Cyclic groups

1. Cyclic groups

Definition

Recall, from Section **??**, the notion of a cyclic subgroup.

Definition 1

A group G is **cyclic** *means there exists $g \in G$ such that $\langle g \rangle = G$.*

Example 1

Often we say "infinite cyclic" to describe groups isomorphic to $\mathbb{Z}$ (see Section **??** for the definition of **isomorphism**).

Question

What is the generator for the group $\mathbb{Z}$?

Example 2

$\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

Proof: Assume, to the contrary, that there exist $a, b \in \mathbb{Z}$ such that $\langle (a, b) \rangle = \mathbb{Z} \times \mathbb{Z}$. Then for any arbitrary element $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ there exists an integer n such that $x = na$ and $y = nb$. There exists another integer, m, such that $(x + 1, y) = (ma, mb)$, which implies

$$\begin{aligned} x + 1 = na + 1 &= ma \\ y = nb &= mb \\ \implies n &= m \\ \implies x + 1 = na + 1 &= na, \end{aligned}$$

which is a contradiction. $\square$

We state the **division algorithm**, as it will prove useful, particularly in Section **??**.

Theorem 1 (Division Algorithm)

Suppose $n \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there exist unique integers q (the **quotient***), and r (the* **remainder***) such that*

$$n = q \cdot d + r \quad \text{and} \quad 0 \leq r < d. \tag{1.1}$$

In this context, d is called the **divisor***.* □

Definition 2

For $n \in \mathbb{N}$, the set of all possible remainders upon division by n,

$$\mathbb{Z}_n := \{0, 1, \dots, n-1\},$$

equipped with the binary operation

$$\begin{aligned} \oplus_n : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z}_n \\ (a, b) &\mapsto r, \text{ as in Equation } (1.1), \\ &\qquad \text{putting } a + b = n \text{ and } n = d, \end{aligned}$$

is called the **group of integers mod n**.

Question (cf. Problem 57)

For fixed $n \in \mathbb{N}$, which elements generate $\mathbb{Z}_n$ (besides 1)?

Example 3 (cf. Problem 56)

The following are "addition tables" for each of the groups $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

$\mathbb{Z}_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\mathbb{Z}_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Proposition 1

Every subgroup of a cyclic group is cyclic. $\square$

Corollary 1

Every subgroup of $\mathbb{Z}$ is cyclic. $\square$

Exercise 1 (cf. Problem 58)

Find one generator for the subgroup

(a) $\langle 2, 3\rangle < \mathbb{Z}$.

(b) $\langle 4, 6\rangle < \mathbb{Z}$.

Exercise 2 (cf. Problem 59)

Prove every cyclic group is abelian.

Exercise 3 (cf. Problem 60)

Use Lagrange's Theorem (Theorem **??**) to show any group of prime order must be cyclic.