Group Theory

Zac Zerafa

September 27, 2025

Contents

Part I

Groups and Subgroups

Chapter 1

Groups

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*.

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

1.1 Groups

Definition 1.1. A *group* is an ordered pair $(G, \cdot)$ of a set G and a binary operation $\cdot$ acting on G with the following properties:

- $\cdot$ is associative on G
- G contains an identity element with respect to $\cdot$
- Every element of G is invertible with respect to $\cdot$
- G is the set of elements the group works over
- $\cdot : G \times G \to G$ is the operation of the group

$(G, \cdot)$ is a group $\iff$ $\cdot$ is associative on $G \wedge \exists 1_G \in G[\forall g \in G(g \cdot 1_G = 1_G \cdot g = g)] \wedge \forall g \in G[\exists g^{-1}(g \cdot g^{-1} =$

When the operation is apparent, a group $(G, \cdot)$ may be denoted as G, and the expression $g \cdot h$ may be contracted to gh.

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. The *order* of a group is the cardinality of its set.

Definition 1.3. A *finite group* is a group with a finite order.

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 1.4. An *Abelian group* is a group such that $\cdot$ is also commutative.

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

Even though some groups may not be Abelian, they could have a collection of elements.

Definition 1.5. The *center* of a group G is a set $Z(G)$ containing the elements that commute with every other element.

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

1.2 Properties of Groups

To obtain a deeper intuition of the behaviour of a group, it is vital to deduce some common properties that all groups share.

Notably, one can derive properties regarding the uniqueness of identity and inverse elements of groups.

Proposition 1.1. Let $(G, \cdot)$ be a group:

- G contains a unique identity element with respect to $\cdot$
- Every element of G is invertible by a unique inverse element with respect to $\cdot$

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

Proposition 1.2.

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

The cancellation law is also permitted by groups thanks to inverse elements.

Proposition 1.3 (Cancellation law for Groups)**.** Let $(G, \cdot)$ be a group and $g, g_1, g_2 \in G$, then $g \cdot g_1 = g \cdot g_2$ iff $g_1 = g_2$

$$G \text{ is a group} \wedge g, g_1, g_2 \in G \implies g \cdot g_1 = g \cdot g_2 \iff g_1 = g_2$$

1.3 Notation for Groups

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

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

Group presentation - Notation for representing a group based on its elements and the conditions it is subject to

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

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

1.4 Examples of Groups

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

- It is Abelian
- It has order $\aleph_0$

Example 1.2. The *Klein fourgroup* $(K_4, \circ)$

- It is Abelian
- It has order 4

Example 1.3. The *dihedral group* $\mathrm{Dih}(n)$

- It has order $2n$

Example 1.4. The *general linear group* $(\mathrm{GL}(n, \mathbb{R}), \cdot)$

Chapter 2

Subgroups

2.1 Subgroups

Definition 2.1. A *subgroup* of $(G, \cdot)$ is a group $(H, \cdot)$ such that H is a subset of G. $H \leq G$ denotes that H is a subgroup of G.

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

Theorem 2.1. Let $(G, \cdot)$ be a group:

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

2.2 Examples of Subgroups

Proposition 2.1.

$$Z(G) \leq G$$

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

Example 2.1. The *additive group of n-multiples* $(n\mathbb{Z}, +)$ Subgroup of $(\mathbb{Z}, +)$ of multiples of n.

Example 2.2. The *special linear group* $\mathrm{SL}(n, \mathbb{R})$ Subgroup of $\mathrm{GL}(n)$ of matrixes with determinant 1.

Example 2.3. The *orthogonal group* $\mathrm{O}(n, \mathbb{R})$ Subgroup of $\mathrm{GL}(n)$ of orthogonal matrixes

Example 2.4. The *special orthogonal group* $\mathrm{SO}(n, \mathbb{R})$ Subgroup of $\mathrm{O}(n)$ of matrixes with determinant 1

- It is Abelian for $n \leq 2$

2.3 Properties of Subgroups

Proposition 2.2. Let H be a subgroup of G, then 1_G is in the subgroup H.

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

Chapter 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*.

3.1 Cosets

Definition 3.1. Given the subgroup $(H, \cdot)$ of $(G, \cdot)$, a *left coset* of $(H, \cdot)$ is a set gH containing the elements of the form $g \cdot h$, where $h \in H$.

$$gH = \{g \cdot h : h \in H\}$$

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

Definition 3.2. If $(H, \cdot)$ is a subgroup of $(G, \cdot)$, a *right coset* of $(H, \cdot)$ is a set Hg containing the elements of the form $h \cdot g$, where $h \in H$.

$$Hg = \{h \cdot g : h \in H\}$$

3.2 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 3.1. The cardinality of left cosets of $(H, \cdot)$ is the order of $(H, \cdot)$

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

Proposition 3.2.

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

3.3 Lagrange's theorem

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 3.1.

$$H \leq G \wedge h \in H \implies hH = 1_G H$$

The previous proposition discusses the result of forming cosets with a subgroup element, which is useful to know, however forming cosets on foreign elements will provide deeper insight.

Lemma 3.2. Left cosets are equivalence classes on G.

Lemma 3.3. Left cosets are either equal or disjoint.

Theorem 3.1 (Lagrange's theorem)**.** 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 3.3.

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

Part II

Group homomorphisms

Chapter 4

Group homomorphism

Definition 4.1. Let $(G, \cdot)$ 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.

$$f(g_1 \cdot g_2) = f(g_1) + f(g_2)$$

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

Proposition 4.1.

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

Proposition 4.2.

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

4.1 Examples of Group homomorphism

4.2 Group monomorphism

4.3 Group epimorphism

4.4 Group endomorphism

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

phisms.

Chapter 5

Group isomorphism

Definition 5.1. Let $(G, \cdot)$ 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 $(G, \cdot) \cong (H, +)$.

5.1 Properties of Group isomorphism

5.2 Examples of Group isomorphism

5.3 Group automorphism

Definition 5.2. Let $(G, \cdot)$ be a group. A *group automorphism* $f : G \to G$ is an isomorphism onto the same group.

Proposition 5.1. For any group $(G, \cdot)$ there exists a class of automorphisms called the *inner automorphisms* defined as $\varphi_g(x) = gxg^{-1}$.

Some Theorems

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.

Definition 5.3. Let $(G, \cdot)$ 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 5.2.

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

Definition 5.4.

$$\text{Im}(f) = \{f(g) \in H : g \in G$$

Isometry

Part III

Quotient Groups

Chapter 6

Normal subgroups

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.

We have discovered that cosets formed from subgroups essentially *divides* a groups elements into equally sized classes. One may ask if a group on these cosets can be formed with the operator + behaving similar to the original group in the sense that $g_1H + g_2H = (g_1 \cdot g_2)H$.

One slightly small caveat is that cosets formed by different elements be the same coset (more specifically, if $b \in aH$, then $aH = bH$), so if we have $aH = bH$,we want $(a \cdot g)H = (b \cdot g)H$, which is not true in general! So as a precursor to defining these 'groups divided into cosets', we must first address this concern by finding what type of subgroup permits this type of behaviour.

6.1 Normal subgroups

Normal subgroups are what is required to ensure that identical cosets are treated the same by our 'coset operation'.

Definition 6.1. A *normal subgroup*

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

Here is a useful sufficient condition for normal subgroups.

Proposition 6.1. If a subgroup is Abelian, then it is normal.

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

This immediately implies the following.

Proposition 6.2. Centers are normal subgroups.

$$Z(G) \lhd G$$

Although kernels are not necessarily Abelian, they are indeed normal.

Proposition 6.3. Kernels are normal subgroups.

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

6.2 Quotient map

Now we can define the behaviour of this operation through a homomorphism without quarrel.

Definition 6.2. The *Quotient map* π of a normal group N is the following group epimorphism from the original group G to cosets of the normal subgroup gN.

$$\pi : g \mapsto gN$$

Chapter 7

Quotient groups

Definition 7.1. A *quotient group* is a group G/N of unique cosets on the normal subgroup gN with the operation defined by the quotient map.

7.1 Examples of quotient groups

Example 7.1. 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 7.2. The *circle group* $(\mathbb{T}, \cdot)$, 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.*

7.2 First isomorphism theorem

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

Lemma 7.1.

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

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.

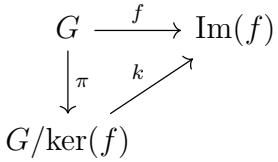
Lemma 7.2.

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

One way of interpreting this lemma is that kernel cosets correspond to sets of elements with the same homomorphism mappings. This is the essence of the *first isomorphism theorem*.

Theorem 7.1 (First isomorphism theorem for groups)**.** Let $f : G \to H$ be a homomorphism . Then $\mathrm{Im}(f) \cong G/\ker(f)$ the following isomorphism k.

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



Corollary 7.1.

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

Corollary 7.2.

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

Part IV

Cyclic Groups

Chapter 8

Cyclic Group

8.1 Properties of Cyclic Groups

Definition 8.1. A *cyclic group* $(G, \cdot)$ is a group such that there exists some element γ that can generate all other elements of the group under the operation. That is, all elements are of the form g^n. We say that such a γ *generates* G.

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

If the group operator is clear, one may write the set of elements generated by the element g as the following.

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

.

Definition 8.2. Let $(G, \cdot)$ be a cyclic group. A *generator of a cyclic group* is an element γ that generates G. The order of a generator is the order of the group that it forms.

$$\gamma \in G \text{ is a generator of } (G, \cdot) \iff G = \langle \gamma \rangle$$

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).

Definition 8.3. $\text{Cyc}(n)$ is the cyclic group of order n

Let's consider subgroups of cyclic groups.

Definition 8.4. A *cyclic subgroup*

8.2 Properties of Cyclic Groups

The following theorem greatly expands our power to work with cyclic groups since it equates it (up to an isomorphism) to a very familiar friend.

Proposition 8.1.

$$\mathrm{Cyc}(n) \cong \mathbb{Z} \setminus n\mathbb{Z}$$

Proposition 8.2. Groups of prime order are cylcic.

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

Proposition 8.3. Subgroups of cyclic groups are cyclic.

Proposition 8.4. If d divides the order of a cyclic group, then there is a unique cyclic subgroup of order d.

Proposition 8.5.

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

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 8.6 (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.

Part V

Product Groups

Chapter 9

Direct Product Groups

Definition 9.1. A *product of group subsets* is the set closed by multiplying elements of two subsets together.

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

Definition 9.2. A *product group* is a group $(G \times H, \cdot)$ formed by the groups $(G, \cdot_G)$ and $(H, \cdot_H)$ with the operation as such.

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$$

- $G \times H$ is the cartesian product of the group sets
- $G \times H$ is the cartesian product of the group sets

Proposition 9.1.

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

Proposition 9.2.

$$H, K \leq G \land H \times K \cong G \iff H \cap K = \{1_G\} \land HK = G \land K \lhd G$$

9.1 A 'Chinese remainder theorem' for groups

Proposition 9.3. Let $(n_i)_{i=1}^r \in \mathbb{Z}$ be coprime integers and $N = \prod_{i=1}^r n_i$. Then $\mathbb{Z}$
$N\mathbb{Z} \cong \times_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$.

- Sylow's theorem

Chapter 10

Semidirect Product Groups

- semidirect product group

10.1 Relationship between Direct and Semidirect Product Groups

- when is a direct-semidirect map an isomorphism?

Part VI

Symmetric Groups

Chapter 11

Symmetric Group

Definition 11.1. A *permutation function on* X is a bijective function $\sigma : X \to X$. It represents the idea of permuting (swapping around) elements of X.

Definition 11.2. 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 operator

Definition 11.3. $\mathrm{Sym}(n)$ represents the symmetry group with permutations on $\mathbb{N} \cap [1, n]$.

Proposition 11.1.

$$n \in \mathbb{N} \wedge |X| = n \implies \mathrm{Sym}(X) \cong \mathrm{Sym}(n)$$

Proposition 11.2.

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

Since symmetric groups of identical orders are all isomorphic, we shall only speak about symmetric groups in the context of $\mathrm{Sym}(n)$, and permutation functions are always considered on $\mathbb{N} \cap [1, n]$.

There are 3 standard notations to represent the mappings of a permutation

- Standard function notation
- Matrix notation

- Cycle notation

As with any general function, a permutation is expressible as an equality of the function on its argument to its mappings, for instance, $\sigma(n) = \begin{cases} 3 & n = 1 \\ 1 & n = 2 \\ 2 & n = 3 \end{cases}$. However, for permutations this notation grows exponentially inefficient for larger symmetry groups.

The matrix notation uses a matrix where the first row indicates the indexes, and the second row indicates mappings $\sigma = \begin{bmatrix} 123 \\ 312 \end{bmatrix}$ - matrix notation - permutation group

There exists a notation of 'cycles' which is even more efficient; 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 is reducible to a single cycle, however composition of cycles can represent any permutation; this result will be prooved shortly.

$\sigma = (132)$

Definition 11.4. A *permutation group* is a subgroup of a symmetric group.

Chapter 12

Cycles

- cycle notation

12.1 Cycles

Definition 12.1. A *k-cycle* is a permutation . A 2-cycle is calso called a *transposition.* A *simple transposition* is a transposition that permutes adjacent elements, so is of the form $(i, i+1)$.

Definition 12.2. *disjoint pairs of cycles* are a pairs of cycles that permute no element in common; they contain no element in common.

12.2 Properties of Cycles

- commutativity of disjoint cycles - all bijections have unique disjoint cycle product representation - cycle type - conjugate cycle lemma - cycle type-conjugation theorem

12.3 Inversions

The bubble sort algorithm is

Definition 12.3. 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 $n(\sigma) = |I_\sigma|$

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

Proposition 12.1. 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 12.1. For a simple transposition s_i and permutation σ, we have the following.

$$n(\sigma s_i) = ?????$$

Proposition 12.2. σ is a product of $n(\sigma)$ simple transpositions.

Chapter 13

Alternating group

13.1 Permutation signatures

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.

- permutation signature

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

The signature function has a codomain of two elements; by mapping - signature homomorphism

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

Proposition 13.1.

$$\text{sgn}((x_1 x_2 ... x_k)) = (-1)^{k-1}$$

13.2 Alternating group

Signatures of permutations 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 called the *alternating group*.

Definition 13.1. Alt(n) represents the subgroup of Sym(n) of permutations with signature 1.

Proposition 13.2.

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

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

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

13.3 Simple group

Definition 13.2. A *simple group* is a group whose only normal subgroups are the trivial group and itself.

- simple group

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

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

13.4 Cayley's theorem

- Cayley's theorem

Part VII

Group Actions

Chapter 14

Group Actions

14.1 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 operate on natural numbers.

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 14.1. Given a group $(G, \cdot)$, 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.

14.2 Orbits

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. These are called *orbits*.

Definition 14.2. 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. The set of orbits on each set element is denoted $S//G$.

$$Gs = \{\alpha(g, s) : g \in G\}$$

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

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.

Lemma 14.1. Orbits are equivalence classes on S.

Lemma 14.2. Orbits are either equal or disjoint.

Definition 14.3. 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.

Definition 14.4. Given a set element x, the *stabilizer* is the set of all group elements for which x is a fixed point.

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

Similar to the kernel of a homomorphism, stabilizers form a subgroup.

Proposition 14.1.

$$G_x \leq G$$

Proposition 14.2. Let $f : G//G_x \to Gx$ be a function defined by $f(gG_{x_0}) = \alpha(g, x_0)$. f is bijective.

This proposition informally means that the larger the stabilizer is, the smaller the orbits are. It also means there are just as many unique cosets of the stabilizer of x as elements in the orbit of x.

Example 14.1. Given $H \leq G$, let $\alpha : H \times G \to G$ be the group action defined by $\alpha(h, g) = g \cdot h^{-1}$. The orbits of this group action are simply the left cosets. The mapping $g \cdot h$ exhibits the same behaviour but conflicts with the required property of group actions that $\alpha(h_2, \alpha(h_1, g)) = \alpha(h_2 \cdot h_1, g)$. All the stabilizers are $G_x = \{1_G\}$ for this action.

14.3 Burnside's lemma

Group actions are very powerful for creating combinatorial arguments, among the most prominent being *Burnside's lemma*.

We have established that orbits are either equal or disjoint, and elements of orbits of x have a bijection to cosets of the stabilizer of x. This permits the following simple corollary.

Corollary 14.1.

$$|S| = |S^G| + \sum_{x:Gx \in S//G \wedge |Gx|>1} |G//G_x|$$

-Burnside's lemma

Chapter 15

Groups of order p^r

Chapter 16

Sylow theorems

-Sylow p-group -First Sylow theorem -Second Sylow theorem -Third Sylow theorem

Part VIII

Group-like Structures

Chapter 17

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.

Chapter 18

Magmas

Chapter 19

Loops