Group Theory

1 Definitions and first examples

A group $(G, *)$ is a set G equipped with an operation $(x, y) \in G \times G \mapsto x * y \in G$ satisfying the axioms of
G_1 – associativity: $\forall\, x, y, z \in G, x * (y * z) = (x * y) * z$,
G_2 – existence of an identity: $\exists e \in G : \forall\, x \in G, e * x = x * e = x$,
G_3 – existence of inverses: $\forall\, x \in G, \exists x' \in G : x * x' = x' * x = e$.
The axioms imply the uniqueness of an identity element and of inverses. One frequently uses either the additive notation with $+$ for $*$, 0 for the identity element, and $-x$ for the inverse (e.g. $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) or the multiplicative notation with $\cdot$ (or nothing at all) for $*$, 1 for the identity element, and x^{-1} for the inverse (e.g. $G = \mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$). Other examples include $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ when p is prime — see *Modular Arithmetic* . All the examples mentioned so far were commutative (aka abelian) groups, meaning that $x * y = y * x$ for all $x, y \in G$. The symmetric group S_n, i.e., the set of all permutations of $[1 : n]$ equipped with the operation of composition, is an example of a noncommutative group.

A subgroup of a group $(G, *)$ is a subset H of G which forms a group when equipped with the operation $*$. When H is a subset of G, it forms a subgroup of $(G, *)$ if and only if

$$xy^{-1} \in H \qquad \text{whenever } x, y \in H. \tag{1}$$

For a subset X of a group G, the smallest subgroup of G containing X, i.e., the intersection of all subgroups of G containing X, is called the subgroup generated by X. In particular, given $x \in G$, the subgroup generated by $\{x\}$ (or equivalently by $\{x^n, n \in \mathbb{Z}\}$) is called the cyclic group generated by x.

2 Finite Groups

Given a group $(G, *)$, if the set G is a finite, then its cardinality is called the order of G. The order of the cyclic group generated by $x \in G$ is called the order of x — it is the smallest positive integer m such that $x^m = 1$.

Lagrange theorem states that the order of any subgroup H of a group G divides the order of G (in particular, a group of prime order has no nontrivial subgroups). The argument consists in considering the sets $xH := \{xh, h \in H\}$: two sets xH and $x'H$ are either disjoint or equal, thus, they all have the same size m (which is the order of H), and if q is the number of those sets, one has $n = qm$.

Applying Lagrange theorem to cyclic subgroups generated by one element of a group G of order n, one derives in particular that $x^n = 1$ for every element $x \in G$. For instance, any permutation σ of $[1 : n]$ satisfies $\underbrace{\sigma \circ \sigma \circ \cdots \circ \sigma}_{n! \text{times}} = \mathrm{id}$, since the order of S_n is $n!$.

The product of groups $\{(G_i, *_i), i \in I\}$ is the set $\prod_{i\in I} G_i$ equipped with the operation $*$ as defined by

$$\prod_{i\in I} G_i := \{(x_i)_{i\in I}, , x_i \in G_i \text{ for each } i \in I\}, \qquad (x_i)_{i\in I} * (y_i)_{i\in I} := (x_i *_i y_i)_{i\in I}.$$

The structure theorem for finite abelian groups states that any finite abelian group is isomorphic to a product of cyclic groups of orders equal to powers of prime numbers. In other words, if G is a finite abelian group of order n, then it can be written as

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}},$$

where $p_1, \ldots, p_m$ are prime numbers, $k_1, \ldots, k_m$ are positive integers, and $p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} = n$. Saying that groups $(G, *)$ and $(G', \star)$ are isomorphic means that there is an isomorphism from G to G', i.e., f is a homomorphism from G to G' ($f(x * y) = f(x) \star f(y)$ for all $x, y \in G$) and that f is invertible.

3 Exercises

Ex.1: Verify that the axioms G_1, G_2, and G_3 imply the uniqueness of an identity element and of inverses. Verify also that a subset H of a group G forms an subgroup of G iff (1) holds.

Ex.2: Verify that, if f is a homomorphism from a group $(G, *)$ to another group $(G', \star)$, then $f(1_G) = 1_{G'}$ and $f(x^{-1}) = (f(x))^{-1}$ for all $x \in G$. Verify that, if f is in addition invertible, then its inverse f^{-1} is automatically an homomorphism from $(G', \star)$ to $(G, *)$.

Ex.3: Let m be the order of an element x in a group G. Prove that m divides any positive integer k such that $x^k = 1_G$.

Ex.4: Prove that the elements of order $\leq m$ in a group G form a subgroup of G.

Ex.5: Prove that

$$SL_n(\mathbb{Z}) := \{A \in \mathcal{M}_{n\times n}(\mathbb{Z}) : |\det(A)| = 1\}$$

of $n \times n$ matrices with integer entries and determinant equal to ± 1 is a group.

Ex.6: Let p and q be the order of two elements x and y in a group G. Suppose that x and y commute and that p and q are relatively prime. Prove that the order of xy equals pq.

Ex.7: For a subset E of a group G, prove that

$$N(E) := \{x \in G : xE = Ex\},$$
$$C(E) := \{x \in G : xy = yx \text{ for all } y \in E\}.$$

are subgroups of G. If E is a subgroup of G, prove that $N(E)$ is the largest subgroup of G containing E as a subgroup and such that $xE = Ex$ for all $x \in N(E)$.