Group Theory

Yeheli Fomberg

1 Groups

1.1 definition

Let A be a non-empty set and $*$ a binary operation on A. Under the following axioms

- $\forall (z, y, z) \in A^3 : (x * y) * z = x * (y * z)$
- $\exists e \in A : \forall a \in A : a * e = e * a = a$
- $\forall a \in A : \exists a^{-1} : a * a^{-1} = a^{-1} * a = e$

We shall call $(A, *)$ a group. Groups can also be described in "Cayley tables":

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

There is only one way to complete this table. Consider the axioms.

1.2 Isomorphisms of Groups

Let G_1, G_2 be groups and let $\phi : G_1 \to G_2$ be a function such that $\forall x, y \in G_1$

$$\phi(x) * \phi(y) = \phi(x * y)$$

Table of number of groups up to isomorphisms

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

2 Greatest Common Divisor

Let $(A, *)$ be a group and suppose $a, b \in A$. We'll denote $d = gcd(a, b)$ if:

- $d > 0$
- $d|b \quad \text{and} \quad d|a$
- $c|b \quad \text{and} \quad c|a \rightarrow c|d$

Let $a, b \in \mathbb{Z} \setminus \{0\}$ then $d = gcd(a, b)$ exists and is unique and exist n, m such that $d = ma + nb$ Consider the following set

$$A = \{ma + nb | m, n \in \mathbb{Z} \wedge ma + nb > 0\}$$

The set isn't empty since $a^2 + b^2 \in A$ and so vy the well ordering theorem has a first element which we'll pronounce d.

- $d > 0$ by definition
- 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 $a, b \rightarrow c|d$

NOTE: if $gcd(x, y) = 1$ then we say a and b are coprimes. That's equivalent to saying $\exists m, n \in Z \setminus \{0\} : ma + nb = 1$

2.1 Fundamental theorem of arithmetic

Every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors. We'll prove this by induction.
For $n = 2$ we know that $2 = p_1$. Let $p_1 * \ldots * p_m = 2$. Since 2 is the smallest prime number we know that our factorization was unique.
For $n > 2$ if n is prime then we finished. If $n = n_1 n_2$ we know that $1 < n_1, n_2 < n$ and so by the induction $n_1 = p *_1 * \ldots * p_n$ and $n_2 = p_1^*, \ldots, p_m^*$ then we know that $n = (p_1 * \ldots * p_n)(p_1^* * \ldots *, p_m^*)$ like we wanted. 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.

2.2 $\mathbb{Z}_n^*$

Prove that $\mathbb{Z}_n^*$ which is the set of all coprimes to n from the set $[n]$ coupled with multiplication under modular arithmetic is a group.

3 More About Groups

We'll denote the order of a group G - it's size - as $|G|$, and suppose $g \in G$ and $g^n = e$ we'll call n the order of g and denote $O(g) = n$. If that's never the case we'll denote $|G| = \infty \quad \text{and} \quad O(g) = \infty$

3.1 Abelian Groups

A group $(A, *)$ is abelian if

$$\forall (x, y) \in A^2 : xy = yx$$

The Cayley table for an abelian group is symmetric.

3.2 The Symmetric Group

The symmetric group is denoted as $S(X_n)$ or S_n and is defined on the set $X = \{1, 2, \dots, n\}$ by being the set of all bijections $\sigma : X \to X$ with the operation of function composition.

3.3 Practise

3.3.1 If G is of finite order every element of G also has finite order

Let $|G| = n$ and let $g \in G$ consider the elements $g, g^2, \dots, g^{n+1}$ from the pigeonhole principle we know

$$\exists i \neq j : g^i = g^j \Rightarrow g^{i-j} = e$$

And thus $O(g)$ is finite.

4 Subgroups

Let G be a groups and $H \subseteq G$ then $H \neq \emptyset$ is a subgroup if and only if

- $\forall (x, y) \in H^2 : xy \in H$
- $e \in H$
- $x \in H \Rightarrow x^{-1} \in H$

One condition is not necessary. Think which. If the G is a finite group then two conditions are not necessary. Think why.

4.1 Cyclic Groups

G is a cyclic groups if G has a generator x such that for some $n \in \mathbb{N}$

$$G = \langle x \rangle = \{g : g = x^k \wedge k \in \mathbb{Z}\}$$

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.

5 Lagrange's theorem