Groups

Sasha Krassovsky

November 13, 2018

Definition. A group is a pair $G = (G, \star)$ consisting of a set G and a binary operation $\star$ on G such that:

- G has an identity 1_G or just 1 such that

$$\forall g \in G, 1_G \star g = g \star 1_G = g$$

- $\star$ is associative, so

$$\forall a, b, c \in G, (a \star b) \star c = a \star (b \star c)$$

- Every element in G has an inverse. That is

$$\forall g \in G, \exists h \in G, g \star h = h \star g = 1_G$$

Remark. Notice that G is closed under $\star$ implicitly. That is, $\forall g, h \in G, g \star h \in G$.

Definition. A group is abelian if its operation is commutative ($a \star b = b \star a$). Otherwise, it is non-abelian.

Properties of Groups:

- Let G be a group.
  1. The identity 1_G is unique.
  2. The inverse of any element $g \in G$, g^{-1} is unique.
  3. For any $g \in G$, $(g^{-1})^{-1} = g$.
- Let G be a group and $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.
- Let G b ea group and pick a $g \in G$. Then the map $G \to G$ given by $x \mapsto gx$ is a bijection.

Definition. Let $G = (G, \star)$ and $H = (H, *)$ be groups. A bijection $\phi : G \to H$ is called an isomorphism if

$$\forall g_1, g_2 \in G, \phi(g_1 \star g_2) = \phi(g_1) * \phi(g_2)$$

If there exists an isomorphism from G to H, then G and H are isomorphic, i.e. $G \cong H$.

Remark. $\cong$ is an equivalence relation (i.e. it is reflexive, symmetric, and transitive).

Definition. The order of a group G is the number of elements in G, denoted $|G|$. A group is a finite group if $|G|$ is finite.

Definition. The order of an element $g \in G$ is the smallest positive integer n such that $g^n = 1_G$ or ∞ if no such n exists. Denoted $\operatorname{ord} g$.