Section 5: Subgroups

First, some notation to keep in line with the book. Because it can be tedious to keep writing $\star$ for the binary operation, we will drop it from the notation and write $a \star b = a + b$ or ab, depending on context. If the operation is additive, we use 0 for the identity and denote a' by $-a$. If the operation is multiplication, we use 1 for the identity and denote a' by a^{-1}.

Using this notation, we can talk about *powers* of elements. For example, for a group G and element a, if the group is multiplicative, a^n will mean $a \star a \star \cdots \star a$ (n times), or $a^n = aa \dots a$. Similarly, if the group is additive, instead of writing $a \star a \star \cdots \star a = a + a + \cdots + a$, we will write na.

Now, a definition from the worksheet on Wednesday if you didn't get to it:

Definition 0.1. The **order** or **size** of a group G, denoted by $|G|$, is the number of elements in G. The **order** of an element $g \in G$ is the minimal positive integer n such that $g^n = e$.

We will explore this throughout today's class!

So far, you may have noticed that some groups we've discussed have been contained in others. For example, $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$. In each of these inclusions, the operation on the larger set induces the operation on the smaller set: if we view two integers n and m as real numbers, adding them together in $\mathbb{R}$ results in the same thing as adding them together in $\mathbb{Z}$.

This is not always true: certainly $\mathbb{Z}_n \subset \mathbb{Z}$, but the group operations $+_n$ and $+$ are not compatible: taking two elements in $\mathbb{Z}_n$ and adding them in $\mathbb{Z}$ does not produce the same result as adding modulo n in $\mathbb{Z}_n$.

This will bring us to the notion of a *subgroup*: a subset of a group that is compatible with the group operation.

Definition 0.2. A subgroup H of a group G is a subset of G that

- is closed under the binary operation in G, i.e. for any $a, b \in H$, $ab \in H$,
- contains the identity element $e \in G$, i.e. $e \in H$, and
- for any $a \in H$, $a^{-1} \in H$.

We use the notation $H \leq G$ to indicate that H is a subgroup of G and $H < G$ to indicate that H is a subgroup of G and $H \neq G$.

Let's do some examples.

Example 0.3. $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$ but $(\mathbb{Q}^\times, \times)$ is not a subgroup of $(\mathbb{R}, +)$: the binary operations are not compatible and it is not closed: for example, 1 and -1 are in $\mathbb{Q}^\times$ but $1 + -1 = 0 \notin \mathbb{Q}^\times$ (it needs to be closed under the binary operation in G)

Example 0.4. Recall from the worksheet: $(S = \{a + bi \in \mathbb{C} \mid a^2 + b^2 = 1\}, \cdot)$ was a group. This is actually a subgroup of $(\mathbb{C}^\times, \cdot)$.

Example 0.5. Also from the worksheet: $(S = \{A \in M_n(\mathbb{R}) | \det A \neq 0\}, \cdot)$ was a group. This is a special group and has a name.

Definition 0.6. The **general linear group** $\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) | \det A \neq 0\}$.

The subset $H = \{A \in \mathrm{GL}_n(\mathbb{R}) | \det A = 1\}$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Definition 0.7. For any group G, the subset $\{e\}$ is a subgroup called the **trivial** subgroup. The subset G is a subgroup called the **improper** subgroup. Any subgroup $H < G$ is called a **proper** subgroup.

Example 0.8. $\{0, 2\}$ is a subgroup of $\mathbb{Z}_4$ but $H = \{0, 3\}$ is not because it is not closed under $+_4$: $3 +_4 3 = 2$, which is not in H. In fact, if we keep adding 3 to itself, we get that $3 +_4 3 = 2$; $3 +_4 3 +_4 3 = 1$; $3 +_4 3 +_4 3 +_4 3 = 0$, and see that if we keep adding 3 to itself, we eventually run over all elements of $\mathbb{Z}_4$. The mathematical term for this is "3 generates $\mathbb{Z}_4$"; we will define some notions before getting here.

We'll prove this theorem next time:

Theorem 0.9. *Let G be a group and let $a \in G$. Then, $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and it is the smallest subgroup of G containing a.*

Definition 0.10. Let G be a group and $a \in G$. Then, $\{a^n \mid n \in \mathbb{Z}\}$ is called the **cyclic subgroup of G generated by** a. We denote this by $\langle a \rangle$.