Group Theory

Zac Zerafa

April 17, 2026

Contents

Part I

Fundamentals

Chapter 1

Groups and Subgroups

Readers will be familiar with elementary algebra; solving for x by leveraging the laws of operations. Algebra is a useful tool, and it proves powerful when generalized to other objects in mathematics. To generalize the idea of one operation working on a set, we introduce the notion of a *group*.

Our success with these methods has lead us to generalize arithmetic and elementary algebra to *abstract algebra*; the study of algebraic structures. To do this, we consider algebraic structures to be sets with *operations* working on them; functions working on the set that spit out another element of the set (multiplication and addition are operations on $\mathbb{Z}$). These operations may also be bound by certain algebraic equations that define its behaviour.

$xy = yx$ (Commutativity) $x(yz) = (xy)z$ (Associativity) $1x = x$ (Identity element) $xx^{-1} = 1$ (Inverse elements)

See 'Universal Algebra' for more details on operations; this theory is vital for developing group theory.

1.1 Groups

The simplest algebraic structure one can consider is a set with a single operation. There are many classes of such algebraic structures bound by different algebraic equations (loop, magma, monoid, category, etc.), however one structure stands out due to its frequent occurence and body of rich theorems; the *group*.

Definition 1.1 (Group)**.** A *group* is an ordered pair $(G, \circ)$ of a set G and a binary operation $\circ : G \times G \to G$ with the following properties:

- $x \circ (y \circ z) = (x \circ y) \circ z$ ($\circ$ is associative)
- $\exists 1_G \in G[\forall g \in G[g \circ 1_G = 1_G \circ g = g]]$ (G contains an identity element with respect to $\circ$)
- $\forall g \in G[\exists g^{-1} \in G[g \circ g^{-1} = g^{-1} \circ g = 1_G]]$ (Every element of G is invertible with respect to $\circ$)

We often write $g \circ h$ as gh, and call $\circ$ by the name G-composition. When the operation is apparent, a group $(G, \circ)$ may be denoted as G.

Many algebraic strucutres of one operation encountered in mathematics and the sciences can be represented as groups, and the study of groups as an abstraction can lead to some deep propositions with profound consequences. Indeed, more complex algebraic structures often extend upon the notion of a group.

Though all groups find common ground in the three properties above, they may exhibit various behaviours due to extra properties regarding the group's set and operation. One fundamental property that may differ among groups is their *order*.

Definition 1.2 (Order of a group)**.** The *order* of a group is the cardinality of its set. The order of G is denoted as $|G|$ or $\text{ord}(G)$.

Definition 1.3 (Finite group)**.** A *finite group* is a group with a finite order.

Note that when the group operation is clear, we will use the notation g^n for the operation working on g, n times. Note that we can prove the following.

Definition 1.4 (Exponential notation for group operation)**.**

$$g^0 = 1_G$$

$$g^n = g^{n-1}g$$

This notation follows all the familiar relations from arithmetic.

Proposition 1.1.

$$g^n g^m = g^{n+m}$$

$$(g^n)^m = g^{nm}$$

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

1.1.1 Properties of Groups

Groups require the notion of identity elements and inverse elements. With some more work, we can see some elementary properties of these elements, namely their uniqueness.

Proposition 1.2. Let G be a group:

- G contains a unique identity element
- Every element of G is invertible by a unique inverse element

$$\exists! 1_G \in G[\forall g \in G(g1_G = 1_G g = g)]$$

$$\forall g \in G[\exists! g^{-1}(gg^{-1} = g^{-1}g = 1_G)]$$

Proposition 1.3.

$$G \text{ is a group} \wedge g, g_1, g_2 \in G \implies (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$$

The cancellation law is also permitted by groups due to the ability of composing both sides of an equation by inverse elements.

Proposition 1.4 (Cancellation law for Groups)**.** Let G be a group and $g, h_1, h_2 \in G$, then $gh_1 = gh_2$ iff $h_1 = h_2$

$$G \text{ is a group} \wedge g, h_1, h_2 \in G \implies gh_1 = gh_2 \iff h_1 = h_2$$

Here is a curious fact about groups that will frequently be required of us. The cancellation law implies the following proposition, that will be immensely important throughout our study of group theory.

Proposition 1.5. The function $f : G \to G$ defined as $f(h) = gh$ is a bijection.

This essentially means that (left) composition by g permutes group elements around.

1.1.2 Abelian groups

Another fundamental property that some particularly 'nice' groups have is commutativity of it's operation, that is to say, the order of elements under an operation does not affect the result (like how $9 + 10 = 10 + 9$).

Definition 1.5 (Abelian group)**.** An *Abelian group* is a group $(G, \circ)$ such that $\forall g, h \in G[gh = hg]$ ($\circ$ is commutative).

$$(G, \circ) \text{ is Abelian} \iff (G, \circ) \text{ is a group} \wedge \circ \text{ is commutative on } G$$

Even though some groups may not be Abelian, they could have a collection of elements that act commutatively with every other element; this is called the *center*.

Definition 1.6 (Center of a group)**.** The *center* of a group G is a set $Z(G)$ containing the elements that commute with every other element.

$$Z(G) = \{z \in G : \forall g \in G(zg = gz)\}$$

1.1.3 Cayley table and group presentations

Recall how on the back of primary school books, one can find addition and multiplication tables to help students memorize them (or more likely, to cheat on tests).

We can use a generalization of this table to describe the behaviour of a finite group's operation. A *Cayley table* is a table showing the result of applying every combination of two elements with the group operation. It is formally represented as a square matrix $\mathbb{C}$, since finite groups have $|G|^2$ possible combination of elements into the group operation

$$\mathbf{C}_{ij} = g_j g_i$$

Though Cayley tables describe finite groups by explicitly describing the results of the operator, perhaps one wants to define a group by some predicate (condition that the group elements should follow). This is permitted by *group presentations*; they specify a set of elements and rules for generating the group.

$$G = \langle S : R \rangle$$

- S is the set of elements generating the group
- R is the relation that the group must follow

1.1.4 Examples of Groups

In kindergarten we learn that 1+1=2 and that we can add any integers together to get a new integer. I guess kindergarten students aren't aware of the negative numbers though; they are needed in order to ensure inverse elements exist with respect to addition. When little Johnny passes year 1 and learns this fact, he has the *additive group of integers* at his command.

Example 1.1. The *additive group of integers* $(\mathbb{Z}, +)$ Group of integers under addition.

Example 1.2. The *dihedral group* $\mathrm{Dih}(n)$ Group of symmetries a n-gon has when rotating and flipping.

We're literally doing toddler level math right now, but don't feel disheartened if your kid doesn't know the term 'dihedral group' by year 2; this is quite an abstract generalization.

Example 1.3. The *Klein fourgroup* K_4 Group of 4 elements such that each element is its own inverse. $K_4 = \langle a, b \in a^2 = b^2 = (ab)^2 = 1_{K_4} \rangle$

Example 1.4. The *general linear group* $\mathrm{GL}(n, \mathbb{R})$ Group of $n \times n$ matrixes under matrix multiplication.

If you have taken a course in linear algebra you would be taught that the order of multiplying matrixes matters; it could change the result, hence these groups are non-Abelian. We're also taught that not all square matrix have an inverse matrix, therefore such matrixes aren't in this group.

1.2 Subgroups

Sometimes groups consist of smaller groups within themselves, that is, not all the elements of the group are required to form a group.

Definition 1.7 (Subgroup of a group)**.** A *subgroup of* $(G, \circ)$ is a group $(H, \circ)$ such that H is a subset of G and $\circ$ is closed over H. We use the notation $H \leq G$ to denote that H is a subgroup of G.

$$H \leq G \iff (H \subseteq G) \wedge (H, \circ) \text{ is a group}$$

The idea is that it is a subset of the group where G-composition is closed on H, meaning that H preserves its status as a group with $\circ$.

Theorem 1.1. Let $(G, \circ)$ be a group:

- $(G, \circ)$ is a subgroup of itself $G \leq G$
- $(\{1_G\}, \circ)$ is a subgroup of $(G, \circ)$ (i.e the trivial group is a subgroup of every group) $\{1_G\} \leq G$

These subgroups are rather trivial, let's explore some more ways of naturally finding subgroups on some general group.

Proposition 1.6.

$$Z(G) \leq G$$
$$Z(G) \text{ is Abelian}$$

Proposition 1.7. Let H, K be subgroups of G, then $H \cap K \leq G$

Here's another idea for constructing subgroups; imagine we want the element $x \in G$ to end up in our subgroup, we can generate a group from this element by consider the $\circ$-exponentials of x. Taking exponentials is our way of "closing the group up" so that this set meets the requirements of being a group, and we should check that this construction indeed satisfies the criteria to be a group. One may see that this will give us the smallest such subgroup in which x is included.

Definition 1.8 (Subgroup generated by x)**.** The *subgroup generated by* $x \in G$ is the following.

$$\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$$

.

As we will see in a later chapter, groups that can be 'generated' from a single element are called *cyclic groups*, hence subgroups generated by a single element are sometimes called *cyclic subgroups*. When we study cyclic groups in a later chapter, we will see they are of grand importance in understanding group theory in general.

Let's find a way to generate the smallest subgroup containing some arbitrary subset X, rather than just an element. SInce we know that taking interesections preserves the criterion for a group, we can take the intersection of all subgroups containing X. In the end, we obtain the smallest subgroup containing X.

Definition 1.9 (Subgroup generated by X)**.** The *subgroup generated by* $X \subseteq G$ is the following subgroup, generated by taking the intersection of all subgroups containing X.

$$\Lambda = \{H \leq G : X \subseteq H\}$$

$$\langle X \rangle = \bigcap_{H \in \Lambda} H$$

1.2.1 Examples of Subgroups

Example 1.5.

$$k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}$$

Example 1.6. The *additive group of n-multiples* $(n\mathbb{Z}, +)$ Subgroup of $(\mathbb{Z}, +)$ of multiples of n.

Example 1.7. The *special linear group* $\mathrm{SL}(n, \mathbb{R})$ Subgroup of $\mathrm{GL}(n)$ of matrixes with determinant 1.

Example 1.8. The *orthogonal group* $\mathrm{O}(n, \mathbb{R})$ Subgroup of $\mathrm{GL}(n)$ of orthogonal matrixes

Example 1.9. The *special orthogonal group* $\mathrm{SO}(n, \mathbb{R})$ Subgroup of $\mathrm{O}(n)$ of matrixes with determinant 1

- It is Abelian for $n \leq 2$

1.2.2 Properties of Subgroups

Proposition 1.8. Let H be a subgroup of G, then 1_G is in the subgroup H.

$$H \leq G \implies 1_G \in H$$

1.3 Cosets

There is an interesting property relating to how the orders of groups relate to the orders of their subgroups. Bringing this fact to light requires experimenting how subgroup elements behave with foreign elements in its 'supergroup'; this will be done by the use of *cosets*.

Definition 1.10 (Left coset)**.** Given the subgroup $(H, \circ)$ of $(G, \circ)$, a *left coset* of $(H, \circ)$ is a set gH containing the elements of the form gh, where $h \in H$.

$$gH = \{gh : h \in H\}$$

¡/p¿ The set G/H is the set of all unique left cosets of H on G.

Definition 1.11 (Right coset)**.** If $(H, \circ)$ is a subgroup of $(G, \circ)$, a *right coset* of $(H, \circ)$ is a set Hg containing the elements of the form hg, where $h \in H$.

$$Hg = \{hg : h \in H\}$$

The set $G\ H$ is the set of all unique right cosets of H on G.

1.3.1 Properties of Cosets

Among the more basic properties that cosets have are consequences of the basic properties of groups. The following propositions will explicitly deal with left cosets for brevity, however right cosets have similar properties.

Proposition 1.9. The cardinality of left cosets of $(H, \circ)$ is the order of $(H, \circ)$

$$|gH| = |Hg| = |H|$$

This follows immediately from the fact that $f(h) = gh$ is a bijection. Heres another result that isn't too surprising.

Proposition 1.10.

$$H \leq G \wedge H \text{ is an Abelian group } \implies Hg = gH$$

Lemma 1.1. Let $H \leq G$, then there are the same amount of left cosets on H as right cosets. Therefore we can use the notation $[G : H]$ to represent the cardinality of either the right or left cosets.

$$H \leq G$$

$$|G/H| = |G\ H| = [G : H]$$

Lemma 1.2.

$$H \leq G \wedge h \in H \implies hH = H$$

We can generalize this result even further.

Lemma 1.3.

$$H \leq G$$
$$k \in gH \implies gH = kH$$

Proposition 1.11.

$$H \leq G \wedge H \text{ is an Abelian group} \implies Hg = gH$$

1.3.2 Examples of cosets

Consider the cosets of the group $4\mathbb{Z} \leq \mathbb{Z}$

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

$$2 + 4\mathbb{Z}$$
$$(2 + 3) + 4\mathbb{Z}$$
$$(6 + 3) + 4\mathbb{Z}$$
$$(10 + 3) + 4\mathbb{Z}$$
$$(14 + 3) + 4\mathbb{Z}$$

It's almost like the cosets have an algebra of their own (foreshadowing).

Here's an important note of caution; recall our notation $k\mathbb{Z}$. Unfortunately, $(\mathbb{Z}, \circ)$ where $\circ$ is multiplication of integers doesn't even form a group, but we accept this 'abuse of notation' to write the subgroups of $(\mathbb{Z}, +)$ more easily. This is the only example where we take a left coset of something that isn't a group, and though we cannot treat it like a left coset, we can still use its notation for subgroups of $(\mathbb{Z}, +)$.

1.3.3 Lagrange's theorem

We've now got some intuition for cosets, but we've left the best property for last; cosets form a partition on a group. Cosets can be used to describe a very interesting property about finite subgroups. We will construct a repertoire of lemmas to propound a notorious theorem in group theory.

Lemma 1.4. Left cosets are either equal or disjoint.

Lemma 1.5. Left cosets are equivalence classes on G.

Theorem 1.2 (Lagrange's theorem (group theory))**.** Let H be a subgroup of G, then the order of H divides the order of G by the amount of distinct left cosets.

$$H \leq G \implies |G| = [G : H]|H|$$

Proposition 1.12 (Euler's theorem for groups)**.** Let G be a group, then the following holds.

$$g^{|G|} = 1_G$$

1.4 Conjugacy

Before finishing the chapter, it is worth going over the idea of *conjugacy*; it will occur spontaneously in many problems, and a formal theory on it will be most beneficial.

1.4.1 Commutator

We now introduce a useful operation generally across group theory.

Definition 1.12 (Group commutator)**.**

$$[x, y] = x^{-1}y^{-1}xy$$

Why have such an operation? It was probably conceived because it can be used as a statistic that flags when elements can commute.

Proposition 1.13.

$$xy = yx \iff [x, y] = 1_G$$

Therefore in Abelian groups the commutator is always the identity, however it appears in many identities to do with conjugation.

Chapter 2

Group homomorphisms

2.1 Group homomorphism

A powerful tool in abstract algebra is the idea of a *homomorphism*. Sometimes different groups can have similar behaviours, and homomorphisms are the primary technique by which this is expressed.

Definition 2.1 (Group homomorphism)**.** Let $(G, \circ)$ and $(H, *)$ be two groups. A *group homomorphism* $f : G \to H$ is a function between groups that 'preserves' the group's operation in the following sense; if g_1, g_2 are elements of G, we have the following.

$$f(g_1 \circ g_2) = f(g_1) * f(g_2)$$

Homomorphisms have some elementary properties relating to mappings of identity and inverse elements.

Proposition 2.1.

$$f(1_G) = 1_H$$

Proposition 2.2.

$$f(g)^{-1} = f(g^{-1})$$

Definition 2.2 (Group monomorphism)**.** injective homomorphism

Definition 2.3 (Group epimorphism)**.** surjective homomorphism

Definition 2.4 (Group endomorphism)**.**

I've listed terminology for injective and surjective homomorphisms, however I will defer 'bijective homomorphisms' for their own section since they are so special.

2.1.1 Examples of Group homomorphism

Example 2.1 (The determinant)**.**

$$\det : \mathrm{GL}(n, \mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \times)$$

We know from linear algebra that $\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B})$ and that $\det(\mathbf{I}) = 1$; these are the exact conditions of a homomorphism.

Example 2.2 (Permutation signature)**.**

When we learn about special group constructions (quotient groups, product groups, etc.) we will rely heavily on the notions of homomorphisms to describe the behaviour of the constructions we create. When we have these tools available to us, we can in turn find more interesting homomorphisms lurking between related constructs.

These types of group homorphisms have particularly interesting properties, but group isomorphisms are perhaps the most important class of homomorphisms.

2.2 Group isomorphism

One of the most notable types of homomorphism is the *isomorphism*. This mapping expresses groups that have *exactly* the same behavior. To express this, we want our homomorphism to be bijective, since this means that every element in the domain group has a direct counterpart in the codomain group and vice versa.

Definition 2.5 (Group isomorphism)**.** Let $(G, \circ)$ and $(H, *)$ be two groups. A *group isomorphism* $f : G \to H$ is a bijective isomorphism. If there exists an isomorphism between G and H, then the groups are *isomorphic* to eachother, also written as $(G, \circ) \cong (H, *)$ or if the group operations are known, $G \cong H$.

G is isomorphic to $H \iff \exists f : G \to H[f \text{ is a homomorphism} \wedge f \text{ is bijective}]$

$$G \cong H \iff G \text{ is isomorphic to } H$$

When groups are isomorphic, mathematicians tend to view them as the same group 'up to a change of symbols'; isomorphic groups have the exact same behaviour as a group, and the isomorphism is used to translate which

symbol in the domain group acts identically to which symbol in the codomain group. They'll often say such groups are equal *up to an isomorphism*.

It's important to note that although as groups isomorphic groups behave identically, when considering external spaces and structures the groups may exhibit different behaviour; the isomorphic relation is not equality.

Definition 2.6 (Group automorphism)**.** Let $(G, \circ)$ be a group. A *group automorphism* $f : G \to G$ is an isomorphism onto the same group.

Proposition 2.3. For any group $(G, \circ)$ there exists a class of automorphisms called the *inner automorphisms* defined as $\varphi_g(x) = gxg^{-1}$.

2.2.1 Properties of Group isomorphism

According to the way I have described the desired properties of the isomorphism, we would hope that the isomorphism relation is an equivalence relation, which indeed it is.

Proposition 2.4. The group isomorphism relation $\cong$ is an equivalence relation.

2.2.2 Kernel of a group homomorphism

A *Canonical map* is a function between two objects that arises from their definitions. It is a function used to define the behaviour of some object.

From set theory we are familiar that functions give rise to the ideas of domains, codomains, images, preimages, fibers etc. however when considering group homomorphisms we can now define the idea of a *kernel*; the set of all elements in a homomorphism mapped to the identity.

Definition 2.7 (Kernel (group homomorphism))**.** Let $(G, \circ)$ and $(H, *)$ be two groups and $f : G \to H$ a homorphism. The *kernel of a group homomorphism* is the set of elements that a homomorphism maps to the other group's identity element.

$$\ker(f) = \{g \in G : f(g) = 1_H\}$$

Proposition 2.5.

$$f : G \to H \text{ is a group homomorphism} \implies \ker(f) \leq G$$

Proposition 2.6.

$$f : G \to H \text{ is a group isomorphism} \implies \ker(f) = \{1_G\}$$

2.2.3 Examples of isomorphisms

Example 2.3 (The exponential function)**.**

$$\exp : (\mathbb{R}, +) \to (\mathbb{R}_+, \times)$$

$$\exp(x) = e^x$$

The fact that for exponentials, addition in the exponent is multiplication of factors, is really a homomorphism between addition over the reals to multiplication over positive reals (since exponentials are always greater than 0 with real exponents). This function is particularly interesting since it is also a bijection; bijective homomorphisms are called *isomorphisms*, and we will have much to say about them.

Groups can be used to prove a key insight in about metric spaces; isometries are simply reflections and rotations. In terms of isomorphisms, this is saying that the group of isometries on a space X is isomorphic to the group $\mathrm{O}(n, X)$.

Chapter 3

Quotient Groups

Now that some familiarity with the basic theory of groups is established, we can now turn towards some common groups constructions; ways in which different groups can be related to one another to form new groups.

3.1 Normal subgroups

Recall that left cosets of a subgroup form an equivalence relation over a group, essentially *dividing* the group into a bunch of sets that partition the group. Imagine we want to synthetically form group that acts just like G, except all elements of the same left coset are treated as the same element; can we always make such a group? The right approach is to treat the left cosets as the elements of this group themselves. Now the question becomes this; can we make a group of these equivalences classes, where composition $*$ acts as such?

$$xH * yH = (xy)H$$

Let's define a function from G to G/H that shows

Definition 3.1 (Quotient map)**.** The *Quotient map* π is the following function.

$$\pi : G/H \to G$$

$$\pi(x) = xH$$

Using the definition of our quotient map, we can restate the condition we want to the following.

$$xH * yH = (xy)H \implies f(x)f(y) = f(xy)$$

But this is the condition of a homomorphism! So if our quotient map is an epimorphism (since we want our group to contain all left cosets), then such a group can be created. One can immediately see that the quotient map is surjective, so it remains to see that the homomorphism condition is satisfied.

Unfortunately the quotient map isn't always a homomorphism. To see why, imagine we have $aH = bH$ (i.e a, b are in the same left coset), if the quotient map was a homomorphism then we have $(ag)H = (bg)H$, since a, b should 'act' the same, but this is not true in general.

For what subgroups is this true? For such subgroups, the quotient map would be a homomorpism and our constructed group would be valid. The answer lies in *normal subgroups*.

Definition 3.2 (Normal subgroup)**.** A *normal subgroup*

$$N \lhd G \iff \forall g \in G[gNg^{-1} = N]$$

Assume N is a normal subgroup and we have $aN = bN$, let's show that $(ag)H = (bg)H$

$$agh_1 = ah_2g = bh_3g = bgh_4$$

$$\implies (ag)H = (bg)H$$

If we begin with the assumption that $aH = bH \implies agH = bgH$, we can prove that the group must be a normal subgroup as such.

$$gh_1 = a^-1agh_1 = a^-1bgh_2 = h_3gh_2$$

$$gh_1 = h_3gh_2$$

$$g(h_1h_2^{-1}) = h_3g$$

As mathematicians, we would like to be familiar with sufficient conditions to form a normal subgroup so that we can involve them when we start studying quotient groups.

Proposition 3.1. If a subgroup is Abelian, then it is normal.

$$N \leq G \wedge N \text{ is Abelian} \implies N \lhd G$$

Corollary 3.1. Centers are normal subgroups.

$$Z(G) \lhd G$$

Proposition 3.2. Kernels are normal subgroups.

$$\ker(f) \lhd G$$

$$f : G \to H \text{ is a homomorphism } \implies \ker(f) \lhd G$$

3.2 Quotient groups

We can now introduce the quotient group; a group of cosets.

Definition 3.3 (Quotient group)**.** Let $(G, \circ)$ be a group and $N \lhd G$ be a normal subgroup, *the quotient group of* G *by* N is the group $(G/N, *)$ of unique left cosets of N with $*$-composition defined in the following way.

- G/N is the set of left cosets of N in G
- $(gN) * (kN) = (gk)N$

We should make sure that $*$-composition is well defined; we didn't introduce normal subgroups for nothing!

For the sake of simplicity, we'll often use the equivalence class notation $[g] = gN$ when the normal subgroup is familiar and omit the $*$-composition symbol. Here's an example below.

$$gN * kN = [g] * [k] = [g][k]$$

When is a quotient group is Abelian? For quotient group G/N, it is when $g^-1h^-1gh \in N$.

$G/Z(G)$ is an abelian subgroup iff it is isomorphic to the trivial group.

And of course, we know the folloing from our previous discussion.

Proposition 3.3. Let G/N be a quotient group, then the quotient map $\pi : G \to G/N$ is an epimorphism.

3.2.1 Examples of quotient groups

Example 3.1. Consider the *additive group of integers modulo n* $(\mathbb{Z}/n\mathbb{Z}, +)$ Recall that $n\mathbb{Z} \leq \mathbb{Z}$ and that $\mathbb{Z}$ and its subgroups are Abelian, hence it is indeed well defined. Since numbers with the same Euclidean remainder when divided by n fall in the same coset, the cosets are $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\}$

Example 3.2. The *circle group* $(\mathbb{T}, \circ)$, where $\mathbb{T} = \{z \in C : |z| = 1\}$ can be represented isomorphically as a quotient group. One can show that $\mathbb{T} \cong \mathbb{R}/2\pi\mathbb{Z}$ by a result called the *first isomorphism thorem.*

3.2.2 First isomorphism theorem

We can create quotient groups given any normal subgroup. Remember that kernels of homomorphisms actually form subgroups themselves; that's pretty neat. However can one make quotient groups with the kernel?

Proposition 3.4. Given a homomorphism $f : G \to H$, its kernel is a normal subgroup of G.

$$\ker(f) \lhd G$$

This means we can make quotient groups using kernels. So the cosets on the kernel form their own group. Experimenting with the cosets of the kernel brings the following lemma.

Lemma 3.1.

$$\varphi : G \to H \text{ is a homomorphism } \implies [g_1\ker(\varphi) = g_2\ker(\varphi) \iff \varphi(g_1) = \varphi(g_2)]$$

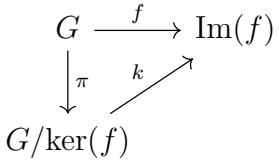
One way of interpreting this lemma is that kernel cosets correspond to sets of elements with the same homomorphism mappings. In other words, elements in the same left coset of the kernel map to the same H. To eliminate this redundancy, one can consider a map from the quotient group which bundles these identically treated elements as oe left coset; this gives us a monomorphism from the quotient group to H; This is the essence of the *first isomorphism theorem.*

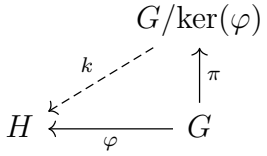
There are a few ways this theorem is traditionally posed. We will derive a general version of the theorem and prove the rest of the theorem as corollaries.

Theorem 3.1 (First isomorphism theorem (group theory))**.** Let $\varphi : G \to H$ be a homomorphism. Then there exists a unique epimorphism $k : G/\ker(\varphi) \to H$ defined as

$$k : g\ker(f) \mapsto f(g)$$

Since k is an epimorphism, we have $\mathrm{Im}(f) \cong G/\ker(f)$





If the image of the original homomorphism φ is the whole of H (i.e φ is surjective, an epimorphism), our epimorphism gets promoted to an isomorphism, and we have the following instantly.

Corollary 3.2.

$$f : G \to H \text{ is an epimorphism } \implies G/\ker(f) \cong H$$

With Lagrange's theorem, we can now obtain an interesting way to view the order of finite groups through the perspective of homomorphims.

Corollary 3.3.

$$f : G \to H \text{ is a homomorphism } \implies |\mathrm{Im}(f)||\mathrm{Ker}(f)| = |G|$$

Chapter 4

Cyclic Groups

Sometimes it is interesting to see how many distinct elements can be formed by repeating the operation on some specific element; we call this the order of the element.

4.1 Cyclic Groups

Definition 4.1 (Cyclic group)**.** A *cyclic group* $(G, \circ)$ is a group such that there exists some element x such that all elements are of the form x^n. We say that such a x *generates* G.

$$G \text{ is cyclic} \iff \exists x \in G[\forall g \in G(\exists n \in \mathbb{Z}[x^n = g])]$$

Such an x is called a *generator of* G

If the group operation is clear, one may write the set of elements generated by the element x as $\langle x \rangle$.

$$\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$$

.

One may see that this is indeed forms its own group, and furthermore, a cyclic one.

Proposition 4.1.

$$(G, \circ) \wedge x \in G$$
$$(\langle x \rangle, \circ) \leq (G, \circ)$$
$$(\langle x \rangle, \circ) \text{ is cyclic}$$

This is how we construct cyclic subgroups, and this gives us a reason to think of 'orders of elements' as 'orders of the cyclic subgroup they generate'.

Definition 4.2 (Order of a group element)**.** The *order* of a group element g is the cardinality of $\langle g \rangle$. The order of g is denoted as $\text{ord}(g)$.

$$\text{ord}(g) = |\langle g \rangle|$$

4.2 Isomorphisms of Cyclic Groups

Finite cyclic groups of the same order are all isomorphic by the isomorphism $f(\gamma^n) = \eta^n$, where $G = \langle \gamma \rangle, H = \langle \eta \rangle$, hence we define a notation to represent the unique cyclic group of order n (unique up to an isomorphism).

Example 4.1. The *cyclic group of order* n $\text{Cyc}(n)$ Cyclic group of n elements. $\text{Cyc}(n) = \langle x : x^n = 1 \rangle$

When proving theorems on cyclic groups, we often find ourselves working in the exponent of the same element, and the exponent acts like modular arithmetic; the law $g^a \circ g^b = g^{a+b}$ looks and feels very much like an isomorphism to $\mathbb{Z}/n\mathbb{Z}$ (where n is the order of g). This suspicion is correct, and leads us to one of the most powerful methods of thinking of cyclic groups; treating them like modular arithmetic.

Proposition 4.2. $f : \text{Cyc}(n) \to \mathbb{Z}/n\mathbb{Z}$ $f(x^n) = [n]$

$$\text{Cyc}(n) \cong \mathbb{Z}/n\mathbb{Z}$$

4.3 Properties of Cyclic Groups

Proposition 4.3. Groups of prime order are cyclic.

$$|G| \text{ is prime} \implies G \cong \text{Cyc}(|G|)$$

Lagrange's theorem implies that groups of prime order only have themselves and the trivial group as subgroups, hence each element is a generator of the group, hence it is cyclic.

The isomorphic equivalence $\text{Cyc}(n) \cong \mathbb{Z}/n\mathbb{Z}$ really means that cylic groups are actually all about additive integer groups modulo n. This permits

us to invoke techniques from number theory to fully realize the properties of cyclic groups.

The following lemma helps us understand more about the cyclic nature of $\mathbb{Z}/n\mathbb{Z}$

Proposition 4.4. Let $a \in \mathbb{Z}/n\mathbb{Z}$, then $\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$ iff a is coprime to n.

Corollary 4.1. There are $\varphi(n)$ generators of $\mathrm{Cyc}(n)$.

Here is a more constructuve result which calculates the order of any element of $\mathbb{Z}/n\mathbb{Z}$.

Corollary 4.2. Let $x \in \mathbb{Z}/n\mathbb{Z}$, then the order of x is $\frac{\mathrm{lcm}(x,n)}{x}$, or equivalently, $\frac{n}{\gcd(x,n)}$.

Corollary 4.3. $a \in \mathbb{Z}/n\mathbb{Z}$ is a generator of the group iff $\gcd(a, n) = 1$.

Now to prove some propositions on the subgroups of cyclic groups.

Proposition 4.5. Subgroups of cyclic groups are cyclic.

The following proposition is proved by switching from $\mathrm{Cyc}(n)$ to $\mathbb{Z}/n\mathbb{Z}$ showing that all elements in subgroups of $\mathbb{Z}/n\mathbb{Z}$ must be multiples (repeated operation) of the smallest nonzero number in that subgroup (if such a smallest nonzero number is in the group, which is true for all but the trivial group). This is a good example of leveraging the properties of integers, bringing their nice properties to facilitate proofs.

Theorem 4.1 (Fundamental theorem of cyclic groups)**.** If d divides the order of a cyclic group, then there is a unique cyclic subgroup of order d.

$$d|n \implies \exists! H \leq \mathrm{Cyc}(n)[|H| = d]$$

Again leveraging number theory, existence follows by noting that $\frac{|G|}{/}d$ generates a group isomorphic to $\mathbb{Z}/d\mathbb{Z}$ (which is cyclic). Then the proof is finished by showing that any other generator of order d is a multiple of our $\frac{n}{d}$.

Just as modular groups can be used to prove stuff about cyclic groups, the theory of cyclic groups can conversely prove propositions in number theory.

Proposition 4.6.

$$n = \sum_{d|n} \varphi(d)$$

Chapter 5

Product Groups

5.1 Direct Product Groups

There are several group constructions that are called 'product groups', however the simplest is perhaps the *direct prodcut group*; a group formed by taking the cartesian product of two groups (hence creating ordered pairs) with the new operation applying both group's operations component wise.

Definition 5.1 (Direct product of 2 groups)**.** Let $(G, \circ_G)$ and $(H, \circ_H)$ be groups, the *direct product of G and H* is a group $(G \times H, \circ)$ where $G \times H$ and $\circ : G \times H \to G \times H$ are defined as such.

- $G \times H$ is the cartesian product of the group sets
- $(g_1, h_1) \circ (g_2, h_2) = (g_1 \circ_G g_2, h_1 \circ_H h_2)$

This construction is indeed always a group; it can be checked rather quickly. It's really the simplest way to slap groups together; there isn't even a condition for H, G to be related to eachother in any way!

Proposition 5.1.

- $(1_G, 1_H)$ is the identity element
- $(g, h)^{-1} = (g^{-1}, h^{-1})$
- $G \cong G \times \{1_H\}$ and $H \cong \{1_G\} \times H$)

Proposition 5.2 (Chinese remainder theorem (group theory))**.** Let $(n_i)_{i=1}^k \in \mathbb{Z}$ be coprime integers and $N = \prod_{i=1}^k n_i$. Then $\mathbb{Z}/N\mathbb{Z} \cong \times_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$.

5.2 Product of group subsets

Factoring a group into a direct product representation is a colorful process; .

Since factoring groups into direct product representations is quite an unruly process, let's consider just the case of factoring groups into subgroups. There is a theorem that states exactly when this can be done, however it requires delving into the idea of *products of subgroups*.

For completeness, we first introduce the less powerful *product of group subsets*; a precursor to product of subgroups.

Definition 5.2 (Product of group subsets)**.** A *product of group subsets* is the set closed by composing elements of two subsets together.

$$S, T \subseteq G \implies ST = \{st : s \in S \land t \in T\}$$

There are a few important points to note about the definition we've just created. Firstly, S and T are subsets of G and not necessarily subgroups of G. Secondly, we can interpret ST as the composition closure of elements of S and T from the left and right respectively.

When checking to see if inverses exist, the identity exists, and composition is well defined, we can see that this doesn't necessarily yield a group.

5.2.1 Product of subgroups

Since S and T aren't subgroups, we're restricted from invoking many properties of groups; all we really know is that $s \circ t$ is well defined, but that's about it. This construction is a group merely when it is closed under inversion, contains the identity, and composition is well defined. To make our studies less insipid, let's look at the case when forming *product of subgroups*.

Definition 5.3 (Product of subgroups)**.** A *product of subgroups* is the set closed by composing elements of two subgroups together.

$$H, K \leq G \implies HK = \{hk : h \in H \land k \in K\}$$

Unfortunately products of subgroups aren't necessarily subgroups either, but the following proposition tells us exactly when they are groups.

Proposition 5.3. Let G be a group with subgroups $H, K \leq G$ Then $HK \leq$ iff $HK = KH$

$$HK \leq G \iff HK = KH$$

Furthermore, if $HK \leq G$ then $\langle H \cup K \rangle = HK$.

If HK is a group, then for any $hk \in HK$ we also have $(hk)^{-1} = k^{-}-1h^{-1} \in HK$, however $k^{-1}h^{-1} \in KH$. Since the inverse map $f(hk) = k^{-1}h^{-1}$ is a bijection from HK to KH, we see that a necessary condition is that $HK = KH$.

To prove that $HK = KH$ is also a sufficient condition is left as an exercise for the reader; it's not too difficult (plus I can't be fucked explaining).

Proposition 5.4 (Dedekind's modular law)**.** Let G be a group with subgroups $H, K, L \leq G$ and $K \subseteq L$.

$$(HK) \cap L = (H \cap L)K$$

5.2.2 Second isomorphism theorem

Second isomorphism theorem is a pleothora of results pertaining to products of subgroups where one of the subgroups is normal.

Consider HN, by corollary of our previous proposition, $HN \leq G$.

$N \lhd NH$ since $N \subseteq NH$ and $N \lhd G$. Consider the 'reduced' quotient map $\pi : H \to G/N$ one sees that $\ker(\pi) = H \cap N$ and hence $H \cap N \lhd H$ (since the kernek is a normal subgroup of the domain group).

The fact that $HN/N \cong H/(H \cap N)$ follows by applying the first isomorphism theorem to our π, noting that $\mathrm{Im}(\pi) = HN/N$

Proposition 5.5 (Second isomorphism theorem)**.** Let $H \leq G$, $N \lhd G$, then the following hold.

$$HN \leq G$$

$$N \lhd HN$$

$$H \cap N \lhd H$$

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

5.2.3 Third isomorphism theorem

When considering product of normal subgroups, even more can be proven

Proposition 5.6 (Third isomorphism theorem)**.** Let $N, M \lhd G$, then the following hold.

$$M/N \lhd G/N$$

$$(G/N)/(M/N) \cong G/M$$

5.2.4 Product of subgroups and direct product

An interesting question to ask is when our product of subgroups is isomorphic to the direct product of those subgroups. The following proposition reveals all.

Proposition 5.7. Let G be a group and $N, M \lhd G$ normal subgroups with $N \cap M = \{1_G\}$. Then we have $N \times M \cong NM$

$$N, M \lhd G \wedge N \cap M = \{1_G\} \implies NM \leq G \wedge M \times N \cong MN$$

Why does this hold? By the second isomorphism theorem we definitely have $NM \leq G$ (since it would be enough to have only one normal subgroup). We then consider the function $f(n, m) = nm$, for which we want to prove to be an isomorphism. While proving that $f(n_1n_2, m_1m_2) = f(n_1, m_1)f(n_2, m_2)$, we end up with $f(n_1n_2, m_1m_2) = n_1n_2m_1m_2$; we must commute those middle terms to prove the result (i.e we need $n_2m_1 = m_1n_2$, or equivalently $n_2m_1n_2^{-1}m_1^{-1} = 1_G$).

Since N and M are both normal, we see that $n_2m_1n_2^{-1}m_1^{-1}$ is in both N and M since we can consider $n_2m_1n_2^{-1} = m_*$ and $m_1n_2^{-1}m_1^{-1} = n_*$. But because $N \cap M = \{1_G\}$, this must be the identity (or equivalently, the elements commute). $f(1_N, 1_M) = 1_N1_M$ is trivial, so f is a homomorphism.

To check for bijectivity, we note that surjectivity is trivial and start checking injectivity. The trivial intersection ensures that elements of NM have a unique representation of the form nm, since if $n_1m_1 = n_2m_2$, we then have $n_2^{-1}n_1 = m_2m_1^{-1}$, so $n_2^{-1}n_1 \in N \cap M$ and therefore the trivial intersection implies that $n_2^{-1}n_1 = 1_G$ and $n_2 = n_1$. A similar argument shows that $m_2 = m_1$.

If our product of normal subgroups equals the group, then it turns out that we've found a direct product representation for the group from its own normal subgroups!

Corollary 5.1.

$$N, M \lhd G \wedge N \cap M = \{1_G\} \wedge NM = G \implies N \times M \cong G$$

It is worth noting that this is only a sufficient condition and is not the only condition by which a group can be factored as a direct product; finding direct product group representation can be quite a difficult problem. Recall that we also have CRT from earler, which works with completely different

conditions and on an narrower class of groups (cyclic ones with composite order).

That said, our little theorem here is a good connection between the notion of a product of subgroups and a direct product.

5.3 Inner semidirect product group

Definition 5.4 (Inner semidirect product)**.** Let $N \lhd G$, $H \leq G$, and $N \cap H = \{1_G\}$, then the inner semidirect product $N \rtimes H$ is defined as such.

$$N \rtimes H = NH$$

The innder semidirect product is a generalization of the pro

Proposition 5.8.

$$H \leq G \land N \lhd G \land HN \cong G \iff H \cap N = \{1_G\} \land HN = G$$

This proposition gives a sufficient condition for the product of group subsets to form a group; this is known as the inner semidirect product group and is made by 'factoring' the group into a subgroup and normal subgroup as discussed.

Definition 5.5 (Inner semidirect product group)**.**

$$H \leq G$$

$$N \lhd G$$

$$N \rtimes H \iff NH = G \land N \cap H = \{1_G\}$$

Note that $N \rtimes H$ is trivially a group since by definition it equals G (which is a group by default).

There are equivalent ways of defining a semidirect prouct group by restating our definition directly in terms of group elements or by homomorphisms or isomorphisms.

5.4 Outer semidirect product group

Chapter 6

Symmetric Group

In combinatorics an elementary question that students encounter is how to count permutations; how many ways can n distinct objects be ordered? We can represent a certain permutation of elements on a set as a bijective function.

Definition 6.1 (Permutation function)**.** A *permutation function on* X is a bijective function $\sigma : X \to X$. It represents the idea of permuting (swapping around) elements of X.

As with any general function, a permutation is expressible as an equality of the function on its argument to its mappings, for instance, there is an element $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ denoted as such.

$$\sigma(n) = \begin{cases} 3 & n = 1 \\ 1 & n = 2 \\ 2 & n = 3 \end{cases}$$

.

Since permutations are bijective functions, this is perhaps the most mathematically faithful, and it can theoretically represent any permutation (even when considering infinite symmetric groups!). However, this notation grows exponentially inefficient for representing permutations of larger symmetry groups.

The 'two line' notation uses a matrix where the first row indicates the indexes, and the second row indicates mappings

$$\sigma = \begin{bmatrix} 123 \\ 312 \end{bmatrix}$$

This can be more concise than the function notation, however can only really be used for permutations of finite (maybe countable with some adjustments) symmetric groups.

Generalizing this to any $\mathbb{Z}/n\mathbb{Z}$

$$\sigma(m) = \sigma_{m2}$$

This book is about group theory afterall, and indeed, permutatiuon functions form a group! Not only this, but they form extremely powerful and fundamental groups.

Definition 6.2. A *symmetric group* is a group $(\mathrm{Sym}(X), \circ)$.

- $\mathrm{Sym}(X)$ is the set of all permutation functions on X
- $\circ$ is the function composition operation

A subgroup of a symmetric group is called a permutation group Note that composition of this group is literally the composition of functions.

Since we usually don't care about the actual elements of X but rather how many elements there are in X (since these will all be isomorphic to eachother anyways), we usually just consider the elements to be the first n natural numbers.

Definition 6.3. $\mathrm{Sym}(n)$ represents the symmetry group with permutations on $\mathbb{N} \cap [1, n]$.

As alluded to, finite symmetric groups can always (up to an isomorphism) be represented as some $\mathrm{Sym}(n)$.

Proposition 6.1. Symmetric groups on sets of the same cardinality are isomorphic.

$$|X| = |Y| \implies \mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$$

As we know from combinatorics, there are $n!$ permutations of n distinct objects.

Proposition 6.2.

$$|\mathrm{Sym}(n)| = n!$$

- permutation group is a subgroup of a symmetry group

6.1 Cayley's theorem

Aside from combinatorial applications, symmetric groups are useful in the classification of groups; representing groups in terms of more basic groups. A simple example of this being Cayley's theorem.

Consider the following class of functions.

$$\sigma_g(h) = gh$$

These functions can be seen to be permutations of $\mathrm{Sym}(G)$, and furthermore, $g \to \sigma_g$ is an injective homomorphism. The image of this injective homomorphism represents a subgroup of $\mathrm{Sym}(G)$, hence every group is isomorphic to some permutation group.

Theorem 6.1 (Cayley's theorem)**.** Every group is isomorphic to a permutation group.

$$(G, \circ)$$
$$\exists H \leq \mathrm{Sym}(G)[G \cong H]$$

It has been noted that as interesting as this result may be, it doesn't seem to have profound implications regarding the methods used by group theorists.

6.2 Cycles

There exists a special class of permutation functions called 'cycles'; it describes where to send an element, and then where to send that displaced element to, and then the next displaced element, until the original element's index is filled. Not every permutation function is a cycle, however as it turns out, compositions of cycles can represent any permutation in a symmetric group; this result will be proved shortly.

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

Assume indexed in order, the cycle then says to send 'index 3' to 'index 1, 'index 2' to 'index 3', and finally 'index 1' to 'index 2'.

Definition 6.4 (k-cycle)**.** A *k-cycle* is a permutation $\sigma : X \to X$ such that there is a $x \in X$ such that for any $y \in X$ we either have an $n \leq k$ where $\sigma^n(x) = y$ or $\sigma(y) = y$. Call x the generator of this cycle.

A 2-cycle is calso called a *transposition*. A *simple transposition* is a transposition that permutes adjacent elements, so is of the form $(i, i+1)$.

Let σ be a k-cycle, then $\sigma^k(x) = x$.

Let σ be a k-cycle, then there are k generators of that cycle, precisely the elements of the form $\sigma^n(x)$, where x is a known generator.

We can represent a special notation for cycles; tuples that represent those elements that such an x generates under repeated composition.

We represent a *k-cycle* as $(x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x))$.

One may note that any element in this tuple can

Definition 6.5 (Disjoint pair of cycles)**.** *disjoint pairs of cycles* are a pairs of cycles that permute no element in common; they contain no element in common.

6.2.1 Properties of Cycles

- commutativity of disjoint cycles

Proposition 6.3. Let σ, τ be disjoint cycles. then $\sigma\tau = \tau\sigma$.

Proposition 6.4. All permutation functions are the unique representation as the product of disjoint cycles.

Definition 6.6 (Cycle type)**.**

Lemma 6.1 (Conjugate cycle lemma)**.** Let σ be a permutation function and $\tau = (t_1, \ldots, t_n)$ be a cycle, then the following holds.

$$\sigma\tau\sigma^{-1} = (\sigma(t_1), \ldots, \sigma(t_n))$$

Theorem 6.2 (Cycle type-conjugation theorem)**.** Given a k-cycle τ, any other k-cycle can be represented by some $\sigma\tau\sigma^{-1}$ for some permutation function σ.

I've just come up with the following theorem, it's not very important.

Theorem 6.3. Let σ be a permutation of n disjoint cycles with lengths $l_1, l_2, ..., l_n$. Then $\sigma^{\text{lcm}(l_1,l_2,\ldots,l_n)} = \sigma$ Hence we have $\sigma^{\text{lcm}(l_1,l_2,\ldots,l_n)-1} = \sigma^{-1}$

6.3 Inversions

It's often useful to see how 'out of order' a permutation is from the identity permutation (in other words, how many simple transpositions are required to form the permutation). The idea of inversions captures this.

Definition 6.7 (Inversion set of a permutation)**.** The *inversion set of a permutation* is the set of all pairs of elements that are 'out of order' in the sense that permutation permutes some number to a larger number. Let $n(\sigma) = |I_\sigma|$ be the *inversion number function.*

$$I_\sigma = \{(i, j) : 1 \leq i < j \leq N \wedge \sigma(i) > \sigma(j)\}$$

Proposition 6.5. σ is identity permutation iff $n(\sigma) = 0$

When two 'adjacent' elements are permuted by a simple transposition, the number of inversions changes by 1. This is characterized in the following lemma.

Lemma 6.2. For a simple transposition s_i and permutation σ, we have the following.

$$n(\sigma s_i) = \begin{cases} n(\sigma) + 1 & \sigma(i) < \sigma(i+1) \\ n(\sigma) - 1 & \sigma(i) > \sigma(i+1) \end{cases}$$

Proposition 6.6. σ is a product of $n(\sigma)$ simple transpositions.

6.4 Alternating group

6.4.1 Permutation signature

So far we have been counting the amount of simple transpositions required to form a permutation; we can class permutations by the parity of this count.

Definition 6.8 (Permutation signature)**.** The *permutation signature* is a function $\text{sgn} : \text{Sym}(n) \to \{\pm 1\}$ defined on symmetry groups that keeps parity of the amount of inversions.

$$\text{sgn}(\sigma) = (-1)^{n(\sigma)}$$

The signature function has a codomain of two elements; however an important homomorphism can be established.

Proposition 6.7. The signature function is a homomorphism from $\mathrm{Sym}(n)$ to $\mathbb{Z}/2\mathbb{Z}$.

Calculating the signature for a cycle is simply a matter of counting the amount of elements it cycles between.

Proposition 6.8.

$$\mathrm{sgn}((x_1, x_2, \ldots, x_k)) = (-1)^{k-1}$$

6.4.2 Alternating group

Permutation signatures serve as a function that encapsulates a notion of 'parity' of permutations; does it require an even or odd amount of simple transpositions to form?

What happens when one considers the subgroup of only 'even' signatures? This is the kernel of the signature homomorphism, hence it is a normal subgroup. It is specifically called the *alternating group*.

Definition 6.9. $\mathrm{Alt}(n)$ represents the subgroup of $\mathrm{Sym}(n)$ of permutations with signature 1. Alternatively, it is $\ker(\mathrm{sgn})$, where $\mathrm{sgn} : \mathrm{Sym}(n) \to \mathbb{Z}/2\mathbb{Z}$ is the permutation signature function.

$$\mathrm{Alt}(n) < \mathrm{Sym}(n)$$

$$\mathrm{Alt}(n) = \{\sigma \in \mathrm{Sym}(n) : \mathrm{sgn}(\sigma) = 1\}$$

Proposition 6.9.

$$|\mathrm{Alt}(n)| = \frac{n!}{2}$$

Since the signature function is a homomorphism to $\mathbb{Z}/2\mathbb{Z}$ we can create the following isomorphism by the first isomorphism theorem.

Proposition 6.10.

$$\mathrm{Sym}(n)/\mathrm{Alt}(n) \cong \mathbb{Z}/2\mathbb{Z}$$

Proposition 6.11. Let $\sigma \in \mathrm{Alt}(n)$, then σ is a product of 3-cycles.

6.5 Simple group

Definition 6.10. A *simple group* is a group whose only normal subgroups are the trivial group and itself.

Every permutation of $\mathrm{Alt}(n)$ where $n \geq 3$ is a product of 3-cycles.

Proposition 6.12. For $n \geq 5$, $\mathrm{Alt}(n)$ is simple.

Chapter 7

Group Actions

7.1 Group Actions

Groups have thus far been very interesting to study in and of themselves, however groups are equally interesting to study on how they can interact with generic sets. The groups $\mathrm{Sym}(n)$ have permutation functions as their object, however these permutations are functions operating on $\mathbb{N} \cap [1, n]$.

This is quite a motivating example to develop some theory of how group elements can 'act' on some set; imagine we want to prove things about permutations that don't move 5 around? Some of this we've been doing implicitly (mutually exclusive permutations), however this idea can be generalized.

Definition 7.1 (Left group action)**.** Given a group $(G, \circ)$, a *left group action* $\alpha : G \times S \to S$ is a map $\alpha(g, s) = g \cdot s$ with the following properties for any $s \in S$ and $g, h \in G$.

- $\alpha(1_G, s) = s$
- $\alpha(g, \alpha(h, s)) = \alpha(gh, s)$

We say that group G acts on S.

When the group action and set element is apparent, a group action $\alpha(g, s)$ may be denoted as $g \cdot s$.

It is sometimes useful to 'curry' group actions; this means that instead of interpreting it as a group element and set element to make a set element, we can think of group actions as group elements making functions from the set to itself. These functions can be proven to be bijective.

Instead of one bivariate function, we have a class at most $|G|$ univariate functions.

$$\alpha_g : S \to S$$
$$\alpha_g(s) = \alpha(g, s)$$

Proposition 7.1. $\alpha_g(s)$ is bijective.

We provide some exmaples of group actions.

Example 7.1 (Left regular action)**.**

$$\alpha : G \times G \to G$$
$$\alpha(g, h) = gh$$

Example 7.2 (Conjugation action)**.**

$$\alpha : G \times G \to G$$
$$\alpha(g, h) = ghg^{-1}$$

Noting that the actions 'group' here is H and 'set' is G, we can think of left cosets as orbits of the following left action.

Example 7.3 (Left coset projection action)**.**

$$\alpha : H \times G \to G$$
$$\alpha(h, g) = gh^{-1}$$

We inver h so that $\alpha(h_1, \alpha(h_2, g)) = \alpha(h_2 h_2, g)$ is satisfied.

Example 7.4 (Permutation functions)**.**

$$\alpha : \mathrm{Sym}(n) \times \mathbb{N} \cap [1, n] \to \mathbb{N} \cap [1, n]$$
$$\alpha(\sigma, i) = \sigma(i)$$

Example 7.5.

$$\alpha : G \times G/H \to G/H$$
$$\alpha(g_1, gH) = (g_1 g)H$$

7.2 Orbits

We know that if we fix the first (group) argument of an action, the image is the set S it works over (since such functions are bijections), but what if we fix the second (set) argument and then consider its image? This is a more interesting situation, and the image of such a function is the idea of an *orbit*.

Simply put, orbits represent all possible actions on a set element. They are a generalization of the notion of a left coset.

Definition 7.2 (Orbit of a set element)**.** Given a group action $\alpha : G \times S \to S$, the *orbit of* s is the set of element obtainable by G acting on a specific s.

$$\mathrm{Orb}_\alpha(s) = G \cdot s = \{\alpha(g, s) : g \in G\}$$

The set of unique orbits on each set element is denoted S/G.

$$S/G = \{G \cdot s : s \in S\}$$

We have already seen examples of these hidden; in the left coset projection action, the orbits are the left cosets formed by each g. Much like the idea of how cosets are a way to study behaviour of some g on a subgroup H, we can study the behaviour of a group action with various group arguments on a set element s.

Let's now discuss the elementary properties of orbits, we will see some similar properties to left cosets. Indeed, some of the properties we had discovered about left cosets were really just general properties group actions! Similarly to the idea of how cosets partition a group, orbits partition a generic set.

Proposition 7.2. Orbits are either equal or disjoint.

$$G \cdot s \neq G \cdot t \implies G \cdot s \cap G \cdot t = \emptyset$$

Corollary 7.1. Orbits are equivalence classes on X.

Proposition 7.3.

$$S = \bigcap_{s \in S} G \cdot s$$

Since the distinct cosets partition a group, we obtained Lagrange's theorem. Since distinct orbits partition a set, a weaker but more general result

holds for group actions. Since orbits do not generally exhibit the same bijective behaviour as cosets, different orbits may have different cardinalities, so the cardinality of an orbit may doesn't divide the cardinality of the set like cosets do, but at least we know that the distinct orbits sum up to the set.

The following result is a generalization of Lagrange's theorem of cosets to a group from actions to a set. Indeed, applying the result on the left-coset action $\alpha(h, g) = gh^{-1}$ and using the fact that for any $g_1, g_2 \in G$ we have $|g_1 H| = |g_2 H|$ is exactly Lagrange's theorem!

Corollary 7.2. Consider the following equivalence classes that capture elements with the same orbit.

$$[x] = \{y \in S : Gy = Gx\}$$

Then the following E is used to index the distinct orbits.

$$B = \{[x] : x \in S\}$$

Then the following holds.

$$|S| = \sum_{[x] \in B} |Gx|$$

Later on we will find another formulation of this formula in terms of another object called a *stabilizer* which we will see shortly.

7.3 Stabilizers

When considering actions, it is of interest to examine the fixed points of the action (i.e the input set element is the output set element).

Definition 7.3 (Fixed point of G)**.** A *fixed point of* G is some element s such that for any $g \in G$,$g \cdot s = s$. The set of fixed points of S under G is denoted S^G.

$$\mathrm{Fix}_\alpha(G) = \{s \in S : \forall g \in G[\alpha(g, s) = s]\}$$

We can also consider the fixed points with respect to a group subset.

$$\mathrm{Fix}_\alpha(H) = \{s \in S : \forall h \in H \leq G[\alpha(h, s) = s]\}$$

This set gives us the fixed points of the group action, however what if we want to see group elements can be fixed to make some set element x (or better yet, any element in some X) act as fixed points?

In a similar vein to orbits, we can fix the second (set) argument and see what group elements produce fixed points for that element, this is the notion of a *stabilizer*.

Simply put, stabilizers represent all group elements for which a set element is a fixed point (or for which a collection of set elements are all fixed points).

Definition 7.4 (Stabilizer of X)**.** Given a set element x, the *stabilizer of* x is the set of all group elements for which x is a fixed point.

$$\text{Stab}_\alpha(x) = G_x = \{g \in G : \alpha(g, x) = x\}$$

Given a subset $X \subseteq S$, the *stabilizer of* X is the set of all group elements for which every action on an $x \in X$ is stil in X.

$$\text{Stab}_\alpha(X) = G_X = \{g \in G : \forall x \in X[\alpha(g, x) \in X]\}$$

Proposition 7.4.

$$\text{Stab}_\alpha(x) \leq G$$

Unfortunately even though it forms a subgroup, it may not always form a normal subgroup, meaning we can't always make quotient groups from them. For the sake of curiosity, I have fished out a necessary and sufficient condition when they are normal subgroups.

Proposition 7.5. Let G be a group. A stabilizer $\text{Stab}_\alpha(x)$ is a normal subgroup iff every set element in the orbit $\text{Orb}_\alpha(x)$ forms the same stabilizer as $\text{Stab}_\alpha(x)$.

$$\text{Stab}_\alpha(x) \lhd G \iff \forall \omega \in \text{Orb}_\alpha(x)[\text{Stab}_\alpha(x) = \text{Stab}_\alpha(\omega)]$$

Even though the set of left cosets of stabilizers doesn't always form a quotient group, we will study it anyways because it has an interesting connection to orbits by the orbit stabilizer theorem!

7.4 Orbit-Stabilizer theorem

Orbits and stabilizers have an interesting combinatorial relation between them. We start by comparing the behaviour of gG_x and $g \cdot x$ with different g and notice the following insight; when $gG_x = hG_x$ we also have $g \cdot x = h \cdot x$.

As it turns out, there is a bijection between the set of x-stabilizer left cosets and x-orbits!

Theorem 7.1 (Orbit-Stabilizer theorem)**.** Let $f : G/G_x \to Gx$ be a function defined by $f(gG_{x_0}) = \alpha(g, x_0)$. f is bijective; x stabilizer cosets are in bijection with elements of the orbit of x.

We obtain a juicy corollary from the orbit-stabilizer theorem since a bijective function between sets implies equal cardinalities of domain and codomain.

By taking the cardinality of the domain and image of this bijection and applyting Lagrange's theorem, we get an interesting result.

Corollary 7.3.

$$|G/\mathrm{Stab}_\alpha(x)| = |\mathrm{Orb}_\alpha(x)|$$

Futhermore, we can apply Lagrange's theorem to derive the following.

$$|G| = |\mathrm{Orb}_\alpha(x)||\mathrm{Stab}_\alpha(x)|$$

The cardinality of an x-orbit is the amount of distinct cosets of the x-stabilizer. Not only that, but the use of Lagrange's theorem tells us that the cardinality of an x-orbit divides the order of the group! x-stabilizers are subgroups, hence Lagrange implies this automatically, however x-orbits require this orbit-stabilizer theorem for such a result.

Example 7.6. Given $H \leq G$, let $\alpha : H \times G \to G$ be the group action defined by $\alpha(h, g) = gh^{-1}$. The orbits of this group action are simply the left cosets. The mapping gh exhibits the same behaviour but conflicts with the required property of group actions that $\alpha(h_2, \alpha(h_1, g)) = \alpha(h_2h_1, g)$. All the stabilizers are $G_x = \{1_G\}$ for this action.

We expressed our 'generalized Lagrange's theorem' in terms of orbits, but due to the orbit-stabilizer theorem and its corollary we can translate our statement to be in terms of stabilizers instead.

Corollary 7.4. Let G be a finite group acting on S, then the following holds where B is a set constructed by choosing one element from each orbit with over one element.

Consider the following equivalence classes that capture elements with the same orbit.

$$[x] = \{y \in S : G/\text{Stab}_\alpha(y) = G/\text{Stab}_\alpha(x)\}$$

Then the following E is used to index the distinct orbits.

$$B = \{[x] : x \in S\} \setminus \{[x] : x \in \text{Fix}_\alpha(G)\}$$

Then the following holds.

$$|S| = |\text{Fix}_\alpha(G)| + \sum_{[x]\in B} |G/\text{Stab}_\alpha(x)|$$

7.4.1 Burnside's lemma

Group actions are very powerful for creating combinatorial arguments due to its ability to generalize Lagrange's theorem from a group to any set that is compatible with a desired group action. Extending on those results leads us to a prominent result known as *Burnside's lemma*.

Using this corollary, one can derive *Burnside's lemma*. It states that we can count the amount of unique orbits by finding the 'average' of each 'g-invariant set of elements' (set elements where the group action with g has no effect). It is an indispensable tool in combinatorics; particularly for counting how many symmetrically unique colorings there are on an n-gon.

Lemma 7.1 (Burnside's lemma)**.**

$$|S/G| = \frac{\sum_{g\in G} |\text{Fix}_\alpha(\{g\})|}{|G|}$$

7.5 Conjugacy

We have sufficient background in group actions to look at applications to the study of groups. Although we have studied left cosets without resorting to group actions, group actions prove extremely useful in studying the congugacy action, which like the left coset projection action, can be defined naturally on any group.

Recall the action $\alpha(g,h) = ghg^{-1}$ is called *conjugation*. The *conjugacy class of* h is the orbit of h of conjugation.

Definition 7.5 (Conjugacy class of h)**.** The *conjugacy class of* h is the set of elements possible by conjugating h by group elements.

$$C(G,h) = \{ghg^{-1} \in G : ginG\}$$

The conjugacy class of $\{h\}$ is the orbit $G \cdot h$ by the conjugacy action.

Definition 7.6 (Centralizer of a group subset)**.** The *centralizer of* S *in* G is the set of elements that commute with the elements of S.

$$Z(G,S) = \{g \in G : \forall s \in S \subseteq G[gsg^{-1} = s]\}$$

The centralizer of $\{h\}$ is the stabilizer $\mathrm{Stab}_\alpha(\{h\})$ for the conjugacy action.

Note also that the set of all fixed points (with respect to conjugacy action) is therefore just the center $Z(G)$

$$Z(G,G) = Z(G) = \mathrm{Fix}_\alpha(G)$$

Definition 7.7 (Normalizer of a group subset)**.** The *normalizer of* S *in* G is the set of elements that make S conjugate to itself.

$$N(G,S) = \{g \in G : gSg^{-1} = S\}$$

The normalizer of S is the stabilizer $\mathrm{Stab}_\alpha(S)$ for the conjugacy action.

Consider the normalizers of a singleton $\{h\}$ (so $N(G,\{h\}) = \{g \in G : ghg^{-1} = h\}$), since $gh = hg \iff ghg^{-1} = h$, such normalizers happens to be the stabilizer for the conjugation action.

By applying one of our counting theorem with the conjugacy action, we get the following formula to enumerate any group.

Corollary 7.5. Let G be a finite group, then the following holds where B is a set constructed by choosing one element from each conjugacy class with over one element.

$$[h] = \{g \in G : C(h) = C(g)\}$$

$$B = \{[g] : g \in G \wedge |[g]| > 1\}$$

$$|G| = |Z(G)| + \sum_{[g] \in B} |G/Z(G,\{g\})|$$

7.6 Groups of order p^r

Definition 7.8 (p-group)**.** A *p-group* is a group of order p^n.

By considering the generalized Lagrange theorem on p-groups, we notice the following proposition and corollary.

Proposition 7.6. Let G be a p-group with order larger than 1 acting on a finite set S, then the following holds.

$$|S| \equiv |S^G| \mod p$$

Corollary 7.6. Let G be a finite p-group with order larger than 1, then the following holds.

$$|G| \equiv |Z(G)| \mod p$$

Corollary 7.7. Let G be a finite p-group with order p^2, then G is Abelian.

7.7 Sylow theorems

Definition 7.9 (Sylow p-subgroup)**.** Let G be a finite group of order $p^n m$ where p is prime and m is coprime to p, a subgroup of G with order p^n is called a *Sylow p-subgroup*.

$$p \text{ is prime }, \gcd(p, m) = 1, n \in \mathbb{N} \setminus \{0\}$$

$$H \text{ is a Sylow p-subgroup of } G \iff H \leq G \wedge |G| = p^n m \wedge |H| = p^n$$

Theorem 7.2 (First Sylow theorem)**.** Let G be a finite group, for each prime factor p of $|G|$, G has a Sylow p-subgroup.

Theorem 7.3 (Second Sylow theorem)**.** Let H, K be two Sylow p-subgroups of the finite group G, then H and K are conjugate to eachother. That is, there exists a $g \in G$ where the following holds.

$$gHg^{-1} = K$$

Theorem 7.4 (Third Sylow theorem)**.**

$$|\mathrm{Syl}_p(G)| \equiv 1 \mod p$$

$$m \equiv 0 \mod |\mathrm{Syl}_p(G)|$$

$$|\mathrm{Syl}_p(G)| = |G/N(P)|, P \in \mathrm{Syl}_p(G)$$

-Sylow p-group

Recall our beloved Lagrange's theorem; it's pretty cool that the order of subgroups divide the order of the group. However, if a number divides the order of a group, does that mean a subgroup with an order of that number be made? This is the converse to Lagrange's theorem, and it is not true in general, however it turns out that this is true for prime numbers and these groups happen to be cyclic!

Proposition 7.7 (Cauchy's theorem)**.** Let G be a finite group. If a prime number p divides the order of G, then there exists a cyclic subgroup of G with order p.

7.8 Wreath product

Chapter 8

Group-like Structures

Regarding algebraic structures of 1 set and 1 operation, we study groups in greatest depth because many mathematical objects we know (operations on numbers, composition of functions, symmetries of a shape etc.) are representable by groups, and groups have a rich set of results. It is useful to know structures that are similar yet weaker to groups, for the sake of terminology or in the creation of more complex algebraic structures.

We skip the algebraic structure of a category; this is covered in Category Theory.

8.1 Monoids

Groups are very intersting structures to study, however sometimes what we want to model doesn't quite have the properties of a group. There are a range of group-like structures that relax some of the properties of a group. Perhaps the runner up to the group is the *monoid*.

Monoids are essentialy groups without the guarantee of elements being invertible. One notable place where monoids arise is category theory, where a category of one object is a monoid.

Monoids also find wide usage in theoretical computer science, specifically in automata theory.

8.2 Magmas

8.3 Loops

Part II

Advanced

Chapter 9

Free groups

Free groups

9.1 Tietze transformations

Theorem 9.1 (Tietze's theorem)**.**

9.2 Lattices

Lattices are a special subset of a linear space (usually $\mathbb{R}^n$) with these properties:

- Lattice points are closed under vector addition and subtraction
- There is some minimum distance such that every lattice point is at least this distance from any other lattice point.
- There is some maximum distance such that the distance between every point and their closest lattice point is less than this distance.

$$\Lambda = \{\sum_{i=1}^{n} a_i \mathbf{b}_i : a_i \in \mathbb{Z}\}$$

Lattices are isomorphic to free Abelian groups

Chapter 10

Torsion elements

Definition 10.1 (Torsion element)**.**

$$g \text{ is a torsion element of } G \iff \exists n \in \mathbb{Z}[g^n = 1_G]$$

We know that For finite groups, all elements are torsion elements. We've also been using torsion elements as a way to define cyclic subgroups. Where things get interesting is when we consider infinite groups where all elements are torsion elements.

Definition 10.2 (Torsion group)**.**

$$G \text{ is a torsion group} \iff \forall g \in G[g \text{ is a torsion element of } G]$$