

# Groups

Sasha Krassovsky

November 14, 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  $G$  be a group and pick a  $g \in G$ . Then the map  $G \rightarrow G$  given by  $x \mapsto gx$  is a bijection.

**Definition.** Let  $G = (G, \star)$  and  $H = (H, *)$  be groups. A bijection  $\phi : G \rightarrow H$  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  $\infty$  if no such  $n$  exists. Denoted  $\text{ord } g$ .

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

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

**Lagrange's Theorem For Orders.** Let  $G$  be any finite group. Then  $\forall x \in G, x^{|G|} = 1_G$ . 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  $GL_n(\mathbb{R})$ .

**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  $SL_n(F)$  is the subgroup of  $GL_n(F)$  such that  $\forall x \in SL_n(F), \det(x) = 1$ .

**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 undecidable.

**Definition.** Let  $G = (G, \star)$  and  $H = (H, *)$  be groups. A **group homomorphism** is a map  $\phi : G \rightarrow H$  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 the same as an isomorphism, only lacking the requirement that  $\phi$  be a bijection.

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

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

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

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

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

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

**Proposition.** The map  $\phi$  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  $g_1H = g_2H$ , even if  $g_1 \neq g_2$ .

*Remark.* Given cosets  $g_1H$  and  $g_2H$ , the map  $x \mapsto g_2g_1^{-1}x$  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  $(g_1N) \cdot (g_2N) = (g_1g_2)N$ .

*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  $|G|$ .

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