): If $a|n$ and $d = n/a$ then $\langle g^d \rangle$ has order a by a previous lemma. Let us show that this is the unique subgroup of G of order a. Suppose that H is any subgroup of order a. By part (1), we have $H = \langle g^b \rangle$ where b is the smallest positive integer such that $g^b \in H$. But

$$a = n/d = \#H = \mathrm{ord}(g^b) = n/\gcd(b, n)$$

hence $d = \gcd(b, n)$. In particular, $d|b$, so thaht $g^b \in \langle g^d \rangle$. But then

$$H = \langle g^b \rangle \subset \langle g^d \rangle$$

while both subgroups have the same size inside G, which is finite. It follows that $H = \langle g^d \rangle$. A similar argument shows that $\langle g^k \rangle = \langle g^{\gcd(k,n)} \rangle$ as $g^k \in \langle g^{\gcd(k,n)} \rangle$, while both subgroups have the same size.

Assertion (2) is left as an exercise. □

3.37 The Lattice of Subgroups

Let G be a group. We can visualize the collection of all subgroups of G using a diagram, called *the lattice of subgroups of* G. In precise terms, this diagram is a directed graph whose vertices correspond to the subgroups of G and where, given two subgroups $H_1, H_2 \leq G$, there is an edge $H_1 \to H_2$ if and only if $H_1 \subset H_2$ (equivalently $H_1 \leq H_2$) and there is no other subgroup between H_1 and H_2 except H_1 and H_2. We often arrange this diagram so that the trivial subgroup, $\{1\}$ is places at the bottom, and the whole group G, is placed at the top.

Remark 3.38. If one considers the collection of all subgroups of G as a partially ordered set, with respect to inclusion, it is indeed a *lattice*, which has a precise mathematical meaning: Every pair of elements has a greatest lower bound and least upper bound. The greatest lower bound of H_1 and H_2 is the intersection $H_1 \cap H_2$, and the least upper bound is the *join*, $\langle H_1, H_2 \rangle$, i.e. the subgroup generated by the union of H_1 and H_2. This lattice has a unique minimal element $\{1\}$ and a unique maximal element G.

Much more can be said about this lattice. For example, there is a so-called *Galois insertion* between the lattice of subgroups and the lattice of all subsets of G, given by sending a subgroup H to the underlying subset of H, and sending a set S to $\langle S \rangle$. Galois connections and insertions will not be covered in this course.

Let us discuss a few examples of lattices of subgroups. In the examples below, we use the following fact.

Lemma 3.39. *Let $G = \langle g \rangle$ be cyclic of finite order n with generator g. Let H_1 and H_2 be subgroups of G. Then $H_1 \leq H_2$ if and only if $\#H_1 | \#H_2$.*

Proof. Exercise. *Hint:* Use the uniquness properties of subgroups of a cyclic group. □

Example 3.40. The group $\mathbb{Z}/2$ has precisely two subgroups, $\{0\}$ and $\mathbb{Z}/2$. The lattice of subgroups can be visualized as

$$\begin{array}{c} \mathbb{Z}/2 \\ \uparrow \\ \{0\} \end{array}$$

Example 3.41. The lattice of subgroups of $\mathbb{Z}/4$ is given by

$$\begin{array}{c} \mathbb{Z}/4 \\ \uparrow \\ \langle 2 \rangle \\ \uparrow \\ \langle 0 \rangle \end{array}$$

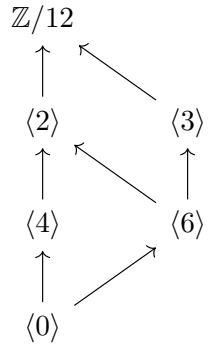
The lattice of subgroups of $\mathbb{Z}/8$ is given by

$$\begin{array}{c} \mathbb{Z}/8 \\ \uparrow \\ \langle 2 \rangle \\ \uparrow \\ \langle 4 \rangle \\ \uparrow \\ \langle 0 \rangle \end{array}$$

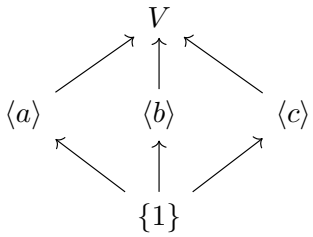
Example 3.42. Let p be a prime number and k a positive integer. The lattice of subgroups of $\mathbb{Z}/p^k$ has the following form:

$$\begin{array}{c} \langle p^0 \rangle = \mathbb{Z}/p^k \\ \uparrow \\ \langle p^1 \rangle \\ \uparrow \\ \langle p^2 \rangle \\ \uparrow \\ \vdots \\ \uparrow \\ \langle p^{k-1} \rangle \\ \uparrow \\ \langle p^k \rangle = \langle 0 \rangle \end{array}$$

Example 3.43. The lattice of subgroups of $\mathbb{Z}/12$ has the following form:



Example 3.44. The *Klein Four Group*, denoted by V here, is the unique group with four elements such that every element has order dividing 2. It is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ (verify these assertions!). Letting $\{1, a, b, c\}$ denote its four elements, its lattice of subgroups is



Example 3.45. The lattice of subgroups of S_3, D_8 and of Q_8 were discussed during lecture. See the handwritten notes for details.

3.46 Injective homomorphisms

We conclude this section about subgroups by describing their relationship with injective homomorphisms.

Theorem 3.47. *Let G be a group.*

1. *Suppose that H is a subgroup of G. Then the inclusion map $\iota : H \to G$ is an injective homomorphism of groups.*

2. *Suppose that $\iota : H \to G$ is an injective homomorphism of groups. Then ι induces an isomorphism $H \cong \mathrm{im}(\varphi)$, given by $h \mapsto \varphi(h)$.*

Proof. Assertion (1) is clear, since $\iota(g \cdot h) = \iota(g) \cdot \iota(h)$ by definition, and ι is injective (this is a tautology!). As for assertion (2), simply note that since $\iota : H \to G$ has image $\operatorname{im} \varphi$, and so canonically induces a map $H \to \operatorname{im} \varphi$ which is bijective since ι is injective. This map is a homomorphism since ι was, and therefore $H \cong \operatorname{im} \varphi$. □

In conclusion, any subgroup $H \leq G$ gives rise to an injective homomorphism $\iota : H \to G$ given by the canonical inclusion map, and, conversely, if $\iota : H \to G$ is an injective homomorphism, then H is isomorphic to the image of φ, which is a subgroup of G.

In the following section, we will give an analogous description of *surjective* homomorphisms in terms of *quotients* of groups.

4 Quotients

We will take a somewhat unorthodox path toward describing quotients of groups, starting with a homomorphism $f : G \to H$ of groups. First, by replacing $f : G \to H$ with the associated homomorphism $f : G \to \operatorname{im} H$, we may as well assume that $f : G \to H$ is surjective.

What we would like to do is to use H to define a group structure on the collection of *fibers* of f. Recall that, given a function $g : A \to B$ of sets and $b \in B$, the *fiber* of g over b is the preimage

$$g^{-1}(b) := \{a \in A \mid g(a) = b\}.$$

In our case of a surjective homomorphism $f : G \to H$, we consider the set

$$\{f^{-1}(h) \mid h \in H\}.$$

Some comments are in order:

1. Since f is surjective, $f^{-1}(h)$ is nonempty for every $h \in H$.
2. The sets $f^{-1}(h)$ are pairwise disjoint: $f^{-1}(h_1) = f^{-1}(h_2)$ if and only if $h_1 = h_2$.
3. The sets $f^{-1}(h)$ cover all of G, i.e. $G = \bigcup_{h \in H} f^{-1}(h)$.

To ease the notation, we write $F_h := f^{-1}(h)$. We therefore see that the map $H \to \{F_h \mid h \in H\}$ given by $h \mapsto F_h$ is a *bijection*. This allows us to use the group structure of H to define a group structure on $\{F_h | h \in H\}$ by defining

$$F_{h_1} \cdot F_{h_2} := F_{h_1 \cdot h_2}.$$

The identity is thus F_1 and $F_h^{-1} = F_{h^{-1}}$. In fact, the map $h \mapsto F_h$ provides an *isomorphism* $H \cong \{F_h \mid h \in H\}$. This begs the following question: What information is needed to describe the sets F_h, $h \in H$?

It will be worthwhile to think about the following example. Consider the surjective homomorphism

$$p : \mathbb{Z} \to \mathbb{Z}/n$$

given by $p(a) = a \bmod n$. The fiber over $a \bmod n$ is the set of integers a' such that $a' \bmod n = a \bmod n$, which is precisely th set $a \bmod n$ itself! In other words, the fiber over $a \bmod n$ is the set $\{a + k \cdot n \mid k \in \mathbb{Z}\}$. The kernel of this map is $n \cdot \mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$, so the fiber over $p(a)$ is precisely $\{a + b \mid b \in \ker(p)\}$. This generalizes.

Definition 4.1. Let N be a subgroup of G and let $g \in G$ be given. We define

$$g \cdot N := \{g \cdot n \mid n \in N\},\ N \cdot g := \{n \cdot g \mid n \in N\}.$$

The set $g \cdot N$ (resp. $N \cdot g$) is called the *left* (resp. *right*) *coset* of N associated to $g \in G$, An element of $g \cdot N$ (resp. $N \cdot g$) is called a *representative* of the coset.

Lemma 4.2. *In the context above, put $K := \ker(f)$, and let $g \in G$ be given. Then $F_{f(g)} = g \cdot K = K \cdot g$. In particular, if $g \in F_h$ is any element, then $F_h = g \cdot K = K \cdot g$.*

Proof. Exercise. □

Lemma 4.3. *In the above context, suppose that $h_i \in H$, $i = 1, 2$ are given, and that $g_1, g_2 \in G$ satisfy $g_i \in F_{h_i}$. Then*

$$F_{h_1 \cdot h_2} = (g_1 \cdot g_2) \cdot K = K \cdot (g_1 \cdot g_2).$$

Proof. By the previous lemma, it suffices to observe that $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2) = h_1 \cdot h_2$. □

Here is a summary of the discussion above. We started with a surjective homomorphism $f : G \to H$ of groups, and, for $h \in H$, we denoted $F_h := f^{-1}(h)$. We considered the set of fibers

$$\mathcal{F} := \{F_h \mid h \in H\}$$

and saw that the map

$$\delta : H \to \mathcal{F},\quad \delta(h) = F_h$$

is a bijection. This allowed us to define a group structure on $\mathcal{F}$ where the operation is given by $F_h \cdot F_{h'} = F_{h \cdot h'}$. With this group structure, δ becomes an isomorphism of groups.

Next, we say that for $g \in F_h$, one has $F_h = g \cdot K = K \cdot g$, where $K := \ker(f)$. In particular,

$$\mathcal{F} = \{g \cdot K \mid g \in G\}.$$

With this description, we saw that the group structure on $\mathcal{F}$ can be described as

$$(g \cdot K) \cdot (g' \cdot K) = (g \cdot g') \cdot K.$$

In other words, the group $\mathcal{F}$ is detemined completely by the following data:

1. The subgroup K, which is the kernel of f.
2. The group structure on G.

Finally, note that if $f : G \to H$ is an *atribtrary* homomorphism, then f induces a surjective homomorphism

$$f' : G \to \mathrm{im}(f),$$

and that $\ker(f) = \ker(f')$. This suggests that our next task is to classify which subgroups of G are kernels of some homomorphisms (as any kernel is a kernel of some surjective homomorphism). The discussion above then shows that when K is the kernel of a surjective homomorprhism $f : G \to H$, then the group H is *isomorphic* to the group

$$\{g \cdot K \mid g \in K\},$$

with the group structure given by $(g \cdot K) \cdot (g' \cdot K) = (g \cdot g') \cdot K$.

4.4 More on cosets

Lemma 4.5. *Let G be a group and N a subgroup of G.*

1. *The collection of left-cosets of N, $\{g \cdot N \mid g \in G\}$, is a partition of the set G.*
2. *The collection of right-cosets of N, $\{N \cdot g \mid g \in G\}$, is a partition of the set G.*
3. *For $g, h \in G$, one has $g \cdot N = h \cdot N$ if and only if $h^{-1} \cdot g \in N$.*

4. *For $g, h \in G$, one has $N \cdot g = N \cdot h$ if and only if $g \cdot h^{-1} \in N$.*

Proof. We prove (1) and (3), leaving the (analogous) assertions (2) and (4) to the reader. First of all, note that $g \in g \cdot N$ hence any element of G is contained in some left coset of N. Second, if $g \cdot N \cap h \cdot N \neq \varnothing$, and $x \in g \cdot N \cap h \cdot N$ then $x = g \cdot n = h \cdot m$ for some $m, n \in N$. Thus $g = h \cdot w$, with $w := m \cdot n^{-1} \in N$ (as N is a subgroup). It is easy to see then that $g \cdot N = (h \cdot w) \cdot N \subset h \cdot N$, since N is closed under multiplication. conversely, any element of the form $h \cdot n$ with $n \in N$ can be written as

$$h \cdot n = h \cdot w \cdot w^{-1} \cdot n = g \cdot (w^{-1} \cdot n) \in g \cdot N.$$

Thus $g \cdot N = h \cdot N$. This proves (1).

As for (3), suppose that $h^{-1} \cdot g \in N$ and $g \cdot n \in g \cdot N$ is given. Then

$$g \cdot n = h \cdot h^{-1} \cdot g \cdot n = h \cdot (h^{-1} \cdot g \cdot n) \in h \cdot N,$$

hence $g \cdot N \subset h \cdot N$. Since N is a subgroup, $(h^{-1} \cdot g)^{-1} = g^{-1} \cdot h \in N$, so by symmetry we also deduce that $h \cdot N \subset g \cdot N$, hence $g \cdot N = h \cdot N$. Conversely, if $g \cdot N = h \cdot N$ then $g = g \cdot 1 = h \cdot n$ for some $n \in N$ so that $h^{-1} \cdot h = n \in N$, as required. □

Corollary 4.6. *Let N be a subgroup of G.*

1. *The rule $g \sim h$ if and only if $h^{-1} \cdot g \in N$ is an equivalence relation on G. If $g \in G$ then the equivalence class represented by g with respect to this relation is precisely $g \cdot N$.*

2. *The rule $g \sim h$ if and only if $g \cdot h^{-1} \in N$ is an equivalence relation on G. If $g \in G$ then the equivalence class represented by g with respect to this relation is precisely $N \cdot g$.*

Theorem 4.7. *Let N be a subgroup of G, and let $\mathcal{L} := \{g \cdot N \mid g \in G\}$ denote the set of left cosets of N. The following are equivalent:*

1. *The operation $\mathcal{L} \times \mathcal{L} \to \mathcal{L}$ defined by*

$$(g \cdot N, g' \cdot N) \mapsto (g \cdot g') \cdot N$$

   is well-defined.

2. *For all $g \in G$ and $n \in N$, one has $g \cdot n \cdot g^{-1} \in N$.*

3. *For all $g \in G$, one has $g \cdot N = N \cdot g$.*

4. *For all $g \in G$, one has $g \cdot N \cdot g^{-1} = N$.*

5. *One has $N_G(N) = G$.*

Proof. The equivalence of 3, 4 and 5 are elementary and left as an exercise. Clearly 4 implies 2. Condition 2 obviously implies $g \cdot N \cdot g^{-1} \subset N$, while for $n \in N$, condition 2 implies that $g^{-1} \cdot n \cdot g = m$ for some $m \in N$, so that $n = g \cdot m \cdot g^{-1} \in g \cdot N \cdot g^{-1}$. Thus 2 is equivalent to 4.

We conclude by showing that 1 and 2 are equivalent. Assume 1. Let $g \in G$ and $n \in N$ be given. By condition 1, we know that

$$(g^{-1} \cdot N) = (n \cdot g^{-1}) \cdot N,$$

since $n \cdot N = 1 \cdot N$. Thus $n \cdot g^{-1} = g^{-1} \cdot m$ for some $m \in N$ hence $g \cdot n \cdot g^{-1} = m \in N$.

Conversely, suppose 2 holds true. Suppose that $g \cdot N = g' \cdot N$ and $h \cdot N = h' \cdot N$. Thus $g' = g \cdot m$ and $h' = h \cdot n$ for some $m, n \in N$. We must show that $g' \cdot h' \in (g \cdot h) \cdot N$. We calculate:

$$g' \cdot h' = (g \cdot m) \cdot (h \cdot n) = g \cdot h \cdot ((h^{-1} \cdot m \cdot h) \cdot n).$$

By condition 2, we find that $h^{-1} \cdot m \cdot h \in N$ and since $n \in N$ as well, it follows that $(h^{-1} \cdot m \cdot h) \cdot n \in N$ so that indeed $g' \cdot h' \in (g \cdot h) \cdot N$. This concludes the proof of the theorem. □

Definition 4.8. A subgroup N of a group G is called *normal* provided that the equivalent conditions of Theorem 4.7 hold true for N. We write $N \trianglelefteq G$ (or $N \triangleleft G$) to denote the fact that N is a normal subgroup of G. In this case, G/N is a group with respect to the operation $(g \cdot N) \cdot (g' \cdot N) = (g \cdot g')N$, and the canonical map

$$\pi_N : G \to G/N$$

defined by $g \mapsto g \cdot N$ is a surjective homomorphism which will be called the *canonical projection assocaited to N*. The group G/N will be called the *quotient of G by N*.

Theorem 4.9. *Let G be a group. A subgroup N of G is normal if and only if it is the kernel of some homomorphism $\varphi : G \to H$.*

Proof. Suppose that N is the kernel of φ. If $g \in G$ and $n \in N$ then $\varphi(g \cdot n \cdot g^{-1}) = \varphi(g) \cdot \varphi(n) \cdot \varphi(g)^{-1} = 1$, hence $g \cdot n \cdot g^{-1} \in N$ as well, so that N is normal. Conversely if N is normal then G/N is a group and

$$\pi : G \to G/N$$

is a surjective homomorphism whose kernel is N. □

Example 4.10. Let G be a group.

1. G and $\{1\}$ are both normal subgroups of G.
2. If G is abelian, then any subgroup of G is normal.
3. $\langle r \rangle$ is a normal subgroup of D_8, while $\langle s \rangle$ is not normal.

Example 4.11. Let G be a group. Define

$$\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$$

to be the image of the canonical map $\rho : G \to \mathrm{Aut}(G)$ given by $\rho(g)(h) = g \cdot h \cdot g^{-1}$. Then $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$. In fact, if $\sigma \in \mathrm{Aut}(G)$ then $\sigma \circ \rho(g) \circ \sigma^{-1} = \rho(\sigma(g))$. To see this, simply calculate:

$$\sigma(\rho(g)(\sigma^{-1}(h))) = \sigma(g \cdot \sigma^{-1} h \cdot g^{-1})$$

and note that this is precisely

$$\sigma(g) \cdot h \cdot \sigma(g)^{-1}$$

since $\sigma(\sigma^{-1}(h)) = h$ and σ is an automorphism. The elements of $\mathrm{Inn}(G)$ are called *inner automorphisms of* G and the quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group of* G.

5 Lagrange's Theorem

Definition 5.1. Let G be any group and H a subgroup of G. The *index* of H in G, denoted $[G : H]$, is defined to be $\#(G/H)$, the size of the set of left cosets of H in G.

Theorem 5.2 (Lagrange's Theorem)**.** *Suppose that G is a finite group and H is any subgroup of G. Then $\#H$ divides $\#G$ and $\#H \cdot [G : H] = \#G$.*

Proof. The members of G/H form a partition of G hence

$$\#G = \sum_{A \in G/H} \#A.$$

Note that for any $g \in G$, the map $H \to g \cdot H$ given by $h \mapsto g \cdot h$ is a bijection. Hence the sets in G/H all have the same size, which agrees with $\#H$. Thus

$$\#G = \sum_{A \in G/H} \#A = \sum_{A \in G/H} \#H = [G : H] \cdot \#H,$$

as required. □

Corollary 5.3. *Suppose that G is a finite group and $g \in G$ is given. Then* $\mathrm{ord}(g)$ *divides* $\#G$.

Proof. The subgroup $\langle g \rangle$ has size $\mathrm{ord}(g)$. Conclude by applying Lagrange's theorem. □

Corollary 5.4. *Suppose that G is finite of prime order. Then any non-identity element of G generates G In particular, G is cyclic.*

Proof. Suppose that g is a nonidentity element of G. The order of g is at least 2, and it divides $\#G$, which is prime. Hence $\mathrm{ord}(g) = \#G$, so that $\langle g \rangle = G$. □

Corollary 5.5. *Let G be a finite group of order k and $g \in G$ an element. Then $g^k = 1$.*

Proof. Note $e := \mathrm{ord}(g)$ divides k, so that there exists some $m \in \mathbb{Z}$ such that $e \cdot m = k$. Thus $g^k = (g^e)^m = 1^m = 1$. □

Example 5.6. Consider $G := S_3$, a group of order 6, and put $H := \langle (123) \rangle = \{1, (123), (132)\}$. Note that $(12) \in N_G(H)$ since $(12)^{-1} = (12)$ and

$$(12)(123)(12) = (132),\ (12)(132)(12) = (123).$$

We have $H \leq N_G(H)$, but the above calulation shows this is a proper inclusion. Since $H \leq N_G(H) \leq G$, while H has size 3 and G has size 6, Largange's theorem ensures that $N_G(H) = G$ hence H is normal in G.

5.7 Products of subgroups

Definition 5.8. Let G be a group and suppose that H and K are both subgroups of G. Define $H \cdot K := \{h \cdot k \mid h \in H,\ k \in K\}$.

Theorem 5.9. *Suppose that H and K are subgroups of a group G. Assume that H and K are finite. Then*

$$\#(H \cdot K) = \frac{\#H \cdot \#K}{\#(H \cap K)}.$$

Proof. Note

$$H \cdot K = \bigcup_{h \in H} h \cdot K.$$

For $h, h' \in H$, $h' \cdot K = h \cdot K$ if and only if $h^{-1} \cdot h' \in K$ if and only if $h^{-1} \cdot h' \in K \cap H$ if and only if $h' \cdot (H \cap K) = h \cdot (H \cap K)$. Also, $\#(h \cdot K) = \#K$

and the cosets of K represented by elements of H are pairwise disjoint. Thus, the above calculations show that

$$\#(H \cdot K) = \#(H/(H \cap K)) \cdot \#K$$

and the assertion follows by applying Lagrange's theorem to $H \cap K \leq H$. $\square$

Theorem 5.10. *Suppose that H and K are subgroups of G. Then $H \cdot K$ is a subgroup of G if and only if $H \cdot K = K \cdot H$.*

Proof. Suppose that $H \cdot K = K \cdot H$. Note that $1 \in H \cdot K$ so that it is nonempty. If $h_1 \cdot k_1$ and $h_2 \cdot k_2$ are arbitrary elements of $H \cdot K$ with $h_i \in H$ and $k_i \in K$, then

$$(h_1 \cdot k_1) \cdot (h_2 \cdot k_2)^{-1} = h_1 \cdot (k_1 \cdot k_2^{-1}) \cdot h_2^{-1},$$

while $(k_1 \cdot k_2^{-1}) \cdot h_2^{-1} \in K \cdot H$ hence there exist $h_3 \in H$ and $k_3 \in H$ such that $(k_1 \cdot k_2^{-1}) \cdot h_2^{-1} = h_3 \cdot k_3$. Substituting into the above, we find

$$(h_1 \cdot k_1) \cdot (h_2 \cdot k_2)^{-1} = (h_1 \cdot h_3) \cdot k_3$$

which is visibly an element of $H \cdot K$. The "one-step subgroup test" ensures that $H \cdot K$ is a subgroup.

Conversely, suppose that $H \cdot K$ is a subgroup, and note that $H \leq H \cdot K$ and $K \leq H \cdot K$ hence $K \cdot H \leq H \cdot K$. Conversely, if $h \cdot k \in H \cdot K$ is arbitrary with $h \in H$ and $k \in K$ then $(h \cdot k)^{-1}$ is an element of $H \cdot K$ as well, since $H \cdot K$ is a subgroup. Thus there exist $h' \in H$ and $k' \in K$ such that

$$(h \cdot k)^{-1} = k^{-1} \cdot h^{-1} = h' \cdot k'.$$

Inverting again we find

$$h \cdot k = (k')^{-1} \cdot (h')^{-1} \in K \cdot H.$$

This shows that $H \cdot K \subset K \cdot H$ while the other inclusion was shown above. $\square$

Corollary 5.11. *Suppose that H and K are subgroups of a group G. If $H \leq N_G(K)$, then $H \cdot K$ is a subgroup of G. In particular, if K is a normal subgroup of G, then $H \cdot K$ is a subgroup of G for any $H \leq G$.*

Proof. If $H \leq N_G(K)$ then for all $h \in H$ one has $h \cdot K = K \cdot h$. Thus

$$H \cdot K = \bigcup_{h \in H} h \cdot K = \bigcup_{h \in H} K \cdot h = K \cdot H.$$

Apply the theorem above to conclude. $\square$

Lemma 5.12. *Suppose that H and K are subgroups of a group G and assume that $H \cdot K$ is a subgroup of G. Then $H \cdot K = \langle H, K \rangle$.*

Proof. We know that $\langle H, K \rangle$ is the smallest subgroup of G which contains both H and K, and since $H \cdot K$ is a subgroup with this property it follows that $\langle H, K \rangle \subset H \cdot K$. Conversely, since H and K are contained in $\langle H, K \rangle$ which is a subgroup, we have $H \cdot K \subset \langle H, K \rangle$. □

6 The Isomorphism Theorems

6.1 The Universal property of quotients

Let G be a group and N a normal subgroup of G. Suppose that $\varphi : G \to H$ is a homomorphism of groups. In this subsection, we study the question of whether φ factors through the canonical projection:

$$\pi : G \to G/N,$$

i.e. whether there exists a homomorphism $\overline{\varphi} : G/N \to H$ satisfying $\overline{\varphi} \circ \pi = \varphi$.

Suppose that such a $\overline{\varphi}$ exists and let $n \in N$ be given. Then $\varphi(n) = \overline{\varphi}(\pi(n)) = \overline{\varphi}(\mathbf{1}) = 1$ hence $n \in \ker \varphi$. We deduce therefore that $N \subset \ker \varphi$.

Conversely, if $N \subset \ker \varphi$, then the rule $\overline{\varphi}(g \cdot N) := \varphi(g)$ gives a well-defined function $\overline{\varphi} : G/N \to H$. Indeed, $g \cdot N = g' \cdot N$ if and only if $g^{-1} \cdot g' \in N$ which then implies that $\varphi(g^{-1} \cdot g') = 1$ since $N \subset \ker \varphi$, whence $\varphi(g)^{-1} \cdot \varphi(g') = 1$ so that $\varphi(g) = \varphi(g')$. It is straightforward to see that $\overline{\varphi}$ is indeed a homomorphism and that $\varphi = \overline{\varphi} \circ \pi$. We have thus proved the following.

Theorem 6.2. *Suppose that N is a normal subgrroup of G and that $\varphi : G \to H$ is a homomorphism. The following are equivalent:*

1. *One has $N \subset \ker \varphi$.*
2. *There exists a homomorphism $\overline{\varphi} : G/N \to H$ satisfying $\overline{\varphi} \circ \pi_N = \varphi$.*

Furthermore, if these conditions hold, then $\overline{\varphi}$ is uniquely determined by φ and N and the image of φ agrees with the image of $\overline{\varphi}$.

Proof. We only need to show uniqueness and the assertion about the image, as the equivalence of the two assertions was already discussed above. Suppose that $\psi : G/N \to H$ also satisfies condition (2). Then $\psi(g \cdot N) = \psi(\pi(g)) = \varphi(g) = \overline{\varphi}(g \cdot N)$ so that indeed $\overline{\varphi} = \psi$. The assertion about the image follows from the surjectivity of π. □

6.3 The first isomorphism theorem

Theorem 6.4. *Suppose that $\varphi : G \to H$ is a homomorphism of groups. Then the map $\overline{\varphi} : G/\ker\varphi \to H$ given by $\overline{\varphi}(g \cdot \ker\varphi) = \varphi(g)$ is injective, and thus $\overline{\varphi}$ induces an isomorphism*

$$G/\ker\varphi \cong \mathrm{im}(\varphi).$$

Proof. The kernel of $\overline{\varphi}$ consists of cosets of the form $g \cdot \ker\varphi$ with $\varphi(g) = 1$, equivalently, $g \in \ker\varphi$. Injectivity follows since $g \in \ker\varphi$ if and only if $g \cdot \ker\varphi = \ker\varphi$. Thus $\overline{\varphi} : G/\ker\varphi \to H$ is injective, and its image agrees with the image of φ, hence $\overline{\varphi}$ induces the desired isomorphism onto the image of φ. □

Corollary 6.5. *Suppose that $\varphi : G \to H$ is a homomorphism of groups. Then $[G : \ker\varphi] = \#\,\mathrm{im}(\varphi)$.*

Example 6.6. The homomorphism $\mathbb{Z} \to \mathbb{Z}/n$ given by $a \mapsto a \bmod n$ is surjective with kernel $n \cdot \mathbb{Z}$. Hence $\mathbb{Z}/n \cdot \mathbb{Z} \cong \mathbb{Z}/n$.

Example 6.7. The (real) *Heisenberg group* is the group of 3×3 upper-triangular real-valued matrices with 1's on the diagonal. This is indeed a group with respect to matrix multiplciation, and it is denoted by $H(\mathbb{R})$. The center of $H(\mathbb{R})$ consists of those matrices of the form

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

with $a \in \mathbb{R}$ arbitrary. This is also the kernel of the surjective homomorphism $H(\mathbb{R}) \to \mathbb{R} \times \mathbb{R}$ given by

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mapsto (a, b).$$

It follows that $H(\mathbb{R})/Z(H(\mathbb{R})) \cong \mathbb{R} \times \mathbb{R}$.

Example 6.8. The center of D_8 is the set $\{1, r^2\} = \langle r^2 \rangle$. There is a unique homomorphism (why?)

$$\varphi : D_8 \to \mathbb{Z}/2 \times \mathbb{Z}/2$$

which satisfies $\varphi(r) = (1 \bmod 2, 0 \bmod 2)$ and $\varphi(s) = (0 \bmod 2, 1 \bmod 2)$. This homomorphism φ is surjective (why?) and its kernel is $\langle r^2 \rangle$. Thus $D_8/\langle r^2 \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, and both are isomorphic to the so-called *Klein four group* V_4.

6.9 The second and third isomorphism theorems

Theorem 6.10 (The second isomorphism theorem)**.** *Let G be a group, and let $A, B \leq G$ be two subgroups. Assume that $A \leq N_G(B)$. Then:*

1. *$A \cdot B$ is a subgroup of G and B is a normal subgroup of $A \cdot B$.*
2. *$A \cap B$ is a normal subgroup of A.*
3. *The map $A/A \cap B \to A \cdot B/B$ given by $a \cdot (A \cap B) \mapsto a \cdot B$ is an isomorphism $A/(A \cap B) \cong (A \cdot B)/B$.*

Proof. We have already seen that $A \cdot B$ is a subgroup since $A \leq N_G(B)$. Since $B \leq N_G(B)$ as well, it follows that $A \cdot B \leq N_G(B)$ hence B is normal in $A \cdot B$. Consider the composition

$$\varphi : A \xrightarrow{\text{inclusion}} A \cdot B \xrightarrow{\pi_B} A \cdot B/B.$$

This is a composition of two homomorphisms and is thus again a homomorphism. Also, if $a \in A$ and $b \in B$ are arbitrary, then $a \cdot B = (a \cdot b) \cdot B$ hence $\varphi(a) = (a \cdot b) \cdot B$, thus φ is surjective.

If $a \in A \cap B$ then $\varphi(a) = 1$ since $a \cdot B = B$. Conversely, if $\varphi(a) = 1$ with $a \in A$ then $a \cdot B = B$ hence $a \in B$ so that $a \in A \cap B$. This shows that $\ker \varphi = A \cap B$, which then implies that $A \cap B$ is normal in A. Assertion (3) follows from the first isomorphism theorem. □

Theorem 6.11 (The third isomorphism theorem)**.** *Suppose that G is a group, and that H, K are two normal subgroups of G with $H \leq K$. Then K/H is a normal subgroup in G/H and the map*

$$G/K \to (G/H)/(K/H)$$

given by $g \cdot K \mapsto (g \cdot H) \cdot (K/H)$ is an isomorphism. In particular, one has $G/K \cong (G/H)/(K/H)$.

Proof. It is easy to see that K/H is a normal subgroup of G/H (details left as an exercise, see also the following subsection). Consider the composition

$$\varphi : G \xrightarrow{\pi_H} G/H \xrightarrow{\pi_{K/H}} (G/H)/(K/H).$$

As this is a composition of two surjective homomorphisms, it is again a surjective homomorphism. An element $k \in K$ satisfies $\varphi(k) = (k \cdot H) \cdot (K/H) = (K/H)$ since $k \cdot H \in K/H$ hence $K \subset \ker \varphi$. Conversely, if $g \in G$ satisfies $\varphi(g) = 1$ so that $g \cdot H \in K/H$, then there exists some $k \in K$ such that $k^{-1} \cdot g \in H \subset K$. In this case, there exists some $l \in K$ such that $k^{-1} \cdot g = l$ so that $g = k \cdot l \in K$, showing that $\ker \varphi \subset K$. Thus $\ker \varphi = K$ and the claim follows from the first isomorphism theorem. □

6.12 The Fourth Isomorphism Theorem

The fourth isomorphism theorem is sometimes called the *lattice theorem* because it relates the lattice of subgroups of a quotient G/N to a portion of the lattice of subgroups in the original group G. We formulate this theorem as a collection of several results.

Lemma 6.13. *Let $\varphi : G \to H$ be a homomorphism of groups and K a subgroup of H. Then $\varphi^{-1}(K) := \{x \in G \mid \varphi(x) \in K\}$ is a subgroup of G which contains $\ker \varphi$.*

Proof. Exercise. □

Theorem 6.14. *Let G be a group and N a normal subgroup of G. For H a subgroup of G containing N, H/N is a subgroup of G/N, and the map $H \mapsto H/N$ defines a bijection between the following two sets:*

1. *The set of subgroups of G which contain N.*
2. *The set of subgroups of G/N.*

The inverse of $H \mapsto H/N$ is given by the map sending K to $\pi_N^{-1}(K)$. Note that the lemma above ensures that $\pi_N^{-1}(K)$ is indeed a subgroup of G which contains N whenever K is a subgroup of G/N.

Proof. We have seen above that H/N is indeed a subgroup of G/N provided that $H \leq G$ contains N. We check that $\pi_N^{-1}(H/N) = H$. The containment $H \subset \pi_N^{-1}(H/N)$ is obvious. Conversely, if $g \in \pi_N^{-1}(H/N)$ then $\pi_N(g) = g \cdot N \in H/N$. Thus there exists some $h \in H$ such that $g \cdot N = h \cdot N$ and since $N \subset H$ it follows that $g \in H$ as well (why?!). This shows that $\pi_N^{-1}(H/N) = H$.

Suppose now that K is a subgroup of G/N. We show that $K = \pi_N^{-1}(K)/N$. The containment $\pi_N^{-1}(K)/N \subset K$ is clear. For the converse, suppose that $k \in K$. Since $K \subset G/N$, there exists some $g \in G$ such that $g \cdot N = k$. Hence $g \in \pi_N^{-1}(K)$ so that $k = g \cdot N \in \pi_N^{-1}(K)/N$, as required. □

For the rest of this subsection, we will work in the context of Theorem 6.14. We will show that the bijection described there is compatible with several constructions in the lattice of subgroups.

Lemma 6.15. *In the above context, suppose that A, B are subgroups of G which both contain N. Then $A \leq B$ if and only if $A/N \leq B/N$.*

Proof. If $A \leq B$ then clearly $A/N \leq B/N$. Conversely, suppose $A/N \leq B/N$ and let $a \in A$ be given. Then $a \cdot N \in A/N \subset B/N$ hence there exists some $b \in B$ such that $a \cdot N = b \cdot N$. Since $N \subset B$ it follows that $a \in B$ (why?!). This concludes the proof. □

Lemma 6.16. *In the above context, suppose that A, B are subgroups of G which both contain N, and that $A \leq B$. Then $[A : B] = [A/N : B/N]$.*

Proof. The map

$$A/B \to (A/N)/(B/N)$$

given by $a \cdot B \mapsto (a \cdot N) \cdot (B/N)$ is well-defined and bijective (details left as an exercise). The assertion follows. □

Lemma 6.17. *In the above context, suppose that A_i is a family of subgroups of G which contain N. Then*

$$\bigcap_i (A_i/N) = \left(\bigcap_i A_i \right) /N.$$

Proof. The containment $\supset$ is clear. Conversely, suppose that $a \in \bigcap_i (A_i/N)$ so that for all i there exists some $a_i \in A_i$ such that $a = a_i \cdot N$. Choose $g \in G$ such that $a = g \cdot N$. Thus $g \cdot N = a_i \cdot N$ and since A_i contains N it follows that $g \in A_i$ (why!?). This holds for all i, hence $g \in \bigcap_i A_i$ and the proof is done. □

Lemma 6.18. *In the above context, suppose that A_i is a family of subgroups of G which contain N. Then*

$$\langle \bigcup_i (A_i/N) \rangle = \langle \bigcup_i A_i \rangle /N.$$

Proof. We have

$$\langle \bigcup_i (A_i/N) \rangle = \bigcap_K K$$

where K varies over the subgroups of G/N which contain A_i/N for all i. In light of the bijection described above, each such K has the form L/N for some $L \leq G$ with $N \subset L$, and by the lemma above $A_i/N \subset L/N$ if and only if $A_i \subset L$. Thus the intersection could be equally described as

$$\langle \bigcup_i (A_i/N) \rangle = \bigcap_L (L/N)$$

where L varies over all subgroups of G which contain N and which contain A_i for all i. By the previous lemma, this intersection is precisely

$$(\bigcap_L L)/N$$

with L varying over the same set, and, by definition, this is $\langle \bigcup_i A_i \rangle / N$. $\square$

Lemma 6.19. *In the above context, suppose that H is a subgroup of G which contains N. Then H is normal in G if and only if H/N is normal in G/N.*

Proof. Suppose H is normal. Let $h \cdot N \in H/N$ and $g \cdot N \in G/N$ be given. Then $(g \cdot N) \cdot (h \cdot N) \cdot (g \cdot N)^{-1} = (g \cdot h \cdot g^{-1}) \cdot N \in H/N$ since H is normal, hence H/N is indeed normal.

Conversely, suppose H/N is normal. Let $h \in H$ and $g \in G$ be given. Arguing similarly to the above, we find $(g \cdot h \cdot g^{-1}) \cdot N \in H/N$ since H/N is normal, but this implies that $g \cdot h \cdot g^{-1} \in H$ because $N \subset H$ (why!?). $\square$

7 Group actions

In this section, we continue our discussion about the actions of groups on sets. Given a group G and a set X, recall that an action of G on X is a function

$$G \times X \to X$$

often denoted $(g, x) \mapsto g \cdot x$, which satisfies the following conditions

1. One has $1 \cdot x = x$ for all $x \in X$.
2. For all $a, b \in G$ and $x \in X$, one has $a \cdot (b \cdot x) = (a \cdot b) \cdot x$.

Recall that to any action of G on X as above, one can associate its so-called *permutation representation*

$$\rho : G \to \mathrm{Per}(X)$$

defined by $\rho(g)(x) = g \cdot x$. And conversely, given $\rho : G \to \mathrm{Per}(X)$, the rule $g \cdot x := \rho(g)(x)$ defines an action of G on X. Thus, actions of G on X are in one-to-one correspondence with homomorphisms $\rho : G \to \mathrm{Per}(X)$.

Definition 7.1. Suppose that G acts on X with associated permutation representation ρ.

1. The *kernel* of the action of G on X is the kernel of ρ. This is precisely the set $\{g \in G \mid \forall x \in X,\ g \cdot x = x\}$.
2. Given $x \in X$, the *stabilizer of* x is the subgroup
$$\mathrm{Stab}_G(x) := \{g \in G \mid g \cdot x = x\}$$
of G.
3. Given $x \in X$, the *orbit* of x is the subset
$$\mathrm{Orb}_G(x) := \{g \cdot x \mid g \in G\}$$
of X.
4. We say that the action of G on X is *faithful* if the kernel of the action is trivial. In other words, G acts faithfully on X if its associated permutation representation is injective.
5. We say that the action of G on X is *transitive* if there exists some $x \in X$ such that $X = \mathrm{Orb}_G(x)$.

Lemma 7.2. *Let G act on a set X. The orbits of the action form a partition of X, with associated equivalence relation given by $x \sim y$ if and only if $g \cdot x = y$ for some $g \in G$.*

Proof. Unfolding the definition of the orbirs, it suffices to prove that the relation described in the statement is an equivalence relation. Clearly $x \sim x$ since $1 \cdot x = x$. If $x \sim y$ hence $g \cdot x = y$ for some $g \in G$ then $g^{-1} \cdot y = x$ (why?) hence $y \sim x$. If $x \sim y$ and $y \sim z$ hence $g \cdot x = y$ and $h \cdot y = z$ for some $g, h \in G$, then $(h \cdot g) \cdot x = z$ hence $x \sim z$ (why?). This concludes the proof. □

Theorem 7.3 (The orbit-stabilizer theorem)**.** *Let G act on a set X and let $x \in X$ be given. Then the map*
$$\mathrm{Orb}_G(x) \to G/\mathrm{Stab}_G(x)$$
given by $g \cdot x \mapsto g \cdot \mathrm{Stab}_G(x)$ is a well-defined bijection. In particular, one has
$$\#\,\mathrm{Orb}_G(x) = [G : \mathrm{Stab}_G(x)].$$

Proof. The function is well-defined since $g \cdot x = h \cdot x$ if and only if $h^{-1} \cdot g \in \mathrm{Stab}_G(x)$ (why?) which is equivalent to $g \cdot \mathrm{Stab}_G(x) = h \cdot \mathrm{Stab}_G(x)$. This also shows that the map $G/\mathrm{Stab}_G(x) \to \mathrm{Orb}_G(x)$ defined by $g \cdot \mathrm{Stab}_G(x) \mapsto g \cdot x$ is well-defined, and it is now easy to see that these functions are invereses of eachother, hence the claim. □

7.4 Left multiplication

In this subsection, we consider a group G and let G act on itself by *left multiplication*. Thus, the associated permutation representation is the homomorphism

$$\rho : G \to \mathrm{Per}(G), \quad \rho(g)(h) = g \cdot h.$$

Note that the G in $\mathrm{Per}(G)$ is considered *merely as a set*.

Lemma 7.5. *This action is faithful.*

Proof. The kernel is the set of all $g \in G$ such that $g \cdot h = h$ for all $h \in G$. Taking $h = 1$ we find $g = g \cdot 1 = 1$, hence this kernel is trivial. □

Corollary 7.6 (Cayley's Theorem)**.** *The group G is isomorphic to a subgroup of $\mathrm{Per}(G)$. In particular, if G is finite of order n, then G is isomorphic to a subgroup of S_n.*

Proof. The first isomorphism theorem tells us that $G/\ker(\rho)$ is isomorphic to $\mathrm{im}(\rho)$, and since ρ is injective by the previous lemma we find that G is isomorphic to $\mathrm{im}(\rho) \leq \mathrm{Per}(G)$. If G has size n then $\mathrm{Per}(G) \cong S_n$, so the assertion follows by considering the composition

$$G \xrightarrow{\rho} \mathrm{Per}(G) \cong S_n,$$

which is again injective. □

Now let us suppose that H is a subgroup of G. Then left multiplication induces an action of G on G/H via

$$g \cdot (g' \cdot H) := (g \cdot g') \cdot H.$$

This is well-defined since $a \cdot H = b \cdot H$ if and only if $b^{-1} \cdot a \in H$ if and only if $(g \cdot a)^{-1} \cdot (g \cdot b) \in H$, if and only if $(g \cdot a) \cdot H = (g \cdot b) \cdot H$.

Theorem 7.7. *Suppose that G is a finite group and H is a subgroup such that $[G : H]$ is the smallest prime factor of $\#G$. Then H is normal.*

Proof. Let G act on G/H by left multiplication as above, and consider the kernel K of this action. Note that K is a normal subgroup of G since it is the kernel of some homomorphism originating from G. By definition, if $k \in K$ then $k \cdot (1 \cdot H) = k \cdot H = H$ hence $k \in H$. Thus $K \leq H$. Write $[H : K] = m$ and $[G : H] = p$ (the smallest prime factor of $\#G$). Thus $[G : K] = m \cdot p$ while the first isomorphism theorem shows that G/K is isomorphic to a subgroup of $\mathrm{Per}(G/H) \cong S_p$, which has size $p!$. It follows that $p \cdot m | p!$ hence $m | (p-1)!$, but since p is the smallest prime factor of $\#G$ and m divides $\#G$, this is only possible if $m = 1$. Thus $H = K$ and H is normal. □

7.8 The conjugation action

In this subsection, we consider the action of G on itself by *conjugation*. In other words, the permutation representation $\rho : G \to \mathrm{Per}(G)$ is given by

$$\rho(g)(h) = g \cdot h \cdot g^{-1}.$$

We can define a conjugation action of G on the powerset $\mathcal{P}(G)$ of G in a similar way, with permutation representation given by $\rho(g)(S) = g \cdot S \cdot g^{-1}$. These actions are compatible in the sense that

$$g \cdot \{h\} \cdot g^{-1} = \{g \cdot h \cdot g^{-1}\}$$

for $g, h \in G$.

Definition 7.9. Let $a, b \in G$ (resp. $S, T \in \mathcal{P}(G)$) be given. We say that a and b (resp. S and T) are *conjugates* if they lie in the same orbit with respect to the conjugation action described above. This defines an equivalence relation on the set G (resp. the set $\mathcal{P}(G)$). The conjugacy class of a (resp. S) is the equivalence class of a (resp. S) with respect to this equivalence relation (equivalently, its orbit with respect to the conjugation action).

Fact 7.10. *Let $a \in G$ and $S \in \mathcal{P}(G)$ be given, and let G act on G and $\mathcal{P}(G)$ by conjugation.*

1. *One has $N_G(S) = \mathrm{Stab}_G(S)$.*
2. *One has $C_G(a) = \mathrm{Stab}_G(a)$.*

Proof. This is a simple matter of unfolding definitions. □

Corollary 7.11. *Let $a \in G$ and $S \in \mathcal{P}(G)$ be given.*

1. *The number of conjugates of S is the index $[G : N_G(S)]$.*
2. *The number of conjugates of a is the index $[G : C_G(a)]$.*

Proof. Unfold definitions and apply the orbit-stabilizer theorem. □

Lemma 7.12. *Let $a \in G$ be given and let S be its conjugacy class. The following are equivalent:*

1. *$a \in Z(G)$.*
2. *$S = \{a\}$.*

3. $S \cap Z(G) \neq \varnothing$.

4. $S \subseteq Z(G)$.

Proof. Exercise. □

Theorem 7.13 (The Class Equation)**.** *Let G be a finite group, and let $g_1, \ldots, g_r$ be representatives of the distinct conjugacy classes of G which are not contained in $Z(G)$. Then*

$$\#G = \#Z(G) + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Proof. Let $C_1, \ldots, C_k$ denote the conjugacy classes of G. We have

$$\#G = \sum_i \#C_i.$$

By the previous lemma, we deduce (why?)

$$\#G = \#Z(G) + \sum_{i,\ \#C_i > 1} \#C_i$$

and by the corollay above, if g represents C_i then $\#C_i = [G : C_G(g)]$. The assertion follows. More details given in the handwritten notes. □

Definition 7.14. Let p be a prime. A finite group G is called a *p-group* provided that $\#G = p^k$ for some k.

Corollary 7.15. *Let G be a nontrivial finite p-group. Then $Z(G) \neq \{1\}$.*

Proof. Since p divides $[G : C_G(g)]$ by Lagrange's theorem whenever $g \notin Z(G)$, and p divides $\#G$, it follows that p divides $\#Z(G)$, hence $\#Z(G) > 1$ so that $Z(G)$ cannot be trivial. □

Lemma 7.16. *Let G be a group and suppose that $G/Z(G)$ is cyclic. Then G is abelian.*

Proof. Let $g \cdot Z(G)$ be a generator of $G/Z(G)$. Then any element of G has the form $g^k \cdot h$ for some $h \in Z(G)$ (why?). Two such elements always commute since elements of $Z(G)$ commute with any element of G and powers of g commute with other powers of g. □

Corollary 7.17. *Let p be a prime and G a group of size p^2. Then G is abelian. In fact, $G \cong \mathbb{Z}/p^2$ or $G \cong \mathbb{Z}/p \times \mathbb{Z}/p$.*

Proof. The center $Z(G)$ is nontrivial. If $Z(G) = G$, then we are done, and otherwise $Z(G)$ must have size p, thus $G/Z(G)$ is cyclic of order p. It follows that G is abelian. The last assertion was discussed in detail in the handwritten notes on 2021-11-22 (alternatively, use the classification of finitely-generated abelian groups, which will be covered later). □

7.18 More on Symmetric Groups

We are now in a good position to discuss symmetric groups again. Recall that the symmetric group S_n on n-letters is *defined* as the permutation group of $S := \{1, \ldots, n\}$. In particular, there is a natural action of S_n on S whose permutation representation is the *identity homomorphism.*

Lemma 7.19. *Any element σ of S_n has a presentation as a product of disjoint cycles, which is unique up-to permutations of the disjoint cycles.*

Proof. Consider $H = \langle \sigma \rangle$. Compose with the inclusion $H \hookrightarrow S_n$ to obtain an action of H on S. If $A_1, \ldots, A_k$ denote the orbits of this action of H on S, then

$$S = A_1 \cup \cdots \cup A_k,$$

and these are disjoint unions. This is simply because such an action yields an equivalence relation on S, and the orbits are precisely the equivalence classes (see the discussion above).

For each $i = 1, \ldots, k$, let $a_i \in A_i$ be a representative of the orbit A_i (which is really an equivalence class!). The action of H on S restricts to an action of H on A_i (why?). This action on A_i is transitive by the definition of A_i (recall that A_i is itself an orbit), hence, letting $T_i := \mathrm{Stab}_H(a_i)$ we find that A_i is in bijection with H/T_i, and that this bijection is compatible with the action of H, where H acts on H/T_i by left multiplication.

So it suffices to study how H acts on H/T_i. But since H is cyclic, T_i is again cyclic and H/T_i is cyclic as well. Letting d be the smallest positive integer such that $\sigma^d \in T_i$, we deduce that $H/T_i = \{1 \cdot T_i, \sigma \cdot T_i, \ldots, \sigma^{d-1} \cdot T_i\}$. Tracing through the definitions, we find that σ acts on A_i as the cycle $\sigma_i := (a_i,\ \sigma a_i, \ldots,\ \sigma^{d-1} a_i)$. The A_i, $i = 1, \ldots, k$, are disjoint, hence σ acts on S as a product of the disjoint cycles σ_i defined above. Uniqeness is left as an exercise (it follows from the construction above). □

7.20 Transpositions

Recall that a *transposition* is an element of S_n which is a cycle of length two, i.e. an element of the form (i, j) for some $1 \leq i < j \leq n$.

Lemma 7.21. *Let $a_1, \ldots, a_k \in S$ be distinct. The cycle $(a_1 a_2 \ldots a_k)$ agrees with the product of transpositions*

$$(a_1 a_m) \cdot (a_1 a_{m-1}) \cdots (a_1 a_2).$$

Proof. Clear. □

Corollary 7.22. *Any element of S_n can be written as a product of transpositions. In particular, letting T denote the set of all transpositions in S_n, one has $S_n = \langle T \rangle$.*

Proof. Since any element of S_n is a product of cycles, and any cycle is a product of transpositions, the assertion follows. □

7.23 Conjugation in S_n

Let us study conjugation in S_n, particularly for cycles.

Lemma 7.24. *Let $\sigma \in S_n$ be given, and let $(a_1, \ldots, a_k)$ be a cycle in S_n. Then one has*

$$\sigma \cdot (a_1, \ldots, a_k) \cdot \sigma^{-1} = (\sigma a_1, \ldots, \sigma a_k).$$

Proof. Put $\tau := \sigma \cdot (a_1, \ldots, a_k) \cdot \sigma^{-1}$. Since $(a_1, \ldots, a_k)$ fixed all b such that $b \neq a_i$ for all i, it follows that τ fixes σb for such b (by the definition of τ). On the other hand, given $i = 1, \ldots, k$, we can easily calculate that $\tau(\sigma a_i) = \sigma a_{i+1}$ if $i < k$ and $\tau(\sigma a_k) = \sigma a_1$ (why?). The claim follows. □

Definition 7.25. Let σ be an element of S_n. The *cycle type* of σ is the multiset of lengths of cycles appearing in the decomposition of σ into a product of disjoint cycles (including all necessary cycles of length 1 so that every element of $\{1, \ldots, n\}$ appears in this presentation).

For example, the cycle type of

$$(1238)(45) \in S_{14}$$

is

$$\{4, 2, 1, 1, 1, 1, 1, 1, 1, 1\}$$

while the cycle type of

$$(12345)(341) \in S_6$$

is

$$\{5, 1\}$$

since

$$(12345)(341) = (14235).$$

Theorem 7.26. *Two elements of S_n are conjugate if and only if they have the same cycle type. In particular, the conjugacy classes of S_n are in bijection with the partitions of n.*

Proof. If two permutations are conjugate then they have the same cycle type by the above calculation for conjugacy in S_n. Conversely, if two permutations a and b have the same cycle type, say

$$a = a_1 \cdots a_k,\ b = b_1 \cdots b_k$$

with a_i and b_i of the same length, $a_1, \ldots, a_k$ pairwise disjoint and $b_1, \ldots, b_k$ pairwise disjoint. Then there exists some permutation $\sigma \in S_n$ sending the numbers appearing in the decomposition of a into cycles, as above, to the numbers appearing in the decomposition of b, *in order*. This shows that $\sigma a \sigma^{-1} = b$.

Since the sum of the integers in the cycle type of $\sigma \in S_n$ adds up to n, there is a bijection between cycle types and partitions of n, so the claim follows. See the handwritten notes for concrete examples of computations involving representatives of these conjugacy classes. □

7.27 The sign of a permutation

Let us consider the set of polynomials in n variables with integer coefficients

$$P := \mathbb{Z}[X_1, \ldots, X_n]$$

For $f(X_1, \ldots, X_n) \in P$ and $\sigma \in S_n$, define

$$\sigma \cdot f = f(X_{\sigma 1}, \ldots, X_{\sigma n}).$$

Exercise 7.28.

1. In the above context, the map $(\sigma, f) \mapsto \sigma \cdot f$ defines an action of S_n on P.
2. For $a \in \mathbb{Z}$, $f \in P$ and $\sigma in S_n$ one has $\sigma \cdot (a \cdot f) = a \cdot (\sigma \cdot f)$.
3. For $f, g \in P$ and $\sigma \in S_n$, one has $\sigma \cdot (f + g) = \sigma \cdot f + \sigma \cdot g$.
4. For $f, g \in P$ and $\sigma \in S_n$, one has $\sigma \cdot (f \cdot g) = (\sigma \cdot f) \cdot (\sigma \cdot g)$.

We will be particularly interested in the polynomial

$$\Delta_n := \prod_{1 \le i < j \le n} (X_i - X_j).$$

Lemma 7.29. *For all $\sigma \in S_n$, one has $\sigma \cdot \Delta_n = \pm\Delta_n$.*

Proof. The action of σ is compatible with multiplciation. Since σ acts as a permutation of $S = \{1, \ldots, n\}$, we see that σ permutes the factors $(X_i - X_j)$ of Δ_n, possibly introducing a negative in case $\sigma j < \sigma i$. In any case, we find that

$$\sigma \cdot \Delta_n = \prod_{1 \leq i < j \leq n} \sigma(X_i - X_j) = \prod_{1 \leq i < j \leq n} \pm(X_i - X_j) = \pm\Delta_n,$$

as required. □

Definition 7.30. The *sign* of $\sigma \in S_n$ is the unique element $\varepsilon(\sigma) \in \{\pm 1\}$ such that $\sigma \cdot \Delta_n = \varepsilon(\sigma) \cdot \Delta_n$. A permutation $\sigma \in S_n$ is called *even* if $\varepsilon(\sigma) = 1$, and odd if $\varepsilon(\sigma) = -1$.

Lemma 7.31. *The map $\varepsilon : S_n \to \{\pm 1\}$ is a group homomoprhism, where $\{\pm 1\}$ is a group with respect to multiplication.*

Proof. We have

$$\begin{aligned} \varepsilon(\sigma \cdot \tau) \cdot \Delta_n &= \sigma \cdot (\tau \cdot \Delta_n) \\ &= \sigma \cdot (\varepsilon(\tau) \cdot \Delta_n) \\ &= \varepsilon(\tau) \cdot (\sigma \cdot \Delta_n) \\ &= \varepsilon(\tau) \cdot (\varepsilon(\sigma) \cdot \Delta_n) \\ &= \varepsilon(\sigma) \cdot \varepsilon(\tau) \cdot \Delta \end{aligned}$$

The assertion follows. □

Definition 7.32. The n-th *alternating group*, denoted A_n, is the kernel of $\varepsilon : S_n \to \{\pm 1\}$.

Lemma 7.33. *The subgroup A_n is normal in S_n.*

Proof. Clear, since A_n is a kernel of some homomorphism from S_n, and kernels are always normal. □

Lemma 7.34. *For $n \geq 2$, one has $\#A_n = n!/2$.*

Proof. The map $\varepsilon : S_n \to \{\pm 1\}$ is surjective when $n \geq 2$, so the claim follows from Lagrange's theorem and the first isomorphism theorem. □

Lemma 7.35. *If $(i, j) \in S_n$ is given with $1 \leq i < j \leq n$, then $\varepsilon((i, j)) = -1$.*

Proof. Note that $\varepsilon(\sigma \cdot \tau \cdot \sigma^{-1}) = \varepsilon(\tau)$ for all σ, τ. By choosing σ to send i to 1 and j to 2, we may as well assume that $(i, j) = (1, 2)$, in which case the claim can be checked explicitly using the definition. □

Corollary 7.36. *The following hold:*

1. *A product of n transpositions is even if and only if n is even and odd if and only if n is odd.*
2. *A cycle of length m is even if and only if m is odd and odd if and only if m is even.*
3. *Let $\sigma_1, \ldots, \sigma_k$ be cycles of length $m_1, \ldots, m_k$, respectively. Let N be the size of $\{i \mid m_i \text{ is even}\}$. Then $\sigma_1 \cdots \sigma_k$ is even if and only if N is even, and is odd if and only if N is odd.*

Proof. This follows directly from the discussion above (details left as an exercise). □

7.37 Cauchy's Theorem

We conclude this section with a proof of *Cauchy's Theorem*.

Theorem 7.38 (Caychy's Theorem)**.** *Let G be a finite group and p a prime number dividing the order of G. Then G has an element of order p.*

Proof. Let S denote the set of p-tuples $(g_1, \ldots, g_p)$ with $g_i \in G$ which satisfy

$$g_1 \cdots g_p = 1.$$

This forces that $g_p = (g_1 \cdots g_{p-1})^{-1}$ while $g_1, \ldots, g_{p-1}$ have no restriction hence S has size $N := n^{p-1}$ where $n = \#G$. Let $\sigma \in \mathrm{Per}(S) \cong S_N$ be the unique element which acts on $(g_1, \ldots, g_p)$ as

$$\sigma \cdot (g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1}).$$

The cycle type off σ must be of the form $\{p, p, \ldots, p, 1, 1, \ldots, 1\}$ (why?!), and say that there are m terms p appearing and k terms 1 appearing in this cycle type. Thus $N = m \cdot p + k$ and since p divides N it follows that p divides k. Since $k \geq 1$ (because σ fixes the p-tuple $(1, 1, \ldots, 1)$), it follows that $k \geq 2$, hence there must be some p-tuple $(g_1, \ldots, g_p) \in S$ which is fixed by σ and which does not contain only the identity as its factors. Such a p-tuple must be of the form $(g, g, \ldots, g)$ with g a nonidentity element of G, and this implies that this element g must have order p. □

8 The Sylow Theorems

Let G be a finite group and p a prime number. We can write the order of G uniquely as

$$p^k \cdot m$$

where p does not divide m. I.e. k is the maximal power of p such that p^k divides the order of G.

A subgroup of G which is a p-group will be called a *p-subgroup*. If a subgroup H of G has order p^k, with k as above, then H is called a *Sylow p-subgroup* of G. The collection of all Sylow p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$, and the number of Sylow p-subgroups of G is denoted by $n_p(G)$ (or just n_p if G is understood from context).

8.1 The first Sylow theorem

Theorem 8.2. *Let G be a finite group and p a prime number. Then G has a Sylow p-subgroups, i.e. $\mathrm{Syl}_p(G)$ is nonempty hence $n_p(G) \geq 1$.*

Proof. Proceed by (strong) induction on the order of G, with the base-case $\#G = 1$ being trivial. Without loss of generality assume that p divides $\#G$, as otherwise the trivial subgropu is a Sylow p-subgroup of G.

Assume first that p divides the order of $Z(G)$, and use Cauchy's theorem to deduce that $Z(G)$ has an element g of order p. The subgroup $N := \langle g \rangle$ has order p, and N is normal in G (why?). By induction, G/N has a Sylow p-subgroup, say P_0. If we write $\#G = p^k \cdot m$ with m coprime to p, then $\#(G/N) = p^{k-1} \cdot m$ by Lagrange's theorem, hence P_0 has size p^{k-1}. Let P denote the preimage of P_0 under the canonical projection $\pi : G \to G/N$. By the lattice theorem, we know that $N \leq P$ and $P/N = P_0$, hence P has order p^k by Lagrange's theorem. Hence, P is a Sylow p-subgroup of G.

Now assume that p does not divide the order of $Z(G)$. By the class equation, there must be an element $g \in G \setminus Z(G)$ such that p does not divide the index $[G : C_G(g)]$ (why?!). Since g is noncentral, $[G : C_G(g)] \geq 2$, and by Lagrange's theorem it follows that $\#C_G(g) = p^k \cdot m'$ for some m' coprime to p (actually, $m = m' \cdot [G : C_G(g)]$). In any case, since the order of $C_G(g)$ is strictly smaller than that of G, we may apply the inductive hypothesis and deduce that $C_G(g)$ has a Sylow p-subgroup, say P, whose order is p^k. This subgroup is also a subgroup of G, and by mere definitions, we find that P is also a Sylow p-subgroup of G. □

8.3 The second and third Sylow theorems

Let us prove a lemma before proceeding to the proofs of Sylow II and III.

Lemma 8.4. *Suppose that P is a Sylow p-subgroup of G and that Q is any p-subgroup of G. then $Q \cap N_G(P) = Q \cap P$.*

Proof. Consider $H := Q \cap N_G(P)$ and, since P is contained in $N_G(P)$, note that $Q \cap P$ is contained in H. Thus it suffices to show that H is contained in $Q \cap P$, for which it sufficees to show that H is contained in P since H is clearly contained in Q. Since H is contained in $N_G(P)$, we note that $P \cdot H$ is a subgroup of G, and by the formula for $\#(P \cdot H)$ we readily deduce that $P \cdot H$ is a p-subgroup of G. Since P is contained in $P \cdot H$, and P is a *maximal* p-subgroup of G (by the definition of a Sylow subgroup), it follows that $P = P \cdot H$ hence $H \leq P \cdot H = P$, as required. □

Now suppose that P is any Sylow p-subgroup of G, and that Q is a p-subgroup of G. Consider the set $S := \{P_1, \ldots, P_r\}$ of conjugates of P, and let Q act on S by conjugation. Write

$$S = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_k$$

as a disjoint union of orbits with respect to this action of Q, and rearrange the P_i so that $P_i \in \mathcal{O}_i$ for $i = 1, \ldots, k$.

The size of $\mathcal{O}_i$ is precisely $[Q : N_Q(P_i)]$ by the orbit-stabilizer theorem, while

$$N_Q(P_i) = N_G(P_i) \cap Q = Q \cap P_i$$

by the above lemma.

Lemma 8.5. *In the above context, r is congruent to 1 modulo p.*

Proof. In the above discussion, take $Q = P_1$, hence $\#\mathcal{O}_1 = 1$, while $P_i \cap P_1$ is a *proper* subgroup of P_1 for all $i = 2, \ldots, k$, hence $\#\mathcal{O}_i = [P_1 : P_1 \cap P_i] = p^{e_i}$ for some $e_i \geq 1$. This shows that $r = \#Ocal_1 + \cdots + \#\mathcal{O}_k$ is the sum of 1 and some (positive) powers of p, from which it follows that $r \equiv 1\ (p)$, as required. □

Theorem 8.6 (Sylow II)**.** *Let P be a p-Sylow subgroup of G and Q a p-subgroup of G. Then there exists some $g \in G$ such that $Q \leq g \cdot P \cdot g^{-1}$. In particular, all Sylow p-subgroups of G are conjugate.*

Proof. Let $S = \{P_1, \ldots, P_r\}$ denote the conjugates of P. If Q is not contained in any P_i, then $Q \cap P_i$ is a proper subgroup of P_i for all i, hence $[Q : Q \cap P_i] = p^{e_i}$ for some $e_i \geq 1$ for all i. In the notation above, this would mean that all of the $\#\mathcal{O}_i$, $i = 1, \ldots, k$, are p^{e_i}, and this would imply that $r \equiv 0\ (p)$. The claim above shows that, rather, $r \equiv 1\ (p)$, which is impossible.

As for the final statement about all Sylow p-subgroups being conjugate, simply apply the result to any given Sylow p-subgroup Q to deduce that Q is contained in $g \cdot P \cdot g^{-1}$ for some g, and note that Q and $p \cdot P \cdot g^{-1}$ have the same (finite) size, so that they must be equal. □

Theorem 8.7 (Sylow III)**.** *The number $n_p(G)$ satisfies*

$$n_p(G) \equiv 1\ (p).$$

Furthermore, $n_p(G) = [G : N_G(P)]$ for any given $P \in \mathrm{Syl}_p(G)$, hence $n_p(G) | \#G$. If we write $\#G = p^\alpha \cdot m$ with $\gcd(p, m) = 1$, then $n_p(G) | m$.

Proof. In the notation above, we note that $n_p(G) = r$, hence the fact that $n_p(G) \equiv 1\ (p)$ follows from the above lemma. The orbit stabilizer theorem them implies that $r = n_p(G) = [G : N_G(P)]$, by identifying S with the orbit of P with respect to the conjugation action of G, and $N_G(P)$ with the stabilizer of P. The remaining assertions are left as an (easy) exercise (see the handwritten notes for more detail). □

Corollary 8.8. *Let P be a Sylow p-subgroup of a finite group G. The following are equivalent*

1. *P is the unique Sylow p-subgroup of G, i.e. $n_{p(G)} = 1$.*
2. *P is normal in G.*
3. *P is characteristic, i.e. for all automorphisms $\varphi : G \to G$, one has $\varphi(P) = P$.*
4. *Any subgroup of G which is generated by elements of p-power order is a p-group.*

Proof. The equivalence of 1 and 2 follows from the fact that all Sylow p-subgroups are conjugates, and the equivalence with 3 then follows from the definition of a Sylow p-group, while noting that characteristic subgroups are necessarily normal. Detailes are left as an exercise (see the handwritten notes for some further discussion).

As for the equivalence with the last assertion, suppose that X is a set of elements of G of p-power order. Any such element must be contained in a Sylow p-subgroup by the second Sylow theorem. If there is a unique such Sylow p-subgroup P, then X is contained in P hence $\langle X \rangle$ is contained in P, so Lagrange's theorem implies that $\langle X \rangle$ is a p-subgroup. Conversely, take X to be the union of all Sylow p-subgroups (again, Lagrange implies that such an X has only elements of p-power order). By assumption 4, $\langle X \rangle$ is a p-group, hence it is contained in a Sylow p-subgroup P of G. The definitions imply that P is the unique Sylow p-subgroup of G (why?). □

8.9 Groups of oorder $p \cdot q$

Suppose in this section that $\#G = p \cdot q$ where p and q are primes with $p < q$. Let P resp. Q be a Sylow p resp. q subgroup of G. Note that $n_q | p$, while $n_q \equiv 1\ (q)$ ensures that $n_q = 1$, hence Q is normal in G. If p does not divide $q - 1$, then a similar argument shows that P is normal as well.

Suppose for the rest of this subsection that P is normal in G. Then G acts on P by conjugation, and the induced homomorphism

$$G \to \mathrm{Aut}(P)$$

has kernel $C_G(P)$. Thus $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P) \cong (\mathbb{Z}/p)^\times$, which has order $p - 1$. Since neither p nor q can divide $p - 1$, this implies that $G = C_G(P)$, hence P is contained in $Z(G)$.

Since P and Q have prime orders, they are both cyclic. If x is a generator of P and y is a generator of Q, then the above ensures that x and y commute. From this it follows that $P \cdot Q \cong \mathbb{Z}/(p \cdot q)$ (why?), and in particular $G = P \cdot Q \cong \mathbb{Z}/(p \cdot q)$ is cyclic.

8.10 Groups of order 30

Suppose that G has order 30. We will show that G has a normal subgroup which is isomorphic to $\mathbb{Z}/15$. oLet P be a Sylow 5-subgroup of G and Q a Sylow 3-subgroup of G. If either P or Q is normal in G, then $P \cdot Q$ is a subgroup of G, and Lagrange's theorem implies that $P \cdot Q$ has order 15, hence $[G : P \cdot Q] = 2$, so that $P \cdot Q$ is normal (any subgroup of index 2 is normal).

Also, if either P or Q is normal in G, then both P and Q must be characteristic subgroups of $P \cdot Q$ (this follows from the previous example, taking $p = 3$ and $q = 5$, and the group to be $P \cdot Q$). In this case, since $P \cdot Q$

is normal, if $g \in G$ is given, then

$$g \cdot P \cdot g^{-1} \leq g \cdot (P \cdot Q) \cdot g^{-1} = P \cdot Q$$

with the map $t \mapsto g \cdot t \cdot g^{-1}$ being an automorphism of $P \cdot Q$, hence $g \cdot P \cdot g^{-1} = P$, so that P is normal in G. Similarly, Q is normal in G. In this case, the previous example shows that $P \cdot Q$ is a normal subgroup isomorphic to $\mathbb{Z}/15$.

The argument above shows that the other case to consider is when neither P nor Q is normal in G. In this case, the Sylow theorems ensure that $n_5 = 6$ and $n_3 = 10$ (why?). If g is an element of order 5 in G, then g is contained in one of the Sylow 5-subgroups of G. Any two distinct Sylow subgroups of G intersect trivially (why?), while each Sylow 5-subgroup o G has precisely 4 elements of order 5. Thus G must contain $4 \cdot 6 = 24$ elements of order 5. Similarly, G would contain $2 \cdot 10 = 20$ elements of order 3. As there is no overlap between the collection of elements of order 5 and the collection of elements of order 3, this would show that G contains at least $24 + 20 = 44$ elements, which is absurd since $\#G = 30$. It follows that either P or Q must be normal, so the previous argument applies to show that G has a normal subgroup isomorphic to $\mathbb{Z}/15$.

8.11 Groups of order 12

Suppose G has order 12. We show that G has a normal Sylow 3-subgroup or a normal Sylow 2-subgroup.

If $n_3 = 1$, then we are done, since a Sylow 3-subgroup of G would be normal. Suppose then that $n_3 \neq 1$, and let P be a Sylow 3-subgroup. Since $n_3|4$ and $n_3 \equiv 1$ (3), we must have $n_3 = 4$. This shows that G contains 8 elements of order 3. If Q is a Sylow 2-subgroup of G, then Q contains 4 elements of order dividing 4. Since $8 + 4 = 12$, it follows that Q must be unique (why?).

In fact, we can check that G must be isomorphic to A_4 in this case, as follows. Note $n_3 = [G : N_G(P)] = 4$, hence $N_G(P) = P$. Now G acts by conjugation on its four Sylow 3-subgroups, providing a permutation representation

$$\rho : G \to S_4.$$

The kernel of ρ is contained in $N_G(P) = P$ (why?), and since P is not normal by assumption, it follows that this kernel is trivial (why?). Thus G is isomorphic to a subgroup of S_4.

One can check explicitly that S_4 has precisely 8 elements of order 3, all of which are, in fact, contained in A_4. Thus G meets A_4 at a subgroup of

order ≥ 8 in S_4. Since both A_4 and G have order 12, it follows by Lagrange's theorem that the image of ρ is all of A_4, hence G is isomorphic to A_4.

8.12 Groups of order $p^2 \cdot q$

Let p and q be distinct primes, and let G be a group of order $p^2 \cdot q$. We show that G has a normal Sylow subgroup (for either p or q).

Suppose first that $p > q$. Since $n_p | q$ and $n_p \equiv 1\ (p)$, we have $n_p = 1$ (why?) so that aa Sylow p-subgroup would be normal in G.

Now suppose that $p < q$. If $n_q = 1$, then we are done, as a Sylow q subgroup would be normal. Assume that $n_q > 1$. Since $n_q \equiv 1\ (q)$, $n_q | p^2$, and $p < q$, we cannot have $n_q = p$, so that $n_q = p^2$. Thus, writing $n_q = 1 + k \cdot q = p^2$, we have

$$k \cdot q = (p-1) \cdot (p+1).$$

In other words, q divides $(p-1) \cdot (p+1)$, and since q is prime, it must divide either $p-1$ or $p+1$. Taking into account that $p < q$, we see that the only possibility is $p = 2$ and $q = 3$ (why?), in which case G has order 12, so that we may apply the previous example.

8.13 Groups of order 60

Theorem 8.14. *Suppose that G has order 60 and that $n_5(G) > 1$. Then G is simple.*

Proof. Suppose not, and let H be a nontrivial proper normal subgroup of G. By the Sylow theorems, we must have $n_5 = 6$ (why?). Let P be a Sylow 5-subgroup of G, hence $[G : N_G(P)] = 10$ (why?).

Suppose first that 5 divides $\#H$. then H contains a Sylow 5-subgroup of G, and since H is normal, it must contain all Sylow 5-subgroups of G. Indeed, if Q is any Sylow 5-subgroup of G contained in H, and $g \in G$ then

$$g \cdot Q \cdot g^{-1} \leq g \cdot H \cdot g^{-1} = H$$

while all Sylow 5-subgroups are conjugates. Counting the number of elements of order dividing 5 in H shows that $\#H$ is at least $1 + 6 \cdot 4 = 25$. Lagrange's theorem then implies that $\#H = 30$. Arguing as in the previous example would show that H has a unique Sylow 5-subgroup, which would then imply by the above logic that G has a unique Sylow 5-subgroup (as any Sylow 5 subgroup of G is a Sylow 5 subgroup of H). Thus, it follows that 5 does not divide $\#H$.

If $\#H = 6$ or 12, then H has a normal, hence characteristic, Sylow subgroup, by the examples above. Such a Sylow subgroup would be normal in G, since H is normal (why?). Replacing H by such a subgroup if necessary, we reduce to the case where $\#H$ is 2, 3 or 4 (why?).

Consider G/H, which then has size 30, 20 or 15. In each of these cases, G/H has a normal subgroup of order 5 by previous examples. If N is the preimage of such a normal subgroup in G, it follows that N is a proper normal subgroup of G whose order is divisible by 5, which contradicts the argument from the first paragrpah.

In any case, we have reached a contradiction, so the assertion of the theorem is verified. □

Corollary 8.15. *A_5 is simple.*

Proof. The two subgroups $\langle(12345)\rangle$ and $\langle(13245)\rangle$ are distinct Sylow 5-subgroups of A_5, while A_5 has order 60. □