

**Definition 1 (Group).** A set  $G$  with a binary operation  $\star : G \times G \rightarrow G$  is a group if the following axioms are satisfied:

1. Associativity:  $(a \star b) \star c = a \star (b \star c)$  for every  $a, b, c \in G$ .
2. Unit (or Identity): There exists an  $e \in G$  such that  $e \star a = a \star e = a$  for each  $a$  in  $G$ .
3. Inverse: For each  $a \in G$  there is a  $b \in G$  such that  $a \star b = b \star a = e$ .

**Definition 2 (Abelian/Commutative).** A group  $G$  is abelian or commutative if  $a \star b = b \star a$  for all  $a \in G$ .

**Definition 3 (The group  $\mathbb{Z}/n\mathbb{Z}$ ).** The group  $\mathbb{Z}/n\mathbb{Z}$  is the set  $\{0, 1, \dots, n-1\}$ . That is, the possible (integer) remainders upon dividing by  $n$ . Recall that the remainder is the smallest number that you subtract from the original number so that it becomes divisible by  $n$ .

**Definition 4 (Order of a group, order of an element of a group).** Let  $G$  be a group. We call  $|G|$  the order of  $G$  (i.e. the number of elements in  $G$ ). Further, the least  $d > 0$  such that  $g^d = 1$  is called the order of  $g \in G$ .

**Definition 5.** (Cycle, Cycle Decomposition, Length,  $k$ -Cycle) A cycle is a string of integers which represents the element of  $S_n$  which cyclically permutes these integers (and fixes all other integers). The product of all the cycles is called the cycle decomposition. The length of a cycle is the number of integers which appear in it. A cycle of length  $k$  is called a  $k$ -cycle.

**Definition 6 (Subgroup).** A subset  $H$  of a group  $G$  is called a subgroup of  $G$  if the following axioms are satisfied

1. Identity:  $1 \in H$  (we could also write  $1_G \in H$ ).
2. Closed under products:  $h_1 h_2 \in H$  for all  $h_1, h_2 \in H$  (in words, the binary operation of  $G$  applied to elements of  $H$  keeps products in  $H$ ).
3. Closed under inverses:  $h^{-1} \in H$  for all  $h \in H$ .

In this case we write  $H \leq G$ . Observe that  $H$  is indeed a group.

**Definition 7 (Homomorphism).** Let  $G, H$  be groups. A function  $\phi : G \rightarrow H$  is a homomorphism if for every  $a, b \in G$ , we have

$$\phi(ab) = \phi(a)\phi(b) \quad (1)$$

Note the the product  $ab$  on the left is computed in  $G$  and the product  $\phi(x)\phi(y)$  is computed in  $H$ .

**Definition 8 (Kernel).** Let  $\phi : G \rightarrow H$  be a homomorphism. Then

$$\ker(\phi) = \{g \in G : \phi(g) = 1\} \quad (2)$$

(note that 1 is the identity of  $H$ ).

**Definition 9 (Coset).** Let  $H \leq G$  and fixed  $a \in G$ . Let

$$\begin{aligned} aH &= \{ah | h \in H\} \\ Ha &= \{ha | h \in H\} \end{aligned}$$

These sets are called a left coset and right coset of  $H$  in  $G$ .

Write  $G/H$  for the set of left cosets  $\{aH | a \in G\}$ .

**Definition 10 (Index).** If  $G$  is a group (possibly infinite) and  $H \leq G$ , the number of left cosets of  $H$  in  $G$  is called the index of  $H$  in  $G$  and is denoted by  $|G : H|$ . Alternatively,  $|G : H| = |G/H| = |\{aH | a \in G\}|$ . If  $G$  is finite, the  $|G : H| = \frac{|G|}{|H|}$ .

**Definition 11 (Normal Subgroup).** We say that a subgroup  $H$  of  $G$  is normal if  $aH = Ha$  for every  $a \in G$ . Write  $H \trianglelefteq G$ . This means that the left and right cosets of a group of equivalent.

**Definition 12 (Cyclic Group).** A group  $H$  is cyclic if  $H$  can be generated by a single element, i.e., there is some element  $x \in H$  such that  $H = \{x^n | n \in \mathbb{Z}\}$ . Write  $H = \langle x \rangle$  and say  $H$  is generated by  $x$ .

An alternative definition is: Let  $G$  be a group and fix  $x \in G$ . Let  $H$  be the subset of  $G$  that contains all the powers of  $x$ . Then notice that  $H = \{x^n | n \in \mathbb{Z}\}$  is a subgroup of  $G$  (the identity element must be in  $H$  since  $x^0 = 1$ ,  $H$  is closed under products since adding exponents will keep us in  $H$ , and the inverse of  $x^n$  is  $x^{-n}$ , which is also in  $H$ ). We call  $H$  the subgroup of  $G$  generated by  $x$ ,  $H = \langle x \rangle$ , and  $H$  is cyclic.

**Definition 13 (Dihedral Group,  $D_n$ ).** In general,  $D_n$  is a group with  $2n$  elements, where the binary operation is composition. It contains two types of symmetries:

1. The rotation  $\rho$  is  $\frac{2\pi}{n}$  radians clockwise. The set of all rotations is  $\langle \rho \rangle = \{1, \rho, \rho^2, \dots, \rho^{n-1}\}$ .
2. Let  $\epsilon$  be a vertical mirror symmetry. Then the set of all mirror symmetries is  $\{\epsilon, \epsilon\rho, \epsilon\rho^2, \dots, \epsilon\rho^{n-1}\}$ .

**Definition 14 (Quotient Group).** Let  $G$  be a group and  $N \trianglelefteq G$  (that is,  $N$  is a normal subgroup of  $G$ ). Let  $G/N = \{gN | g \in G\}$  be the set of left cosets of  $N$  in  $G$ . Then the quotient group of  $G$  by  $N$  is the group  $(G/N, \cdot)$ , where  $\cdot$  is the binary operation on  $G/N$  defined for all  $g_1N, g_2N \in G/N$  by  $g_1Ng_2N = g_1g_2N$ .

**Definition 15 (Action).** An action of a group  $G$  on  $X$  (or we say  $G$  acts on  $X$ ) is a function  $G \times X \rightarrow X$ ,  $(g, x) \rightarrow gx$  where

1.  $1_Gx = x \quad \forall x \in X$
2.  $g(hx) = (gh)x \quad \forall g, h \in G, \forall x \in X$

**Definition 16 (Orbit).** Given  $x \in X$  the orbit of  $x$  is

$$O(x) = O_x = \{gx | g \in G\} \quad (3)$$

This is the set of all elements that can be reached from  $x$  by applying elements from  $G$ .

**Definition 17 (Stabilizer, Isotropy Subgroup).** Let  $X$  be a  $G$ -set and  $x \in X$ . The stabilizer of  $x$  is

$$G_x = \text{Stab}_G(x) = \{g \in G | gx = x\} \quad (4)$$

also called the isotropy subgroup of  $x$ .

**Definition 18 (Transitive action).** We say that an action of  $G$  on  $X$  is transitive if for every  $x, y \in X$ , there is an element  $g \in G$  such that  $gx = y$ . In words, this means that we can arrive at  $y$  from  $x$  by applying an element from  $G$ .

**Definition 19 (Action induces equivalence relation).** The action of any group  $G$  on  $X$  induces an equivalence relation by saying  $x \sim y$  if there exists a  $g \in G$  such that  $gx = y$ .

**Definition 20 (Conjugation action, conjugacy classes, conjugate).** Consider the action of  $G$  on itself by  $g(x) = gxg^{-1}$ . We call this the conjugation action. The equivalence classes created by this action are called the conjugacy classes of  $G$ . We say that two elements in  $x, y \in G$  are conjugate if they belong to the same conjugacy class.

**Definition 21 (Fixed points).** For any element  $g \in G$ , let  $X^g = \{x \in X | gx = x\}$ . In words, this is the set of all elements in  $X$  such that  $g$  acts on them like the identity.

**Definition 22 (Free, faithful action).** Let  $G$  be a group that acts on a set  $X$ .

1. The action is said to be faithful if for all  $x \in X$

$$gx = x \implies g = 1 \quad (5)$$

Thus the only element that acts like the identity is actually the identity  $g = 1$ . Alternatively,

$$\cap_{x \in X} G_x = \{1\} \quad (6)$$

2. The action is free if for all  $g \in G$  and for all  $x \in X$

$$gx = x \implies g = 1 \quad (7)$$

Alternatively, this means all stabilizers are trivial. We have that for all  $x \in X$ ,

$$G_x = \{1\} \quad (8)$$

Or, any element which has a fixed point is the identity element.

**Definition 23 (Coprime).** An integer  $a$  is coprime to  $n$  if the only positive divisor of both  $a$  and  $n$  is 1.

**Definition 24  $((\mathbb{Z}/n\mathbb{Z})^\times)$ .**

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{1 \leq a \leq n-1 | a \text{ coprime to } n\} \quad (9)$$

$n \geq 2$ . This is called the multiplicative group of integers modulo  $n$ , where the binary operation is multiplication and taking the remainder upon dividing by  $n$ .

**Definition 25 (Permutation representation of action).** Let  $G$  be a group that acts on  $\{1, \dots, n\}$ . Associated to the action is a homomorphism  $\lambda : G \rightarrow S_n$ , defined by

$$\lambda(g)(i) = gi \quad (10)$$

where the RHS is the action of  $g$  on  $i$ ,  $i \in \{1, \dots, n\}$ .

**Definition 26 ( $p$ -Group).** Let  $p$  be a prime number.  $G$  is a  $p$ -group if  $|G|$  is a power of  $p$ .

**Definition 27 (Ring).** Let  $A$  be a set with two binary operations: addition and multiplication.  $A$  is called a ring if:

1.  $A$  is an abelian group under addition:
  - (a) Addition associative: For all  $a, b, c \in A$ ,  $(a + b) + c = a + (b + c)$ .
  - (b) Additive identity: There exists a  $0 \in A$  such that for all  $a \in A$ ,  $a + 0 = 0 + a = a$ .
  - (c) Additive inverse: For all  $a \in A$ , there exists a  $b \in A$  such that  $a + b = b + a = 0$ .
  - (d) Addition commutative: For all  $a, b \in A$ ,  $a + b = b + a$ .
2. Multiplication associative: For all  $a, b, c \in A$ ,  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
3. Multiplicative identity: There exists  $1 \in A$  such that for all  $a \in A$ ,  $1 \cdot a = a \cdot 1 = a$ .
4. Multiplication distributive: For all  $a, b, c \in A$ 
  - (a)  $a \cdot (b + c) = a \cdot b + a \cdot c$ .
  - (b)  $(b + c) \cdot a = b \cdot a + c \cdot a$ .

**Definition 28 (Commutative Ring).** A ring is called commutative if for all  $a, b \in A$ ,  $ab = ba$ .

**Definition 29 (Field).** A commutative ring is called a field if for all  $a \neq 0$ ,  $a \in A$ , there exists a  $b \in A$  such that  $ab = ba = 1$ .