# 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 1.1.** *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 1.2.** *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 1.3.** *A nonempty set $G$ with a binary operation $\cdot$ on $G$ is called a group if the following axioms hold:*

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

**Theorem 1.1.** *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 1.2.** *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 1.4.** *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 $\phi$ is bijective, then $\phi$ is called an isomorphism of $G$ onto $H$, and we write $G \simeq H$. If $\phi$ is just injective, that is, $1 - 1$, then we say that $\phi$ is an isomorphism (or monomorphism) of $G$ into $H$. if $\phi$ is surjective, that is, onto, then $\phi$ 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 1.3.** *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 1.5.** *Let $G$ and $H$ be groups, and let $\phi : G \to H$ be a homomorphism. The kernel of $\phi$ is defined to be the set*

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

*where $e'$ is the identity in $H$*

**Theorem 1.4.** *A homomorphism $\phi : G \to H$ is injective if and only if $Ker\phi = \{e\}$*

## Subgroups and cosets

**Definition 1.6.** *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 1.5.** *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 $ab \in H, ab^{-1} \in H$.*

**Theorem 1.6.** *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 1.7.** *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 1.7.** *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 1.8.** *The center of a group $G$ is a subgroup of $G$*

**Theorem 1.9.** *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 1.10.** *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 1.11.** *Let $G$ be a group and $a \in G$*

$(i)$ $If \; a^n = e \; for \; some \; integer \; n \neq 0, \; then \; o(a)|n$

$(ii)$ $If \; o(a) = m \; then \; for \; all \; integers \; i, a^i = a^{r(i)},$ $where \; r(i) \; is \; the \; remainder \; of \; i \; modulo \; m.$

$(iii)$ $[a] \; is \; of \; order \; m \; if \; and \; only \; if \; o(a) = m.$

**Corolarry 1.1.** *If $G$ is a finite group, then there exist a positive integer $k$ such that $x^k = e$ for all $x \in G$.*

**Definition 1.8.** *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 1.9.** *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 1.12 (Lagrange).** *Let $G$ be a finite group. Then the order of any subgroup of $G$ divides the order of $G$.*

**Corolarry 1.2.** *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 1.13.** *Every cyclic group is isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}/(n)$ for some $n \in \mathbb{N}$*

## Permutation groups

## Generators and reflations

# 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