# Abstract Algebra

Notes by R.J. Buehler
Based on J.A. Gallian's *Contemporary Abstract Algebra*

April 26, 2011

## 0 Preliminaries

► **Theorem 0.1** (The Division Algorithm)**.**
*Let $a$ and $b$ be integers with $b > 0$. Then there exists unique integers $q$ and $r$ with the property that $a = bq + r$, where $0 \leq r < b$.*

► **Theorem 0.2** (GCD is a Linear Combination)**.**
*For any nonzero integers $a$ and $b$, there exists integers $s$ and $t$ such that $gcd(a, b) = as + bt$. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.*

► **Corollary.**

*If $a$ and $b$ are relatively prime, then there exists integers $s$ and $t$ such that $as + bt = 1$.*

► **Euclid's Lemma.**
*$p|ab$ implies $p|a$ or $p|b$*

► **Theorem 0.3** (Fundamental Theorem of Arithmetic)**.**
*Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear.*

### 0.1 Modular Arithmetic

For integers $a$, $b$, and $n$, if

$$a \bmod n = c$$
$$b \bmod n = d$$

then

$$(a + b) \bmod n = (c + d) \bmod n$$
$$(a - b) \bmod n = (c - d) \bmod n$$
$$(a * b) \bmod n = (c * d) \bmod n$$

**Definition: Least Common Multiple**
The least common multiple of two non-zero integers $a$ and $b$ is the smallest positive integer that is a multiple of both $a$ and $b$. We will denote this integer by $lcm(a, b)$.

## 2 Groups

**Definition: Group**
Let $G$ be a set together with a binary operation (usually called 'multiplication') that assigns to each ordered pair $(a, b)$ of elements of $G$ an element in $G$ denoted by $ab$. We say $G$ is a *group* under this operation if the following three properties are satisfied.

1. *Associativity.* The operation is associative; that is, $(ab)c = a(bc)$ for all $a$, $b$, $c$ in $G$.
2. *Identity.* There is an element $e$ (called the *identity*) in $G$ such that $ae = ea = a$ for all $a$ in $G$.
3. *Inverses.* For each element $a$ in $G$, there is an element $b$ in $G$ (called an *inverse* of $a$) such that $ab = ba = e$.

**Definition: Abelian**
A group $G$ is called *Abelian* if the operation is commutative; that is, for all $a$, $b$ in $G$, $ab = ba$.

▶ **Theorem 2.1** (Uniqueness of the Identity)**.**
*In a group $G$, there is only one identity element.*

▶ **Theorem 2.2** (Cancellation)**.**
*In a group $G$, the left and right cancellation laws hold; that is, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.*

▶ **Theorem 2.3** (Uniqueness of Inverses)**.**
*For each element $a$ in a group $G$, there is a unique element $b$ in $G$ such that $ab = ba = e$.*

▶ **Theorem 2.4** (Socks-Shoes Property)**.**
*For group elements $a$ and $b$, $(ab)^{-1} = b^{-1}a^{-1}$.*

## 3 Finite Groups; Subgroups

**Definition: Order of a Group**
The number of elements of a group (finite or infinite) is called its *order*. We will use $|G|$ to denote the order of $G$.

**Definition: Order of an Element**
The *order* of an element $g$ in a group $G$ is the smallest positive integer $n$ such that $g^n = e$ (in additive notation, $ng = e$). If no such integer exists, we say that $g$ has *infinite* order. The order of an element $g$ is denoted by $|g|$.

**Definition: Subgroup**
If a subset $H$ of a group $G$ is itself a group under the operation of $G$, we say that $H$ is a *subgroup* of $G$, denoted $H \leq G$. If $H$ is a strict subset of $G$, also $H < G$.

▶ **Theorem 3.1** (One-Step Subgroup Test)**.**
*Let $G$ be a group and $H$ a nonempty subset of $G$. If $ab^{-1}$ is in $H$ whenever $a$ and $b$ are in $H$, then $H$ is a subgroup of $G$.*

▶ **Theorem 3.2** (Two-Step Subgroup Test)**.**
*Let $G$ be a group and $H$ a nonempty subset of $G$. If $ab$ is in $H$ whenever $a$ and $b$ are in $H$ ($H$ is closed under the operation), and $a^{-1}$ is in $H$ whenever $a$ is in $H$ ($H$ is closed under taking inverses), then $H$ is a subgroup of $G$.*

▶ **Theorem 3.3** (Finite Subgroup Test)**.**
*Let $H$ be a nonempty subset of a group $G$. If $H$ is closed under the operation of $G$, then $H$ is a subgroup of $G$.*

**Definition: Cyclic Group, $\langle a \rangle$**
A group $G$ is *cyclic* if $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. The element, $a$, which generates $G$ is called a *generator of $G$* and need not be unique.

Briefly, every cyclic group is Abelian (consider the form every element must take and the fact that $a^j a^i = a^{i+j} = a^i a^j$). Moreover, it's common to forget that $\langle a \rangle$ contains $a^n$ for all $n \in \mathbb{Z}$—this includes 0 and negative $n$!

▶ **Theorem 3.4** ($\langle a \rangle$ is a Subgroup)**.**
*Let $G$ be a group, and let $a$ be any element of $G$. Then, $\langle a \rangle$ is a subgroup of $G$.*

**Definition: Center of a Group**
The *center*, $Z(G)$, of a group $G$ is the subset of elements in $G$ that commute with every element of $G$. In symbols, $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$.

▶ **Theorem 3.5** (The Center of a Group is a Subgroup)**.**
*The center of a group $G$ is a subgroup of $G$.*

**Definition: Centralizer of $a$ in $G$**
Let $a$ be a fixed element of a group $G$. The *centralizer of $a$ in $G$*, denoted $C(a)$, is the set of all elements in $G$ that commute with $a$. In symbols, $C(a) = \{g \in G \mid ga = ag\}$.

▶ **Theorem 3.6** ($C(a)$ is a Subgroup)**.**
*For each $a$ in a group $G$, the centralizer of $a$ is a subgroup of $G$.*

# 4 Cyclic Groups

▶ **Theorem 4.1** (Criterion for $a^i = a^j$)**.**

*Let $G$ be a group, and let $a$ belong to $G$. If $a$ has infinite order, then $a^i = a^j$ if and only if $i = j$. If $a$ has finite order, say $n$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if $n$ divides $i - j$.*

▶ **Corollary** ($|a| = |\langle a \rangle|$)**.**

*For any group element $a$, $|a| = |\langle a \rangle|$.*

▶ **Corollary** ($a^k = e$ implies that $|a|$ divides $k$)**.**

*Let $G$ be a group and let $a$ be an element of order $n$ in $G$. If $a^k = e$, then $n$ divides $k$.*

▶ **Theorem 4.2** ($\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$)**.**

*Let $a$ be an element of order $n$ in a group and let $k$ be a positive integer. Then $\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{gcd(n,k)}$.*

▶ **Corollary** (Order of Elements in Finite Cyclic Groups)**.**

*In a finite cyclic group, the order of an element divides the order of the group.*

▶ **Corollary** (Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$)**.**

*Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $gcd(n, i) = gcd(n, j)$ and $|a^i| = |a^j|$ if and only if $gcd(n, i) = gcd(n, j)$ .*

▶ **Corollary** (Generators of Finite Cyclic Groups)**.**

*Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $gcd(n, j) = 1$ and $|a| = |a^j|$ if and only if $gcd(n, j) = 1$ .*

▶ **Theorem 4.3** (Fundamental Theorem of Cyclic Groups)**.**

*Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of $n$; and, for each positive divisor $k$ of $n$, the group $\langle a \rangle$ has exactly one subgroup of order $k$–namely $\langle a^{\frac{n}{k}} \rangle$.*

**Definition: Euler Phi Function**
An important number-theoretic function defined by

$$\phi(1) = 1$$

and for $n > 1$,

$$\phi(n) = \text{ the number of positive integers less than } n \text{ and relatively prime to } n$$

Notice that, by definition, $|U(n)| = \phi(n)$.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\phi(n)$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 | 4 |

▶ **Theorem 4.4** (Number of Elements of Each Order in a Cyclic Group)**.**

*If $d$ is a positive divisor of $n$, the number of elements of order $d$ in a cyclic group of order $n$ is $\phi(d)$.*

▶ **Corollary** (Number of Elements of Order $d$ in a Finite Group)**.**

*In a finite group, the number of elements of order $d$ is divisible by $\phi(d)$.*

# 5 Permutation Groups

**Definition: Permutation of A**
A *permutation* of a set $A$ is a bijective function from $A$ to $A$.

**Definition: Permutation Group**
A *permutation group* of a set $A$ is a set of permutations of $A$ that forms a group under function composition.

**Definition: The Symmetric Group of Degree $n$, $S_n$**
The set of all permutations of $\{1, 2, \ldots, n\}$; for $n > 1$, $|S_n| = n!$.

## 5.1 Permutation Notations

There exist two predominant permutation notations. The first is intuitive, placing every element in the set in order, and then writing the element to which it is mapped by the permutation below it. For example,

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$$

is interpreted as specifying that the permutation $\alpha$ has the form $\alpha(1) = 2$, $\alpha(2) = 1$, $\alpha(3) = 4$, and so on. In contradistinction, the second permutation notation, known as *cycle notation*, was introduced later by Cauchy and proves to be, while less intuitive, more useful for our purposes. Cauchy's crucial insight was noticing that every permutation can be written as a series of cycles. Thus, adapting our example from above, we achieve

$$\alpha = (12)(346)(5)$$

In actual use, it's traditional to simply exclude any cycles of size 1. Thus,

$$\alpha = (12)(346)$$

▶ **Theorem 5.1** (Products of Disjoint Cycles)**.**
*Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.*

▶ **Theorem 5.2** (Disjoint Cycles Commute)**.**
*If the pair of cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_m)$ have no entries in common, then $\alpha\beta = \beta\alpha$.*

▶ **Theorem 5.3** (Order of a Permutation (Ruffini-1799))**.**
*The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.*

▶ **Theorem 5.4** (Product of Two Cycles)**.**
*Every permutation in $S_n$, $n > 1$ is a product of 2-cycles.*

▶ **Lemma.**
*If $e = \beta_1\beta_2 \ldots \beta_r$, where the $\beta$'s are 2-cycles, then $r$ is even.*

▶ **Theorem 5.5** (Always Even or Always Odd)**.**
*If a permutation $\alpha$ can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of $\alpha$ into a product of 2-cycles must have an even (odd) number of 2-cycles.*

**Definition: Even and Odd Permutations**
A permutation that can be expressed as a product of an even number of 2-cycles is called an *even* permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an *odd* permutation.

▶ **Theorem 5.6** (Even Permutations Form a Group)**.**
*The set of even permutations in $S_n$ forms a subgroup of $S_n$ and is denoted $A_n$.*

**Definition: Alternating Group of Degree $n$, $A(n)$**
The group of even permutations of $n$ symbols is denoted by $A_n$ and is called the *alternating group of degree $n$*.

▶ **Theorem 5.7.**
*For $n > 1$, $A_n$ has order $\frac{n!}{2}$.*

# 6 Isomorphism

**Definition: Group Isomorphism**
An *isomorphism* $\phi$ from a group $G$ to a group $\bar{G}$ is a bijective mapping (or function) from $G$ onto $\bar{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \qquad \text{for all } a, b \text{ in } G$$

If there is an isomorphism from $G$ to $\bar{G}$, we say that $G$ and $\bar{G}$ are *isomorphic* and write $G \approx \bar{G}$.

## 6.1 Proving Two Groups are Isomorphic

There are four separate steps involved in proving that a group $G$ is isomorphic to a group $\bar{G}$.

**Step 1** 'Mapping', Define a candidate for the isomorphism; that is a function $\phi : G \to \bar{G}$.

**Step 2** 'Injective', Prove that $\phi$ is injective; that is, prove $\phi(a) = \phi(b)$ implies $a = b$.

**Step 3** 'Surjective', Prove that $\phi$ is surjective; that is, prove that $\forall b \in \bar{G}$, there exists $a \in G$ such that $\phi(a) = b$.

**Step 4** 'Operation Preserving', Prove that $\phi$ is operation-preserving; that is, show that $\phi(ab) = \phi(a)\phi(b)$ for all $a$, $b$ in $G$.

▶ **Theorem 6.1** (Cayley's Theorem (1854))**.**
*Every group is isomorphic to a group of permutations.*

► **Theorem 6.2** (Properties of Isomorphisms Acting on Elements)**.**

*Suppose that $\phi$ is an isomorphism from a group $G$ onto a group $\bar{G}$. Then,*

1. $\phi(e_G) = \phi(e_{\bar{G}})$
2. *For every integer $n$ and for every group element $a$ in $G$, $\phi(a^n) = [\phi(a)]^n$.*
3. *For any elements $a$ and $b$ in $G$, $a$ and $b$ commute if and only if $\phi(a)$ and $\phi(b)$ commute.*
4. $G = \langle a \rangle$ *if and only if* $\bar{G} = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$ *for all $a$ in $G$ (isomorphisms preserve orders).*
6. *For a fixed integer $k$ and a fixed group element $b$ in $G$, the equation $x^k = b$ has the same number of solutions in $G$ as does the equation $x^k = \phi(b)$ in $\bar{G}$.*
7. *If $G$ is finite, then $G$ and $\bar{G}$ have exactly the same number of elements of every order.*

► **Theorem 6.3** (Properties of Isomorphisms Acting on Groups)**.**

*Suppose that $\phi$ is an isomorphism from a group $G$ to a group $\bar{G}$. Then,*

1. $\phi^{-1}$ *is an isomorphism from $\bar{G}$ to $G$.*
2. *$G$ is Abelian if and only if $\bar{G}$ is Abelian.*
3. *$G$ is cyclic if and only if $\bar{G}$ is cyclic.*
4. *If $K$ is a subgroup of $G$, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\bar{G}$.*

**Definition: Automorphism**
An isomorphism from a group $G$ to itself is called an *automorphism* of $G$.

**Definition: Inner Automorphism Induced by $a$**
Let $G$ be a group, and let $a \in G$. The function $\phi_a(x) = axa^{-1}$ for all $x$ in $G$ is called the *inner automorphism of $G$ induced by $a$*

► **Theorem 6.4** ($Aut(G)$ and $Inn(G)$ are Groups)**.**

*The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.*

► **Theorem 6.5** ($Aut(\mathbb{Z}_n) \approx U(n)$)**.**

*For every positive integer $n$, $Aut(\mathbb{Z}_n)$ is isomorphic to $U(n)$.*

# 7 Cosets and Lagrange's Theorem

**Definition: Coset of $H$ in $G$**
Let $G$ be a group and let $H$ be a subset of $G$. For any $a \in G$, the set $\{ah \mid h \in H\}$ is denoted by $aH$. Analogously, $Ha = \{ha \mid h \in H\}$ and $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. When $H$ is a subgroup of $G$, the set $aH$ is called the *left coset of $H$ in $G$ containing $a$*, whereas $Ha$ is called the *right coset of $H$ in $G$ containing $a$*. In this case, the element $a$ is called the *coset representative* of $aH$ (or $Ha$). We use $|aH|$ to denote the number of elements in the set $aH$, and $|Ha|$ to denote the number of elements in $Ha$.

▶ **Lemma** (Properties of Cosets)**.**
*Let $H$ be a subgroup of $G$, and let $a$ and $b$ belong to $G$. Then,*

1. $a \in aH$
2. $aH = H$ *if and only if* $a \in H$
3. $aH = bH$ *if and only if* $a \in bH$
4. $aH = bH$ *or* $aH \cap bH = \emptyset$
5. $aH = bH$ *if and only if* $a^{-1}b \in H$
6. $|aH| = |bH|$
7. $aH = Ha$ *if and only if* $H = aHa^{-1}$
8. $aH$ *is a subgroup of $G$ if and only if* $a \in H$

▶ **Theorem 7.1** (Lagrange's Theorem: $|H|$ divides $|G|$)**.**
*If $G$ is a finite group and $H$ is a subgroup of $G$, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of $H$ in $G$ is $\frac{|G|}{|H|}$.*

▶ **Corollary** ($|a|$ Divides $|G|$)**.**
*In a finite group, the order of each element of the group divides the order of the group.*

▶ **Corollary** (Groups of Prime Order are Cyclic)**.**
*A group of prime order is cyclic.*

▶ **Corollary** ($a^{|G|} = e$)**.**
*Let $G$ be a finite group, and let $a \in G$. Then, $a^{|G|} = e$.*

▶ **Corollary** (Fermat's Little Theorem)**.**
*For every integer $a$ and every prime $p$, $a^p \bmod p = a \bmod p$.*

▶ **Theorem 7.2** (Classification of Groups of Order $2p$)**.**
*Let $G$ be a group of order $2p$, where $p$ is a prime greater than 2. Then $G$ is isomorphic to $\mathbb{Z}_{2p}$ or $D_p$.*

# 8 External Direct Products

**Definition: External Direct Product**
Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \ldots \oplus G_n$, is the set of all $n$-tuples for which the $i$th component is an element of $G_i$ and the operation is componentwise. In symbols,

$$G_1 \oplus G_2 \oplus \ldots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\},$$

where $(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n')$ is defined to be $(g_1 g_1', g_2 g_2', \ldots, g_n g_n')$. It is understood that each product $g_i g_i'$ is performed with the operation of $G_i$.

▶ **Theorem 8.1** ( Order of an Element in a Direct Product ).
*The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,*

$$|(g_1, g_2, \ldots, g_n)| = \mathbf{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$$

▶ **Theorem 8.2** ( Criterion for $G \oplus H$ to be Cyclic ).
*Let $G$ and $H$ be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.*

▶ **Corollary** ( Criterion for $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ to be Cyclic ).
*An external direct product $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.*

▶ **Corollary** ( Criterion for $\mathbb{Z}_{n_1 n_2 \ldots n_k} \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_k}$ ).
*Let $m = n_1 n_2 \ldots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_k}$ if and only if $n_i$ and $n_j$ are relatively prime whenever $i \neq j$.*

▶ **Theorem 8.3** ( $U(n)$ as an External Direct Product ).
*Suppose $s$ and $t$ are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. In short,*

$$U(st) \approx U(s) \oplus U(t).$$

*Moreover, $U_s(st)$ is isomorphic to $U(t)$, and $U_t(st)$ is isomorphic to $U(s)$.*

▶ **Corollary.**
*Let $m = n_1 n_2 \ldots n_k$ where $gcd(n_i, n_j) = 1$ for all $i \neq j$. Then,*

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \ldots \oplus U(n_k).$$

# 9 Normal Subgroups and Factor Groups

**Definition: Normal Subgroup**
A subgroup $H$ of a group $G$ is called a *normal* subgroup of $G$ if $aH = Ha$ for all $a$ in $G$. We denote this by $H \lhd G$.

It's important to note that a normal subgroup isn't necessarily Abelian. While $aH = Ha$, it's not necessary that $ah = ha$ for a particular $h \in H$.

► **Theorem 9.1** ( Normal Subgroup Test ).

*A subgroup $H$ of $G$ is normal in $G$ if and only if $xHx^{-1} \subseteq H$ for all $x$ in $G$.*

► **Theorem 9.2** ( Factor Groups ).

*Let $G$ be a group and let $H$ be a normal subgroup of $G$. The set $G/H = \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$.*

► **Theorem 9.3** ( The G/Z Theorem ).

*Let $G$ be a group and let $Z(G)$ be the center $G$. If $G/Z(G)$ is cyclic, then $G$ is Abelian.*

► **Theorem 9.4** ( $G/Z(G) \approx Inn(G)$ ).

*For any group $G$, $G/Z(G)$ is isomorphic to $Inn(G)$.*

► **Theorem 9.5** ( Cauchy's Theorem for Abelian Groups ).

*Let $G$ be a finite Abelian group and let $p$ be a prime that divides the order of $G$. Then $G$ has an element of order $p$.*

**Definition: Internal Direct Product of $H$ and $K$**
We say that $G$ is the *internal direct product* of $H$ and $K$ and write $G = H \times K$ if $H$ and $K$ are normal subgroups of $G$ and

$$G = HK \quad \text{and} \quad H \cap K = \{e\}.$$

**Definition: Internal Direct Product $H_1 \times H_2 \times \ldots \times H_n$**
Let $H_1$, $H_2$, …, $H_n$ be a finite collection of normal subgroups of $G$. We say that $G$ is the *internal direct product* of $H_1$, $H_2$, …, $H_n$ and write $G = H_1 \times H_2 \times \ldots \times H_n$, if

1. $G = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n \mid h_i \in H_i\}$
2. $(H_1H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, 3, \ldots, n-1$.

► **Theorem 9.6** ( $H_1 \times H_2 \times \ldots \times H_n \approx H_1 \oplus H_2 \oplus \ldots \oplus H_n$ ).

*If a group $G$ is the internal direct product of a finite number of subgroups $H_1$, $H_2$, …, $H_n$, then $G$ is isomorphic to the external direct product of $H_1$, $H_2$, …, $H_n$.*

► **Theorem 9.7** ( Classification of Groups of Order $p^2$ ).

*Every group of order $p^2$, where $p$ is a prime, is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$.*

► **Corollary.**

*If $G$ is a group of order $p^2$, where $p$ is a prime, then $G$ is Abelian.*

# 10 Group Homomorphisms

**Definition: Group Homomorphism**
A *homomorphism* $\phi$ from a group $G$ to a group $\bar{G}$ is a mapping from $G$ to $\bar{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all $a$,$b$ in $G$.

**Definition: Kernel of a Homomorphism**
The *kernel* of a homomorphism $\phi$ from a group $G$ to a group $\bar{G}$ is the set $\{x \in G \mid \phi(x) = e_{\bar{G}}\}$. The kernel of $\phi$ is denoted by $Ker\ \phi$.

► **Theorem 10.1** ( Properties of Elements under Homomorphisms ).

*Let $\phi$ be a homomorphism from a group $G$ to a group $\bar{G}$ and let $g$ be an element of $G$. Then*

1. $\phi(e_G) = e_{\bar{G}}$
2. $\phi(g^n) = (\phi(g))^n$ *for all* $n$ *in* $\mathbb{Z}$
3. *If* $|g|$ *is finite, then* $|\phi(g)|$ *divides* $|g|$.
4. $Ker\ \phi$ *is a subgroup of* $G$.
5. $\phi(a) = \phi(b)$ *if and only if* $a\,Ker\ \phi = b\,Ker\ \phi$.
6. *If* $\phi(g) = g'$, *then* $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\,Ker\ \phi$.

► **Theorem 10.2** ( Properties of Subgroups under Homomorphisms ).

*Let $\phi$ be a homomorphism from a group $G$ to a group $\bar{G}$ and let $H$ be a subgroup of $G$. Then*

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ *is a subgroup of* $\bar{G}$.
2. *If* $H$ *is cyclic, then* $\phi(H)$ *is cyclic.*
3. *If* $H$ *is Abelian, then* $\phi(H)$ *is Abelian.*
4. *If* $H$ *is normal in* $G$, *then* $\phi(H)$ *is normal in* $\phi(G)$.
5. *If* $|Ker\ \phi| = n$, *then* $\phi$ *is an* $n$*-to-1 mapping from* $G$ *to* $\bar{G}$.
6. *If* $|H| = n$, *the* $|\phi(H)|$ *divides* $n$.
7. *If* $\bar{K}$ *is a subgroup of* $\bar{G}$, *then* $\phi^{-1}(\bar{K}) = \{k \in G \mid \phi(k) \in \bar{K}\}$ *is a normal subgroup of* $G$.
8. *If* $\phi$ *is surjective and* $Ker\ \phi = \{e\}$, *then* $\phi$ *is an isomorphism from* $G$ *to* $\bar{G}$.

► **Corollary** ( Kernels are Normal ).

*Let $\phi$ be a group homomorphism from $G$ to $\bar{G}$. Then $Ker\ \phi$ is a normal subgroup of $G$.*

► **Theorem 10.3** ( First Isomorphism Theorem (Jordan, 1870)).

*Let $\phi$ be a group homomorphism from $G$ to $\bar{G}$. Then the mapping from $G/Ker\ \phi$ to $\phi(G)$ by $gKer\ \phi \to \phi(g)$ is an isomorphism. In symbols, $G/Ker\ \phi \approx \phi(G)$.*

► **Corollary.**

*If $\phi$ is a homomorphism from a finite group $G$ to $\bar{G}$, then $|\phi(G)|$ divides $|G|$ and $|\bar{G}|$.*

► **Theorem 10.4** ( Normal Subgroups are Kernels ).

*Every normal subgroup of a group $G$ is the kernel of a homomorphism of $G$. In particular, a normal subgroup $N$ is the kernel of the mapping $g \to gN$ from $G$ to $G/N$.*