LECTURE 21

Definition and Examples of Groups

Definition 21.1. *A **group** is a nonempty set G equipped with a binary operation $* : G \times G \to G$ satisfying the following axioms: ı(i) Closure: if $a, b \in G$, then $a * b \in G$. ı(ii) Associativity: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$. ı(iii) Identity: there is an element $e \in G$, such that $a * e = e * a = a$ for all $a \in G$. ı(iv) Inverse: for each element $a \in G$, there is an element $b \in G$ such that $a * b = e = b * a$.*

Definition 21.2. *A group G is said to be **abelian** (or **commutative**) if $a * b = b * a$ for all $a, b \in G$.*

Examples:

1. $\mathbb{Z}$ is an abelian group under addition.

2. $\mathbb{R} - 0$ is an abelian group under multiplication.

3. $M_2(\mathbb{R})$ is an abelian group under the addition of matrices.

4. The set

$$GL(2) = \{M \in M_2(\mathbb{R}) \mid det\ M \neq 0\}$$

is a non-commutative group under matrix multiplication.

5. Every ring is abelian group under addition.

6. Every division ring is a group under multiplication.

7. Every field is a abelian group under multiplication.

8. The set of bijections f from a set S onto itself is a group.

9. Permutation Groups.

Let $T = \{1, 2, 3\}$ and consider the six possible permutations of the elements of T.

$$P_3 = \{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\}$$

To each element $(i, j, k) \in P_3$ of S_3 there corresponds a map $\sigma_{ijk} : P \to P$ defined as follows; σ_{ijk} maps any $(a, b, c) \in P$ to the element of P for which a is the i^{th} component, b is the j^{th} component, and c is the k^{th} component

$$\begin{aligned} \left(\sigma_{ijk}(a, b, c)\right)_i &= a \\ \left(\sigma_{ijk}(a, b, c)\right)_j &= b \\ \left(\sigma_{ijk}(a, b, c)\right)_k &= c \end{aligned}$$

Since $i \neq j \neq k$ we easily conclude that these maps are bijective. In fact, every bijection from T to T must correspond to a σ_{ijk} for some $(i, j, k) \in S_3$. Since the composition of any two bijective functions is itself bijective the set of maps

$$S_3 = \{\sigma_{ijk} \mid (i, j, k) \in P_3\}$$

is closed under functional composition. Note also that the function σ_{123} acts like an identity transformation with respect to functional composition; i.e.,

$$(\sigma_{ijk} \circ \sigma_{123})(1,2,3) = \sigma_{ijk}(1,2,3)$$

and

$$(\sigma_{123} \circ \sigma_{ijk})(1,2,3) = \sigma_{123}(i,j,k) = (i,j,k) = \sigma_{ijk}(1,2,3) .$$

and so

$$\sigma_{123} \circ \sigma_{ijk} = \sigma_{ijk} = \sigma_{ijk} \circ \sigma_{123} \qquad , \quad \forall\, \sigma_{ijk} \in S_3 \quad .$$

Note also that because element of S_3 is a bijection from T to T, and every bijection from T to T can be regarded as an element of T, every element of S_3 has an inverse in S_3. Finally, we note that the composition of maps is associative. We have thus verified that the set S_3 has the structure of a group when the group composition law is defined as the composition of functions.

Consider the composition of $\sigma_{213} \circ \sigma_{312}$, we have

$$(\sigma_{213} \circ \sigma_{312})(1,2,3) = \sigma_{213}(2,3,1) = (3,2,1)$$

Thus,

$$\sigma_{213} \circ \sigma_{312} = \sigma_{132} \quad .$$

Now consider the composition in the opposite order

$$(\sigma_{312} \circ \sigma_{213})(1,2,3) = \sigma_{312}(2,1,3) = (1,3,2)$$

so

$$\sigma_{312} \circ \sigma_{213} = \sigma_{132} \quad .$$

This example generalizes as follows. Let n be a fixed positive integer and let T be the set $\{1,2,3,\ldots,n\}$, and let S_n denote the set of all bijective maps from T to T. Each element $\sigma \in S$ sends a given $i \in T$ to an element $\sigma(i) \in T$.

9. Symmetry Groups of Regular Polygons

D_4 is the group of all rotations and reflections of a square such that the image of the transformation lies over original square. D_4 consists of rotations of 0, 90, 180 and 270 degrees, and reflections across the x-axix, the y-axis, the line $y = x$, and the line $y = -x$.

More generally, D_n is the group of symmetries of a regular polygon with n sides.

Example

The group D_3 is the set of all symmetries of an equilateral triangle. It consists of rotations of 0, 120, and 240 degrees, and reflections about the perpendicular bisectors of each side. D_3 thus consists of 6 elements.

Definition 21.3. *A group G is said to be* ***finite*** *if it has only a finite number of elements. If G is finite, then the number of elements of G is called the* ***order*** *of G and is denoted $|G|$.*

.

Remark: each of the rings $\mathbb{Z}_n$ is a finite commutative group under addition.

Example

Let U_n denote the set of units in $\mathbb{Z}_n$; i.e.,

$$U_n = \{a \in Z_n \mid \exists b \in Z_n \text{ s.t.} ab = [1]_n\} \quad .$$

Then U_n is a finite commutative group under multiplication. According to Corollary 2.9, U_n consists of all $a \in Z_n$ such that $GCD(a, n) = 1$. Thus, for example, the group of units in $\mathbb{Z}_8$ is

$$U_n = \{1, 3, 5, 7\} \quad .$$

THEOREM 21.4. *The G and H be groups. Define an operation $*$ on the Cartesian product $G \times H$ by*

$$(g, h) * (g', h') = (g * g', h * h') \quad .$$

Then $G \times H$ is a group. If G and H are abelian, then so is $G \times H$. If G and H are finite, then so is $G \times H$, and $|G \times H| = |G|\,|H|$.