Group Theory

1 Introduction

Definition 1.1 (Binary operation)**.** A binary operation on a set S is a mapping f from $S \times S$ to S.

Definition 1.2 (Group)**.** Let G be a non-empty set and $*$ a binary operation on A. The pair $(G, *)$ is called a group if the following are satisfied:

- For all $a, b, c \in G$ we have $(a * b) * c = a * (b * c)$; (Associativity)
- There exists $e \in G$ such that for all $a \in G$ we have $a * e = e * a = a$; (Identity element)
- For all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$. (Inverse element)

Definition 1.3 (Cayley table)**.** A Cayley table is a way to describe a finite group by arranging all the possible products of any two elements of the group. For example the table

$(A, *)$	e	x	y
e	e	x	y
x	x	?	?
y	y	?	?

is the Cayley table of some group such that $A = \{e, x, y\}$.

Remark 1.1. There is only one way to complete the above table such that it would describe a group.

Definition 1.4 (Homomorphism of groups)**.** Let $(G, *_G)$ and $(H, *_H)$ be groups. A homomorphism of groups is a function $\varphi\colon G \to H$ such that for any $a, b \in G$ we have

$$\varphi(x *_G y) = \varphi(x) *_H \varphi(y).$$

If there exists a homomorphism between G and H, they are called homomorphic groups.

Definition 1.5 (Isomorphism of groups)**.** An isomorphicm of groups is a bijective homomorphism. If there exists a homomorphism between two group G and H, they are called isomorphic groups.

We see that an isomorphism is a function the preserves the structure of the group in the sense that applying the function on the product of the elements x, y in G, is the same as taking the product of the elements $\varphi(x)$, $\varphi(y)$ in H.

We can see that the Cayley tables of isomorphic groups are the same. For example, if G and H are isomorphic groups of size 3, with the isomorphism $\varphi\colon G \to H$ we can see that

$(G, *_G)$	e	x	y
e	$e *_G e$	$e *_G x$	$e *_G y$
x	$x *_G e$	$x *_G x$	$x *_G y$
y	$y *_G e$	$y *_G x$	$y *_G y$

$\approx$

$(H, *_H)$	$\varphi(e)$	$\varphi(x)$	$\varphi(y)$
$\varphi(e)$	$\varphi(e *_G e)$	$\varphi(e *_G x)$	$\varphi(e *_G y)$
$\varphi(x)$	$\varphi(x *_G e)$	$\varphi(x *_G x)$	$\varphi(x *_G y)$
$\varphi(y)$	$\varphi(y *_G e)$	$\varphi(y *_G x)$	$\varphi(y *_G y)$

Then by applying the homomorphism property we get that the original table is approximately

$(H, *_H)$	$\varphi(e)$	$\varphi(x)$	$\varphi(y)$
$\varphi(e)$	$\varphi(e) *_H \varphi(e)$	$\varphi(e) *_H \varphi(x)$	$\varphi(e) *_H \varphi(y)$
$\varphi(x)$	$\varphi(x) *_H \varphi(e)$	$\varphi(x) *_H \varphi(x)$	$\varphi(x) *_H \varphi(y)$
$\varphi(y)$	$\varphi(y) *_H \varphi(e)$	$\varphi(y) *_H \varphi(x)$	$\varphi(y) *_H \varphi(y)$

which is exactly the Cayley group of H.

Definition 1.6 (Order of a group)**.** Let $(G, *)$ be a group. The size $|G|$ is said to be the order of the group.

The following table shows the amount of different groups up to isomorhism by their order:

Order	Number
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5
9	2

Definition 1.7 (Greatest common divisor)**.** The greatest common divisor (GCD) of integers a and b, at least one of which is nonzero, is the greatest positive integer d such that d is a divisor of both a and b. The greatest common divisor of a and b is denoted $\gcd(a, b)$.

Remark 1.2. We define $\gcd(0, 0) = 0$, but this is mostly not relevant.

Definition 1.8 (Coprime)**.** Let $a, b \in \mathbb{Z}$. We say that a and b are coprime if $\gcd(x, y) = 1$.

Proposition 1.1. *Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b)$ exists and is unique. Moreover, there exist $n, m \in \mathbb{Z}$ such that $d = am + nb$.*

Proof. Consider the following set

$$A := \{ma + nb \mid m, n \in \mathbb{Z} \quad \text{and} \quad ma + nb > 0\}.$$

The set isn't empty since $a^2 + b^2 \in A$, so by the well ordering theorem, it follows that it has a first element which we will call d. By the construction d is a positive integer.

- Without loss of generality suppose $b = qd + r$ and $r \neq 0$.

$$\begin{aligned} b &= q(ma + nb) + r \\ r &= (-qm)a + (1 - qn)b \end{aligned}$$

  $r \neq 0 \Rightarrow r \in A$ but $r < d$ which is a contradiciton!

- $c|b \quad \text{and} \quad c|a \rightarrow c$ divides all linear combinations of $a, b \rightarrow c|d$

□

Proposition 1.2. *Every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors.*

Proof. We will prove this by induction on n. For the base case $n = 2$ we know that $2 = p_1$. Since 2 is the smallest prime number this product (of one element) is unique.

Let $n > 2$. If n is a prime number then the proof is trivial. If is not prime, then $n = n_1 * n_2$ for some $1 < n_1, n_2 < n$. By the induction hypothesis $n_1 = p_1 * \cdots * p_n$ and $n_2 = p'_1, \cdots, p'_m$. Therefore $n = (p_1 * \cdots * p_n) * (p'_1 * \cdots * p'_m)$.

Suppose $n = p_1 * \ldots * p_n = q_1 * \ldots * q_m$ We know $p_1 | q_1 * \ldots * q_m$ so $p_1 = q_j$ for some j then we can rearrange the elements such that $p_2 * \ldots * p_n = q_2 * \ldots * q_m$ and so on to show that the factorization is unique every time. □

Definition 1.9 (The set $\mathbb{Z}_n^*$)**.** Let n be a natural number. We define

$$\mathbb{Z}_n^* = \{m \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}.$$

Proposition 1.3. *The pair $(\mathbb{Z}_n^*, *)$ is a group where $*$ denotes modular multiplication.*

Definition 1.10 (Order of an element)**.** Let $(G, *)$ be a group, let $g \in G$. Let n be the smallest positive integer such that $g^n = e$ where e is the unit element of G. We denote $|g| = n$. If there does not exist such n, we define $|g| = \infty$.

Definition 1.11 (Abelian group)**.** Let $(G, *)$ be a group. We say that G is abelian if for all $a, b \in G$ we have $a * b = b * a$.

Remark 1.3. The Cayley table for an abelian group is symmetric.

Definition 1.12 (The symmetric group)**.** Set $X_n := \{1, 2, \ldots, n\}$. The symmetric group denoted as $S(X_n)$ or S_n, is defined as the set of all bijections $\sigma \colon X_n \to X_n$ coupled with the operation of function composition.

Proposition 1.4. *If $(G, *)$ is a group of finite order, then every element of G also has a finite order.*

Proof. Denote $|G| = n$, and let $g \in G$. Consider the elements $g, g^2, \ldots, g^{n+1}$. From the pigeonhole principle there exists $1 \leq i \neq j \leq n + 1$ such that $g^i = g^j$. This implies that $g^{i-j} = e$. Therefore $O(g)$ is finite. □

Definition 1.13 (Subgroup)**.** Let $(G, *)$ be a group. If the set $(H, *_H)$ such that $H \subset G$ and $*_H = *|_H$ is a group, then H is called a subgroup of G.

Proposition 1.5. *Let $(G.*)$ be a group and $\emptyset \neq H \subseteq G$. Then H is a subgroup if and only if the following conditions are satisfied:*

(1) For all $a, b \in H$ we have $x * y \in H$;

(2) For all $a \in H$ we have $a^{-1} \in H$;

(3) $e \in H$.

Remark 1.4. Condition (3) is not necessary. If G is finite condition (2) is also not necessary.

Definition 1.14 (Cyclic group)**.** Let $(G, *)$ be a group. We say that G is cyclic if there exists an element $g \in G$ such that

$$G = \langle x \rangle := \left\{ g^k \mid k \in \mathbb{Z} \right\}.$$

If the group is of finite order n every subgroup is of order $k|n$. Prove by contradiction. A group generated from a set S is

$$G = \langle S \rangle := \bigcap_{S \subseteq H_a} H_a$$

Where H_a are all the subgroups that contain S. Let $S = \{a, b\}$ then the group will contain all possible products from a, b and their inverses.

Remark 1.5. From now on when we talk about a group and refer to it as G it should be clear that it is to be interpreted as $(G, *)$.

Theorem 1.6. (Lagrange's theorem). *Let G be a group and let H be a subgroup of G. Then $|H|$ is a divisor of $|G|$.*