Groups

Sasha Krassovsky

November 16, 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**.

Definition. A mapping is a **bijection** if it is injective (one-to-one) and surjective (onto).

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 $\operatorname{ord} g$.

Fact. *If $G^n = 1_G$ then $\operatorname{ord} g | n$.*

Fact. *Let G be a finite group. Then for all $g \in G$, $\operatorname{ord} g$ is finite.*

Lagrange's Theorem For Orders. *Let G be any finite group. Then* $\forall x \in G, x^{|G|} = 1_G$ *for any* $x \in G$. *This is the general case of Fermat's Little Theorem.*

Definition. The **General Linear Group** of degree n, denoted GL_n is the set of invertible $n \times n$ matrices along with the operation of matrix multiplication. To specify what is in each matrix, we give it an argument. For example, the GL over $\mathbb{R}^{n\times n}$ is denoted $\mathrm{GL}_n(\mathbb{R})$.

Definition. Let $G = (G, \star)$ be a group. A group $H = (H, \star)$ is a **subgroup** of G if $H \subseteq G$. H is called a **proper subgroup** of G if $H \neq G$.

Remark. If H is a subgroup of G, the binary operation is the same. Therefore, to specify H, you need only provide its elements, not its operation.

Definition. The **Special Linear Group** of degree n over a field F, denoted $\mathrm{SL}_n(F)$ is the subgroup of $\mathrm{GL}_n(F)$ such that $\forall x \in \mathrm{SL}_n(F), \det(x) = 1$.

Definition. Let G be a group. Let S be a subset of G. The subgroup **generated** by S, $\langle S \rangle$ is the set of elements which can be written as a finite product of elements in S and their inverses. If $\langle S \rangle = G$, then S is a set of **generators** for G.

Definition. The **group presentation** of a group is an expression specifying a set of generators and **relations** between the generators. For example,

$$\mathbb{Z}_{100} = \langle x | x^{100} = 1 \rangle$$

Remark. Determining if a group is finite from its presentation is undecideable.

Definition. Let $G = (G, \star)$ and $H = (H, *)$ be groups. A **group homomorphism** is a map $\phi : G \to H$ such that

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

Notice that this is is the same as an isomorphism, only lacking the requirement that ϕ be a bijection.

Definition. The **trivial homomorphism** $G \to H$ sends every element of G to 1_H.

Fact. *Let* $\phi : G \to H$ *be a homomorphism. Then* $\phi(1_G) = 1_H$ *and* $\phi(g^{-1}) = \phi(g)^{-1}$.

Definition. The **kernel** of a homomorphism $\phi : G \to H$ is a subgroup of G such that

$$\ker \phi = \{g \in G : \phi(g) = 1_H\}$$

Definition. The **image** of a homomorphism $\phi : G \to H$ is a subgroup of G such that

$$\operatorname{im} \phi = \phi(G) = \{\phi(x) : x \in G\}$$

Proposition. *The map* ϕ *is injective if and only if* $\ker \phi = 1_G$.

Definition. Let H be any subgroup of G. A set of the form gH for any $g \in G$ is called a **left coset** of H.

Remark. It is possible for $g_1 N = g_2 N$, even if $g_1 \neq g_2$.

Remark. Given cosets $g_1 H$ and $g_2 H$, the map $x \mapsto g_2 g_1^{-1}$ is a bijection, so all cosets have equal cardinality.

Definition. A subgroup N of G is called **normal** if it is the kernel of some surjective homomorphism. We write this as $N \trianglelefteq G$.

Definition. Let $N \trianglelefteq G$. Then the **quotient group**, denoted G/N is the group defined such that:

- The elements of G/N will be the left cosets of N.
- Let $g_1, g_2 \in G$. Then $(g_1 N) \cdot (g_2 N) = (g_1 g_2) N$.

Remark. We can define an equivalence relation $\sim_N$ on G by saying $x \sim_N y$ for $\phi(x) = \phi(y)$. $\sim_N$ divides G into equivalence classes which are in bijection to G/N.

Lagrange's Theorem. *Let G be a finite group, and let H be any subgroup. Then $|H|$ divides $|G|$.*

Proof. Cosets of H have the same size and form a partition on G. If n is the number of cosets, then $n|H| = |G|$, so $|H|$ divides $|G|$. □

Remark. If G is finite and $N \trianglelefteq G$, then $|G/N| = |G|/|N|$.

Remark. For $g_1N \cdot g_2N = (g_1g_2)N$ to hold, N must be normal to G because this condition lets us pick any $g_1, g_2 \in N$ and still end up with the same coset.

Proposition. *Suppose $\phi : G \mapsto K$ is a homomorphism with $H = \ker \phi$. If $h \in H, g \in G$, then $ghg^{-1} \in H$.*

Algebraic Condition for Normal Subgroups. *Let H be a subgroup of G. Then the following are equivalent:*

- $H \trianglelefteq G$
- $\forall g \in G, h \in H, ghg^{-1} \in H$

First Isomorphism Theorem. *Let G, H be groups and let $\phi : G \to H$ be a homomorphism. Then:*

- $\ker \phi \trianglelefteq G$
- $\operatorname{im} \phi \leq H$
- $\operatorname{im} \phi \cong G/\ker(\phi)$

Definition. Let X be a set and G be a group, and let $x \in X, g \in G$. A **group action** is a binary operation $\cdot : G \times X \to X$ that sends x go $g \cdot x$. It satisfies:

- $\forall x \in X, \forall g_1, g_2 \in G, (g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$
- $\forall x \in X, 1_G \cdot x = x$

Definition. Given a group action G on X, define an equivalence relation $\sim$ on X such that $x \sim y$ if $x = g \cdot y$ for some $g \in G$. The equivalence classes under $\sim$ are **orbits**, denoted O. In other words, the orbit is everything that can be reached from x by an action of something in G.

Definition. The **stabilizer** of a point $x \in X$, denoted Stab_G, is the set of $g \in G$ which fix x. In other words, the set of elements of G which don't move when they act on x.

$$\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$$

Orbit-Stabilizer Theorem. *Let O be an orbit, and pick any $x \in O$. Let $S = \mathrm{Stab}_G(x)$ be a subgroup of G. There is a natural bijection between O and left cosets.*

$$|O||S| = |G|$$

In particular, the stabilizers of each $x \in O$ have the same size.

Proof. Every coset of gS specifies an element of O, namely $g \cdot x$. Since there are $|O|$ partitions of G and each one is of size $|S|$, the result follows. □

Burnside's Lemma. *Let G act on a set X. The number of orbits of the action is equal to*

$$\frac{1}{|G|} \sum_{g \in G} |\operatorname{FixPt} g|$$

where $\operatorname{FixPt} g$ *is the set of points $x \in X$ such that $g \cdot x = x$.*

Definition. A common action is **conjugation**. G acts on itself:

$$C_G : G \times G \to G$$
$$C_G(g, h) = ghg^{-1}$$

Definition. The **conjugacy classes** of a group G are the orbits of G under the conjugacy action.

Definition. Let G be a group. The **center** of G, denoted $Z(G)$ is the set of elements of $x \in G$ such that $xg = gx$ for every $g \in G$. $Z(G)$ is a subgroup of G.

$$Z(G) = \{x \in G : gx = xg \forall g \in G\}$$

Remark. If G is abelian, then the conjugacy classes all have sizes one.