

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

Definition 1. Let G be a group. A subgroup N of G is called a normal subgroup of G , written $N \triangleleft G$, if $xNx^{-1} \subset N$ for every $x \in G$.

Theorem 1. Let N be a subgroup of a group G . Then the following are equivalent.

- (i) $N \triangleleft G$
- (ii) $xNx^{-1} = N$ for every $x \in G$
- (iii) $xN = Nx$ for every $x \in G$
- (iv) $(xN)(yN) = xyN$ for all $x, y \in G$.

Theorem 2. Let N be a normal subgroup of the group G . Then G/N is a group under multiplication. The mapping $\phi: G \rightarrow G/N$, given by $x \mapsto xN$, is a surjective homomorphism, and $\text{Ker}\phi = N$.

Definition 2. Let N be a normal subgroup of G . The group G/N is called the quotient group of G by N . The homomorphism $G \rightarrow G/N$, given by $x \mapsto xN$, is called the natural (or canonical) homomorphism of G onto G/N .

Definition 3. Let G be a group, and let S be a nonempty subset of G . The normalizer of S in G is the set

$$N(S) = \{x \in G \mid xSx^{-1} = S\}$$

The normalizer of a singleton $\{a\}$ is written $N(a)$.

Theorem 3. Let G be a group. For any nonempty subset S of G , $N(S)$ is a subgroup of G . Further, for any subgroup H of G ,

- (i) $N(H)$ is the largest subgroup of G in which H is normal;
- (ii) if K is a subgroup of $N(H)$, then H is a normal subgroup of KH .

Definition 4. Let G be a group. For any $a, b \in G$, $aba^{-1}b^{-1}$ is called a commutator in G . The subgroup of G generated by the set of all commutators in G is called the commutator subgroup of G (or the derived group of G) and denoted by G'

Theorem 4. Let G be a group, and let G' be the derived of G . Then

- (i) $G' \triangleleft G$
- (ii) G/G' is abelian
- (iii) if $H \triangleleft G$, then G/H is abelian if and only if $G' \subset H$.

Isomorphism theorems

Theorem 1 (First isomorphism theorem). Let $\phi : G \rightarrow G'$ be a homomorphism of groups. Then

$$G/\text{Ker}\phi \simeq \text{Im}\phi$$

Hence, in particular, if ϕ is surjective, then

$$G/\text{Ker}\phi \simeq G'$$

Corollary 1. Any homomorphism $\phi : G \rightarrow G'$ of groups can be factored as

$$\phi = j \cdot \psi \cdot \eta$$

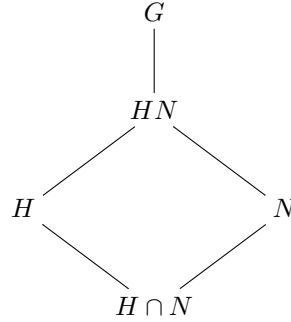
where $\eta : G \rightarrow G/\text{Ker}\phi$ is the natural homomorphism, $\psi : G/\text{Ker}\phi \rightarrow \text{Im}\phi$ is the isomorphism obtained in the theorem, and $j : \text{Im}\phi \rightarrow G'$ is the inclusion map.

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ \eta \downarrow & & \uparrow j \\ G/\text{Ker}\phi & \xrightarrow{\psi} & \text{Im}\phi \end{array}$$

Theorem 2 (Second isomorphism theorem). Let H and N be subgroups of G , and $N \triangleleft G$. Then

$$H/H \cap N \simeq HN/N$$

The inclusion diagram shown below is helpful in visualizing the theorem. Because of this, the theorem is known as the "diamond isomorphism theorem".



Theorem 3 (Third isomorphism theorem). Let H and K be normal subgroups of G and $K \subset H$. Then

$$(G/K)(H/K) \simeq G/H$$

This theorem is also known as the "double quotient isomorphism theorem".

Theorem 4. Let G_1 and G_2 be groups, and $N_1 \triangleleft G_1, N_2 \triangleleft G_2$. Then $(G_1 \times G_2)/(N_1 \times N_2) \simeq (G_1/N_1) \times (G_2/N_2)$.

Theorem 5 (correspondence theorem). Let $\phi : G \rightarrow G'$ be a homomorphism of a group G onto a group G' . Then the following are true:

- (i) $H < G \Rightarrow \phi(H) < G'$.
- (i)' $H' < G' \Rightarrow \phi^{-1}(H') < G$.
- (ii) $H \triangleleft G \Rightarrow \phi(H) \triangleleft G'$
- (ii)' $H' \triangleleft G' \Rightarrow \phi^{-1}(H') \triangleleft G$
- (iii) $H < G$ and $H \supset \text{Ker}\phi \Rightarrow H = \phi^{-1}(\phi(H))$
- (iv) The mapping $H \mapsto \phi(H)$ is a 1-1 correspondence between the family of subgroups of G' ; furthermore, normal subgroups of G correspond to normal subgroups of G' .

Corollary 2. Let N be a normal subgroup of G . Given any subgroup H' of G/N , there is a unique subgroup H of G such that $H' = H/N$. Further, $H \triangleleft G$ if and only if $H/N \triangleleft G/N$.

Definition 1. Let G be a group. A normal subgroup N of G is called a maximal normal subgroup if

- (i) $N \neq G$
- (ii) $H \triangleleft G$ and $H \supset N \Rightarrow H = N$ or $H = G$.

Definition 2. A group of G is said to be simple if G has no proper normal subgroups; that is, G has no normal subgroups except (e) and G .

Corollary 3. Let N be a proper normal subgroup of G . Then N is a maximal normal subgroup of G if and only if G/N is simple.

Corollary 4. Let H and K be a distinct maximal normal subgroups of G . Then $H \cap K$ is a maximal normal subgroup of H and also of K .

Automorphism

Recall that an automorphism of a group G is an isomorphism of G onto G . The set of all automorphism of G is denoted by $Aut(G)$. We have seen that every $g \in G$ determines an automorphism I_g of G (called an inner automorphism) given by $x \mapsto gxg^{-1}$. The set of all inner automorphism of G is denoted by $In(G)$.

Theorem 1. The set $Aut(G)$ of all automorphism of a group G is a group under composition of mappings, and $In(G) \triangleleft Aut(G)$. Moreover,

$$G/Z(G) \simeq In(G)$$

Conjugacy and G-sets

Definition 1. Let G be a group and X a set. Then G is said to act on X if there is a mapping $\phi : G \times X \mapsto X$, with $\phi(a, x)$ written $a * x$, such that for all $a, b \in G, x \in X$,

- (i) $a * (b * x) = (ab) * x$
- (ii) $e * x = x$

The mapping ϕ is called the action of G on X , and X is said to be a G -set.

Theorem 1. Let G be a group and let X be a set

- (i) If X is a G -set, then the action of G on X induces a Homomorphism $\phi : G \mapsto S_x$.
- (ii) Any homomorphism $\phi : G \mapsto S_x$ induces an action of G on X .

Theorem 2 (Cayley's theorem). Let G be a group. Then G is isomorphic into the symmetric group S_G .

Theorem 3. Let G be a group and $H < G$ of index n . Then there is a homomorphism $\phi : G \mapsto S_n$ such that $Ker\phi = \cap_{x \in G} xHx^{-1}$

Corollary 1. Let G be a group with a normal subgroup H of index n . Then G/H is isomorphic into S_n .

Corollary 2. Let G be a simple group with a subgroup $\neq G$ of finite index n . Then G is isomorphic into S_n

Definition 2. Let G be a group acting on a set X , and let $x \in X$. Then the set

$$G_x = \{g \in G | gx = x\}$$

which can be easily shown to be a subgroup, is called the stabilizer (or isotropy) group of x in G .

Definition 3. Let G be a group acting on a set X , and let $x \in X$. Then the set

$$Gx = \{ax | a \in G\}$$

is called the orbit of x in G .

Theorem 4. Let G be a group acting on a set X . Then the set of all orbits in X under G is a partition of X . For any $x \in X$ there is a bijection $Gx \mapsto G/G_x$ and, hence,

$$|Gx| = [G : G_x].$$

Therefore, if X is a finite set,

$$|X| = \sum_{x \in C} [G : G_x],$$

where C is a subset of X containing exactly one element from each orbit.

Theorem 5. Let G be a group. Then the following are true:

- (i) The set of conjugate classes of G is a partition of G
- (ii) $|C(a)| = [G : N(a)]$
- (iii) If G is finite, $|G| = \sum [G : N(a)]$, a running over exactly one element from each conjugate class.

Definition 4. Let S and T be two subsets of a group G . Then T is said to be conjugate to S if there exist $x \in G$ such that $T = xSx^{-1}$.

Theorem 6. Let G be a group. Then for any subset S of G ,

$$|C(S)| = [G : N(S)] \quad [N(S) = \{x \in G | x^{-1}Sx = S\}]$$

Theorem 7. Let G be a finite group order of p^n , where p is prime and $n > 0$. Then.

- (i) G has a nontrivial center Z .
- (ii) $Z \cap N$ is nontrivial for any nontrivial normal subgroup N of G .
- (iii) If H is a proper subgroup of G , then H is properly contained in $N(H)$; hence, if H is a subgroup of order p^{n-1} , then $H \triangleleft G$.

Corollary 3. Every group of order p^2 (p is prime) is abelian.

Theorem 8 (Burnside). Let G be a finite group acting on a finite set X . Then the number k of orbits in X under G is

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Normal series

Normal series

Definition 1. A sequence (G_0, G_1, \dots, G_r) of subgroups G is called a normal series (or subnormal series) of G if

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{r-1} \triangleleft G_r = G.$$

The factors of a normal series are the quotient groups G_i/G_{i-1} , $i \leq i \leq r$

Definition 2. A composition series of a group G is a normal series (G_0, \dots, G_r) without repetition whose factors G_i/G_{i-1} are all simple groups. These factors G_i/G_{i-1} are called composition factors of G .

Lemma 1. Every finite group has a composition series.

Definition 3. Two normal series $S = (G_0, G_1, \dots, G_r)$ and $S' = (G'_0, G'_1, \dots, G'_r)$ of G are said to be equivalent, written $S \sim S'$, if the factors of one series are isomorphic to the factors of the other after some permutation; that is,

$$G'_i/G'_{i-1} \simeq G_{\sigma(i)}/G_{\sigma(i)-1} \quad i = 1, \dots, r,$$

for some $\sigma \in S_r$.

Evidently, \sim is an equivalent relation.

Theorem 1 (Jordan-Holder). Any two composition series of a finite group are equivalent.

Solvable groups

Definition 1. A group G is said to be solvable if $G^k = \{e\}$ for some positive integer.

Theorem 1. Let G be a group. If G is solvable, then every subgroup of G and every homomorphic image of G are solvable. Conversely, if N is normal subgroup of G such that N and G/N are solvable, then G is solvable.

Theorem 2. A group G is solvable if and only if G has a normal series with abelian factors. Further, a finite group is solvable if and only if its composition factors are cyclic groups of prime order.

Nilpotent groups

Permutation groups

Cyclic decomposition

Alternating group

Simplicity of A_n

Structure theorems of groups

Direct products