1 Group Theory

1.1 Basic Axioms and Examples

Definition.

1. A *binary operation* $\star$ on a set G is a function $\star\colon G \times G \to G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$.

2. A binary operation $\star$ on a set G is associative if for all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.

3. If $\star$ is a binary operation on a set G we say elements a and b of G *commute* if $a \star b = b \star a$. We say $\star$ (or G) is *commutative* if for all $a, b \in G$, $a \star b = b \star a$.

Proposition 1. If G is a group under the operation $\cdot$, then

1. The identity of G is unique

2. for each $a \in G$, a^{-1} is uniquely determined

3. $(a^{-1})^{-1} = a$ for all $a \in G$

4. $(a \cdot b)^{-1} = (b^{-1}) \cdot (a^{-1})$

5. for any $a_q, a_2, \ldots, a_n \in G$ the value of $a_1 a_2 \cdots a_n$ is independent of how the expression is bracketed

Proposition 2. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in G, i.e.,

1. if $au = av$, then $u = v$, and

2. if $ub = vb$, then $u = v$.

Definition. For G a group and $x \in G$ define the *order* of x to be the smallest positive integer n such that $x^n = 1$, denoted $|x|$. If there is no such integer than we define the order of x to be infinity.

1.6 Homomorphism and Isomorphisms

Definition. Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi\colon G \to H$ such that $\phi(x \star y) = \phi(x) \diamond \phi(y)$, for all $x, y \in G$ is called a *homomorphism.* Moreover, if ϕ is bijective it is called an *isomorphism* and we say that G and H are *isomorphic* or of the same *isomorphism type*, written $G \cong H$.

Note. If $\phi\colon G \to H$ is an isomorphism then

1. $|G| = |H|$

2. G is abelian if and only if H is abelian

3. for all $x \in G, |x| = |\phi(x)|$

1.7 Group Actions

Definition. A *group action* of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and
2. $1 \cdot a = a$ for all $a \in A$.

Note. Let the group G act on the set A. From each fixed $g \in G$ we get a map σ_g defined by

$$\sigma_g \colon A \to A$$
$$\sigma_g(a) = g \cdot a.$$

The following are true

1. for each fixed $g \in G$, σ_g is a permutation of A, and
2. the map from G to S_A defined bt $g \mapsto \sigma_g$ is a homomorphism. Moreover this map is called the *permutation representation* associated to the given action.

Note. As a consequence of the above remark, if $\phi \colon G \to S_A$ is a homomorphism (here S_A is the symmetric group on the set A), then the map from $G \times A$ to A defined by

$$g \cdot a = \phi(g)(a) \text{for all} g \in G, \text{ and all} a \in A$$

is a group action of G on A.