Lecture 4. groups *September 26, 2025*

1 Groups

1.1 Definitions

In this course we study one of the most fundamental objects in mathematics: groups.

Definition 1. A *group* is a set S together with a map

$$m : S \times S \to S$$

called a *law of composition*. Writing ab for $m(a, b)$, the law of comp. has to satisfy three axioms:

i. (existence of identity): $\exists e \in S$, called the identity, s.t. $ae = ea = a \forall a \in S$;

ii. (existence of inverses): for any element $a \in S \exists b \in S \mid ab = ba = e$, we usually denote this as a^{-1} or $-a$;

iii. (the associative law): for any three elements $a, b, c \in S$ we have

$$a(bc) = (ab)c.$$

This results in some immediate concequnces, namely the uniqueness of the identity element and the *cancellation law*. The proofs are trivial.

We usually represent groups in the form G, as a simplified for (G, m) or $\langle G, m\rangle$ (the latter being less common). The cardinality of the set of a given group is called the order of said group: i.e., the cardinality of the group $|G|$ is the cardinality of the set G (the use of the same notation for groups and sets can be confusing at times but are context dependent).

We have an additional type of group that naturally appears from any of the common number systems $\mathbb{R}, \mathbb{N}, \ldots$, called an abelian group.

Definition 2. An abelian group is a group that is commutative; that is to say:

$$\forall a, b \in G,\ ab = ba.$$

This in general is not true for all groups, as symmetric groups and dihedral groups do not satisfy this definition (you will see more on this later). Additionally, there are a few other structures that arise when we alter the axioms of a group: remove the second axiom and you have a *monoid*, remove the third axiom and you have a *semigroup*. They will appear a few times but not often (for now).

1.2 Constructions

Definition 3. The product of two groups is given by $G \times H$, where the set is the Cartesian product adn the law of composition is given termwise:

$$G \times H = \{(a, b) \mid a \in G, b \in H\} \,\&\, (a, b) \cdot (a', b') \coloneqq (a \cdot a', b \cdot b').$$

We also may use $G \oplus H$, but this is usually more case specific.

Products of greater than two groups, even infinite groups, is much the same; given the groups $G_1, \ldots, G_n$ we can define a product,

$$G_1 \times \ldots \times G_n \coloneqq \{(a_1, \ldots, a_n) \mid a_i \in G_i\},$$

with the law of composition given by

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) \coloneqq (a_1 \cdot b_2, \ldots, a_n \cdot b_n).$$

We ue products and sums to denote infinite and finite group products, respectively:

$$\prod_{i=1}^{\infty} G_i \,\&\, \bigoplus_{i=1}^{n} G_i.$$

At times we may have a group G^n such as $\mathbb{R}^n$, etc, where each G_n contains n-tuples of its elements.

The final note is on groups of polynomials with real coefficients, denoted $\mathbb{R}[x]$. We use

$$\mathbb{R}[x] \coloneqq \{a_0 + a_1 x + a_2^2 \ldots + a_n x^n \mid n \in \mathbb{N} \text{ and } a_i \in \mathbb{R}\}$$

for finite polynomials as a direct sum, and the following for infinite polynomials as a direct product (i.e., the group of polynomial power series),

$$\mathbb{R}[[x]] \coloneqq \{a_0 + a_1 x + a_2^2 \ldots \mid a_i \in \mathbb{R}\}.$$