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*

$$ex = x = xe \qquad for\ \ all\ \ x \in S,$$

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:*

$$\begin{aligned} (i) \quad & a(bc) = (ab)c \ for\ all\ a,b,c \in G. \\ (ii) \quad & There\ exist\ e \in G\ such\ that\ ea = a \\ & for\ all\ a \in G. \\ (iii) \quad & For\ every\ a \in G \\ & there\ exist\ a' \in G\ such\ that\ a'a = e \end{aligned}$$

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,*

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

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

Homomorphism

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

$$\phi : G \to H$$

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

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

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

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

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

where e' is the identity in H

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

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:*

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

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 $\phi : G \to H$ be a homomorphism of groups. Then $Ker\phi$ is a subgroup of G and $Im\phi$ 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,*

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

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 $x_1, x_2, ..., x_n$ such that, for each i, $x_i \in S$ or $x_i^{-1} \in S$*

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

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

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*

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

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 $a \in G$, $o(a)|n$, 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 $x_1, ..., x_n \in n$, such that,*

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

then σ is called a cycle of length r and denoted by $(x_1, ..., x_r$. 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*

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

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 $N \lhd G$, 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.*

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

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

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 $G \to G/N$, 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*

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

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*

$$\begin{aligned} &(i) \quad G' \lhd G \\ &(ii) \quad G/G' is abelian \\ &(iii) \quad if\ H \lhd G,\ then\ G/H\ is\ abelian \\ &\qquad if\ and\ only\ if\ G' \subset H. \end{aligned}$$

Isomorphism theorems

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

$$G/Ker\phi \simeq Im\phi$$

Hence, in particular, if ϕ is surjective, then

$$G/Ker\phi \simeq G'$$

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

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

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

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\eta"] & G' \\ G/Ker\phi \arrow[r, "\phi"] & Im\phi \arrow[u, "j"] \end{tikzcd}$$

Theorem 2 (Second isomorphism theorem). *Let H and N be subgroups of G, and $N \lhd G$. 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".

$$\begin{tikzcd} & G \arrow[d, dash] & \\ & HN \arrow[dl, dash] \arrow[dr, dash] & \\ H \arrow[dr, dash] & & N \arrow[dl, dash] \\ & H \cap N & \end{tikzcd}$$

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 $N_1 \lhd G_1, N_2 \lhd G_2$. Then $(G_1 \times G_2)/(N_1 \times N_2) \simeq (G_1/N_1) \times (G_/N_2)$.*

Theorem 5 (correspondence theorem). *Let $\phi : G \to G'$ 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) $H \lhd G \Rightarrow \phi(H) \lhd G'$

$(ii)'$ $H' \lhd G' \Rightarrow \phi^{-1}(H') \lhd G$

(iii) $H < G$ *and* $H \supset Ker\phi \Rightarrow H = \phi^{-1}(\phi(H))$

(iv) *The maping $H \mapsto \phi(H)$ is a $1-1$ correspondence between the family of subgroups of G'; futhermore, 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, $H \lhd G$ if and only if $H/N \lhd G/N$.*

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) $H \lhd G$ *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 $In(G) \lhd Aut(G)$. 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 $a, b \in G, x \in X$,*

$$\begin{aligned} (i) \quad & a * (b * x) = (ab) * x \\ (ii) \quad & e * x = x \end{aligned}$$

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 and action of G onto 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 is there exist $x \in G$ such that $T = xSx^{-1}$.*

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

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

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 sobgroup of order* p^{n-1}*, then* $H \lhd G$.

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 $(G_0, G_1, ..., G_r)$ of subgroups G is called a normal series (or subnormal series) of G if*

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

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 $(G_0, ..., G_r)$ 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 $S = (G_0, G_1, ..., G_r)$ and $S' = (G'_0, G'_1, ..., G'_r)$ 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,*

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

for some $\sigma \in S_r$.

Evidently, $\sim$ is and 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

Definition 1. *A group G is said to be nilpotent if $Z_m(G) = G$ for some m. The smallest m such that $Z_m(G) = G$ is called the class of nilpotency of G.*

Theorem 1. *A group of order p^n (p prime) is nilpotent*

Theorem 2. *A group G is nilpotent if and only if G has a normal series*

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G$$

such that $G_i/G_i - 1 \subset Z(G/G_{i-1})$ for all $i = 1, ..., m$.

Corollary 1. *Every nilpotent group is solvable.*

Theorem 3. *Let G be a nilpotent group. Then every subgroup of G and every homomorphic image of G are nilpotent.*

Theorem 4. *Let $H_1, ..., H_n$ be a family of nilpotent groups. Then $H_1 \times \cdots \times H_n$ is also nilpotent.*

Permutation groups

Cyclic decomposition

Alternating group

Simplicity of A_n

Structure theorems of groups

Direct products

Theorem 1. *Let $H_1, ..., H_n$ be a family of subgroups of a group G, and let $H = H_1 \cdots H_n$. Then the following are equivalent:*

(i) $H_1 \times \cdots \times \simeq H$ *under the canonical mapping that sends* $(x_1, ..., x_n)$ *to* $x_1 \cdots x_n$.

(ii) $H_i \lhd H$, *and every element* $x \in H$ *can be uniquely expressed as* $x = x_1 \cdots x_n, x_i \in H_i$.

(iii) $H_i \lhd H$, *and if* $x_1 \cdots x_n = e$, *then each* $x_i = e$.

(iv) $H_i \lhd H$, *and* $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\},\ 1 \leq i \leq n.$