

Groups Formulary

Raúl Ultralaser

Semigroups and groups

The simplest algebraic structure to recognize is a semigroup, which is defined as a nonempty set S with an associative binary operation.

Definition 1. Let (S, \cdot) be a semigroup. If there is an element e , in S such that

$$ex = x = xe \quad \text{for all } x \in S,$$

then e is called the identity of the semigroup (S, \cdot) .

Definition 2. Let (S, \cdot) be a semigroup with identity e . Let $a \in S$. If there exist an element b in S such that

$$ab = e = ba$$

then b is called the inverse of a , and a is said to be invertible

Definition 3. A nonempty set G with a binary operation \cdot on G is called a group if the following axioms hold:

- (i) $a(bc) = (ab)c$ for all $a, b, c \in G$.
- (ii) There exist $e \in G$ such that $ea = a$ for all $a \in G$.
- (iii) For every $a \in G$ there exist $a' \in G$ such that $a'a = e$

Theorem 1. A semigroup G is a group if and only if for all a, b in G , each of the equations $ax = b$ and $ya = b$ has a solution.

Theorem 2. A finite semigroup G is a group if and only if the cancelation laws hold for all elements in G ; that is,

$$ab = ac \Rightarrow b = c \quad \text{and} \quad ba = ca \Rightarrow b = c$$

for all $a, b, c \in G$

Homomorphism

Definition 1. Let G, H be groups. A mapping

$$\phi : G \rightarrow H$$

is called a homomorphism if for all $x, y \in G$

$$\phi(xy) = \phi(x)\phi(y)$$

Furthermore, if ϕ is bijective, then ϕ is called an isomorphism of G onto H , and we write $G \simeq H$. If ϕ is just injective, that is, $1-1$, then we say that ϕ is an isomorphism (or monomorphism) of G into H . If ϕ is surjective, that is, onto, then ϕ is called an epimorphism. A homomorphism of G into itself is called an endomorphism of G that is both $1-1$ and onto is called an automorphism of G .

If $\phi : G \rightarrow H$ is called an intro homomorphism, then H is called a homomorphic image of G ; also, G is said to be homomorphic to H . If $\phi : G \rightarrow H$ is a $1-1$ homomorphism, then G is said to be embeddable in H , and we write $G \odot H$.

Theorem 1. Let G and H be groups with identities e and e' , respectively, and let $\phi : G \rightarrow H$ be a homomorphism. Then

- (i) $\phi(e) = e'$
- (ii) $\phi(x^{-1}) = (\phi(x))^{-1}$ for each $x \in G$.

Definition 2. Let G and H be groups, and let $\phi : G \rightarrow H$ be a homomorphism. The kernel of ϕ is defined to be the set

$$\text{Ker}\phi = \{x \in G \mid \phi(x) = e'\}$$

where e' is the identity in H

Theorem 2. A homomorphism $\phi : G \rightarrow H$ is injective if and only if $\text{Ker}\phi = \{e\}$

Subgroups and cosets

Definition 1. Let (G, \cdot) be a group and let H be a subset of G . H is called a subgroup of G , written $H < G$, if H is a group relative to the binary operation in G .

Theorem 1. Let G be a group. A nonempty subset H of G is a subgroup of G if and only if either of the following holds:

- (i) For all $a, b \in H$, $ab \in H$, and $a^{-1} \in H$.
- (ii) For all $a, b \in H$, $ab^{-1} \in H$.

Theorem 2. Let (G, \cdot) be a group. A nonempty finite subset H of G is a subgroup if and only if $ab \in H$ for all $a, b \in H$.

Theorem 3. Let $\phi : G \rightarrow H$ be a homomorphism of groups. Then $\text{Ker } \phi$ is a subgroup of G and $\text{Im } \phi$ is a subgroup of H .

Definition 2. The center of a group G , written $Z(G)$, is the set of those elements in G that commute with every element in G ; that is,

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$$

Theorem 4. The center of a group G is a subgroup of G .

Theorem 5. Let H and K be subgroups of a group (G, \cdot) . Then HK is a subgroup of G if and only if $HK = KH$.

Theorem 6. Let S be a nonempty subset of a group G . Then the subgroup generated by S is the set M of all finite products x_1, x_2, \dots, x_n such that, for each i , $x_i \in S$ or $x_i^{-1} \in S$.

Theorem 7. Let G be a group and $a \in G$.

- (i) If $a^n = e$ for some integer $n \neq 0$, then $o(a) \mid n$.
- (ii) If $o(a) = m$ then for all integers i , $a^i = a^{r(i)}$, where $r(i)$ is the remainder of i modulo m .
- (iii) $[a]$ is of order m if and only if $o(a) = m$.

Corollary 1. If G is a finite group, then there exist a positive integer k such that $x^k = e$ for all $x \in G$.

Definition 3. Let H be a subgroup of G . Given $a \in G$, the set

$$aH = \{ah \mid h \in H\}$$

is called the left coset of H determined by a . A subset C of G is called a left coset of H in G if $C = aH$ for some a in G . The set of all left cosets of H in G is written G/H .

Definition 4. Let H be a subgroup of G . The cardinal number of the set of left (right) cosets of H in G is called the index of H in G and denoted by $[G : H]$.

Theorem 8 (Lagrange). Let G be a finite group. Then the order of any subgroup of G divides the order of G .

Corollary 2. Let G be a finite group of order n . Then for every $a \in G$, $o(a) \mid n$, and, hence, $a^n = e$.

Consequently, every finite group of prime order is cyclic and, hence, abelian.

Cyclic groups

Theorem 1. Every cyclic group is isomorphic to \mathbb{Z} or to $\mathbb{Z}/(n)$ for some $n \in \mathbb{N}$.

Theorem 2. Any two cyclic groups of the same order (finite or infinite) are isomorphic.

Theorem 3. Every subgroup of a cyclic group is cyclic.

Theorem 4. Let G be a finite cyclic group of order n , and let d be a positive divisor of n . Then G has exactly one subgroup of order d .

Permutation groups

Definition 1. Let X be a nonempty set. The group of all permutations of X under composition of mappings is called the symmetric group on X and is denoted by S_X . A subgroup of S_X is called a permutation group on X .

Definition 2. Let $\sigma \in S_n$. If there exist a list of distinct integers $x_1, \dots, x_n \in n$, such that,

$$\begin{aligned}\sigma(x_i) &= x_{i+1}, & i &= 1, \dots, r-1, \\ \sigma(x_r) &= x_1, \\ \sigma(x) &= x & \text{if } x \notin \{x_1, \dots, x_r\},\end{aligned}$$

then σ is called a cycle of length r and denoted by (x_1, \dots, x_r) . A cycle of length 2 is called a transposition.

Theorem 1 (Cayley). Every group is isomorphic to a permutation group.

Definition 3. The group of symmetries of a regular polygon P_n of n sides is called the dihedral group of degree n and denoted by D_n

Theorem 2. The dihedral group D_n is a group of order $2n$ generated by two elements σ, τ satisfying $\sigma^n = e = \tau^2$ and $\tau\sigma = \sigma^{n-1}\tau$, where

$$\sigma = (1 \ 2 \ \dots \ n), \quad \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & n & \dots & 2 \end{pmatrix}$$

Geometrically, σ is a rotation of the regular polygon P_n through an angle $2\pi/n$ in its own plane, and τ is a reflection (or a turning over) in the diameter through the vertex 1.

Definition 4. The dihedral group D_4 is called the octic group.

Generators and relations

Definition 1. Let G be a group generated by a subset X of G . A set of equations $(r_j = 1)_{j \in A}$ that suffice to construct the multiplication table of G is called a set of defining relations for the group (r_j are products of elements of X).

The set X is called a set of generators. The system $(X; (r_j = 1)_{j \in A})$ is called a presentation of the group.

Normal subgroups

Normal subgroups and quotient groups

Isomorphism theorems

Automorphisms

Conjugacy and G-sets

Normal series

Normal series

Solvable groups

Nilpotent groups

Permutation groups

Cyclic decomposition

Alternating group

Simplicity of A_n

Structure theorems of groups

Direct products