Math 2070 Week 3

$\mathbb{Z}_n$, Subgroups, Left Cosets, Index

3.1 The Cyclic Group $\mathbb{Z}_n$

Definition 3.1. *Fix an integer $n > 0$.*

For any $k \in \mathbb{Z}$, let $\overline{k}$ denote the remainder of the division of k by n.

Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. We define a binary operation $+_{\mathbb{Z}_n}$ on $\mathbb{Z}_n$ as follows:

$$k +_{\mathbb{Z}_n} l = \overline{k+l}.$$

Exercise 3.2. *$\mathbb{Z}_n = (\mathbb{Z}_n, +_{\mathbb{Z}_n})$ is a* **cyclic** *group, with identity element 0, and $j^{-1} = n - j$ for any nonzero $j \in \mathbb{Z}_n$.*

3.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**
7. **WeBWorK**
8. **WeBWorK**
9. **WeBWorK**

10. **WeBWorK**
11. **WeBWorK**
12. **WeBWorK**

3.2 Subgroups

Definition 3.3. *Let G be a group. A subset H of G is a* **subgroup** *of G if it satisfies the following properties:*

- **Closure** *If $a, b \in H$, then $ab \in H$.*
- **Identity** *The identity element of G lies in H.*
- **Inverses** *If $a \in H$, then $a^{-1} \in H$.*

In particular, a subgroup H is a group with respect to the group operation on G, and the identity element of H is the identity element of G.

Example 3.4.

- *For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.*
- *$\mathbb{Q}\backslash\{0\}$ is a subgroup of $(\mathbb{R}\backslash\{0\}, \cdot)$.*
- *$\mathrm{SL}(2, \mathbb{R})$ is a subgroup of $\mathrm{GL}(2, \mathbb{R})$.*
- *The set of all rotations (including the trivial rotation) in a dihedral group D_n is a subgroup of D_n.*
- *Let $n \in \mathbb{N}$, $n \geq 2$. We say that $\sigma \in S_n$ is an* **even permutation** *if it is equal to the product of an even number of transpositions. The subset A_n of S_n consisting of even permutations is a subgroup of S_n. A_n is called an* **alternating group**.

Claim 3.5. *A subset H of a group G is a subgroup of G if and only if H is nonempty and, for all $x, y \in H$, we have $xy^{-1} \in H$.*

Proof. Suppose $H \subseteq G$ is a subgroup. Then, H is nonempty since $e_G \in H$. For all $x, y \in H$, we have $y^{-1} \in H$; hence, $xy^{-1} \in H$.

Conversely, suppose H is a nonempty subset of G, and $xy^{-1} \in H$ for all $x, y \in H$.

- **Identity** Let e be the identity element of G. Since H is nonempty, it contains at least one element h. Since $e = h \cdot h^{-1}$, and by hypothesis $h \cdot h^{-1} \in H$, the set H contains e.

- **Inverses** Since $e \in H$, for all $a \in H$ we have $a^{-1} = e \cdot a^{-1} \in H$.
- **Closure** For all $a, b \in H$, we know that $b^{-1} \in H$. Hence, $ab = a \cdot (b^{-1})^{-1} \in H$.

Hence, H is a subgroup of G. □

Claim 3.6. *The intersection of two subgroups of a group G is a subgroup of G.*

Proof. Exercise. □

Theorem 3.7. *Every subgroup of* $(\mathbb{Z}, +)$ *is cyclic.*

Proof. Let H be a subgroup of $G = (\mathbb{Z}, +)$. If $H = \{0\}$, then it is clearly cyclic.

Suppose $|H| > 1$. Consider the subset:

$$S = \{h \in H \,:\, h > 0\} \subseteq H$$

Since a subgroup is closed under inverse, and the inverse of any $z \in \mathbb{Z}$ with respect to $+$ is $-z$, the subgroup H must contain at least one positive element. Hence, S is a non-empty subset of $\mathbb{Z}$ bounded from below.

It then follows from the Least Integer Axiom that exists a minimum element h_0 in S. That is $h_0 \leq h$ for any $h \in S$.

Exercise. Show that $H = \langle h_0 \rangle$.

(*Hint* : The Division Theorem for Integers could be useful here.) □

Exercise 3.8. *Every subgroup of a cyclic group is cyclic.*

3.3 Lagrange's Theorem

Let G be a group, H a subgroup of G. We are interested in knowing how large H is relative to G.

We define a relation $\equiv$ on G as follows:

$$a \equiv b \text{ if} b = ah \text{ for some} h \in H,$$

or equivalently:

$$a \equiv b \text{ if} a^{-1}b \in H.$$

Exercise: $\equiv$ is an **equivalence relation**.

We may therefore partition G into disjoint equivalence classes with respect to $\equiv$. We call these equivalence classes the **left cosets** of H.

Each left coset of H has the form $aH = \{ah \,|\, h \in H\}$.

We could likewise define *right* cosets. These sets are of the form Hb, $b \in G$. In general, the number of left cosets and right cosets, if finite, are equal to each other

Example 3.9. *Let* $G = (\mathbb{Z}, +)$. *Let:*

$$H = 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

The set H *is a subgroup of* G. *The left cosets of* H *in* G *are as follows:*

$$3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z},$$

where $i + 3\mathbb{Z} := \{i + 3k : k \in \mathbb{Z}\}$.

In general, for $n \in \mathbb{Z}$, *the left cosets of* $n\mathbb{Z}$ *in* $\mathbb{Z}$ *are:*

$$i + n\mathbb{Z}, \quad i = 0, 1, 2, \ldots, n - 1.$$

Definition 3.10. *The number of left cosets of a subgroup* H *of* G *is called the* **index** *of* H *in* G. *It is denoted by:*

$$[G : H]$$

Example 3.11. *Let* $n \in \mathbb{N}$, $G = (\mathbb{Z}, +)$, $H = (n\mathbb{Z}, +)$. *Then,*

$$[G : H] = n.$$

Example 3.12. *Let* $G = \mathrm{GL}(2, \mathbb{R})$. *Let:*

$$H = \mathrm{GL}^+(2, \mathbb{R}) := \{h \in G : \det h > 0\}.$$

*(***Exercise:** H *is a subgroup of* G.*)*

Let:

$$s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in G$$

Note that $\det s = \det s^{-1} = -1$.

For any $g \in G$, *either* $\det g > 0$ *or* $\det g < 0$. *If* $\det g > 0$, *then* $g \in H$. *If* $\det g < 0$, *we write:*

$$g = (ss^{-1})g = s(s^{-1}g).$$

Since $\det s^{-1}g = (\det s^{-1})(\det g) > 0$, *we have* $s^{-1}g \in H$. *So,* $G = H \sqcup sH$, *and* $[G : H] = 2$. *Notice that both* G *and* H *are infinite groups, but the index of* H *in* G *is finite.*

Example 3.13. *Let* $G = \mathrm{GL}(2, \mathbb{R})$, $H = \mathrm{SL}(2, \mathbb{R})$. *For each* $x \in \mathbb{R}^\times$, *let:*

$$s_x = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in G$$

Note that $\det s_x = x$.

For each $g \in G$, we have:

$$g = s_{\det g}(s_{\det g}^{-1} g) \in s_{\det g} H$$

Moreover, for distinct $x, y \in \mathbb{R}^\times$, we have:

$$\det(s_x^{-1} s_y) = y/x \neq 1.$$

This implies that $s_x^{-1} s_y \notin H$, hence $s_y H$ and $s_x H$ are disjoint cosets. We have therefore:

$$G = \bigsqcup_{x \in \mathbb{R}^\times} s_x H.$$

The index $[G : H]$ in this case is infinite.