0.1 Properties of Integers

Well Ordering Principle
Every nonempty set of positive integers contains a smallest number.

Theorem 0.1 ***Division Algorithm***
Let a and b be integers with $b > 0$. then there exist unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

Definition 0.1 ***Greatest Common Divisor, Relatively Prime Integers***
The *greatest common divisor* of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by $\gcd(a, b)$. When $\gcd(a, b) = 1$, we say that a and b are *relatively prime*.

Theorem 0.2 ***GCD Is a Linear Combination***
for any nonzero integers a and b, there exist 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 0.2.1
If a and b are relatively prime, then there exist integers s and t such that $as + bt = 1$.

Lemma 0.3 ***Euclid's Lemma*** $p \mid ab$ implies $p \mid a$ or $p \mid b$
If p is a prime that divides ab, then p divides a or p divides b.

Theorem 0.4 ***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. That is, if $n = p_1 p_2 \dots p_r$ and $n = q_1 q_2 \dots q_s$, where the p's and q's are primes, then $r = s$ and, after renumbering the q's, we have $p_i = q_i$ for all i.

Definition 0.2 ***Least Common Multiple***
The *least common multiple* of two nonzero integers a and b is the smallest positive integer that is a multiple of both a and b. We will denote this integer by $\text{lcm}(a, b)$.

0.2 Mathematical Induction

Theorem 0.5 ***First Principle of Mathematical Induction***
Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n + 1$ also belongs to S. Then, S contains every integer greater than or equal to a.

Theorem 0.6 ***Second Principle of Mathematical Induction***
Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

0.3 Equivalence Relations

Definition 0.3 ***Equivalence Relation***
An *equivalence relation* on a set S is a set R of ordered pairs of elements of S such that

1. $(a, a) \in R$ for all $a \in S$ (reflexive property).
2. $(a, b) \in R$ implies $(b, a) \in R$ (symmetric property).
3. $(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$ (transitive property).

Definition 0.4 ***Partition***
A *partition* of a set S is a collection of nonempty disjoint subsets of S whose union is S.

Theorem 0.7 ***Equivalence Classes Partition***
The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

0.4 Functions (Mappings)

Definition 0.5 ***Function (Mapping)***
A *function* (or *mapping*) ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B. The set A is called the *domain of* ϕ, and B is called the *range of* ϕ. If ϕ assigns b to a, then b is called the *image of* a *under* ϕ. The subset of B comprising all the images of elements of A is called the *image of* A *under* ϕ.

Definition 0.6 ***Composition of Functions***
Let $\phi : A \to B$ and $\psi : B \to C$. The *composition* $\psi\phi$ is the mapping from A to C defined by $(\psi\phi)(a) = \psi(\phi(a))$ for all a in A.

Definition 0.7 ***One-to-One Function***
A function ϕ from a set A is called *one-to-one* if for every $a_1, a_2 \in A$, $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.

Definition 0.8 ***Functions from A onto B***
A function ϕ from a set A to a set B is said to be *onto* B if each element of B is the image of at least one element of A. In symbols, $\phi : A \to B$ is onto if for each b in B there is at least one a in A such that $\phi(a) = b$.

Theorem 0.8 ***Properties of Functions***
Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$, then

1. $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (associativity).
2. If α and β are one-to-one, then $\beta\alpha$ is one-to-one.
3. If α and β are onto, then $\beta\alpha$ is onto.
4. If α is one-to-one and onto, then there is a function α^{-1} from B onto A such that $(\alpha^{-1}\alpha)(a) = a$ for all a in A and $(\alpha\alpha^{-1})(b) = b$ for all b in B.

2.1 Definition and Examples of Groups

Definition 2.1 ***Binary Operation***
Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G.

Definition 2.2 ***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 $ab = ba = e$.

2.2 Elementary Properties of Groups

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 right and left 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, $(ab)^{-1} = b^{-1}a^{-1}$.

3.1 Terminology and Notation

Definition 3.1 ***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 3.2 ***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, this would be $ng = 0$.) If no such integer exists, we say that g has *infinite order*. The order of an element g is denoted by $|g|$.

Definition 3.3 ***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.

3.2 Subgroup Tests

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. (In additive notation, if $a - b$ 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 let H be 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 finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Theorem 3.4 $\langle \mathbf{a} \rangle$ ***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 3.4 ***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,

$$Z(G) = \{a \in G \mid ax = xa, \ \forall \ x \in G\}$$

[The notation $Z(G)$ comes from the fact that the German word for center is *Zentrum*. The term was coined by J.A. de Séguier in 1904.]

Theorem 3.5 ***Center Is a Subgroup***
The center of a group G is a subgroup of G.

Definition 3.5 ***Centralizer of*** $\mathbf{a}$ ***in*** $\mathbf{G}$
Let a be a fixed element of a group G. The *centralizer of a in G*, $C(a)$, 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 $\mathbf{C(a)}$ ***Is a Subgroup***
For each a in a group G, the centralizer of a is a subgroup of G.

4.1 Properties of Cyclic Groups

Theorem 4.1 ***Criterion for*** $\mathbf{a^i = a^j}$
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 4.1.1 $|\mathbf{a}| = |\langle \mathbf{a} \rangle|$
For any group element a, $|a| = |\langle a \rangle|$.

Corollary 4.1.2 $\mathbf{a^k = e}$ *Implies That* $\mathbf{|a|}$ *Divides* $\mathbf{k}$
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 $\langle \mathbf{a^k} \rangle = \langle \mathbf{a^{gcd(n,k)}} \rangle$ *and* $\left|\mathbf{a^k}\right| = \mathbf{n/gcd(n,k)}$
Let a be an element of order n in a gruop and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $\left|a^k\right| = n/\gcd(n,k)$.

Corollary 4.2.1 *Orders of Elements in Finite Cyclic Groups*
In a finite cyclic group, the order of an element divides the order of the group.

Corollary 4.2.2 *Criterion for* $\langle \mathbf{a^i} \rangle = \langle \mathbf{a^j} \rangle$ *and* $\left|\mathbf{a^i}\right| = \left|\mathbf{a^j}\right|$
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 4.2.3 *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 $|a| = |\langle a^j \rangle|$ if and only if $\gcd(n,j) = 1$.

Corollary 4.2.4 *Generators of* $\mathbb{Z}_\mathbf{n}$
An integer k in $\mathbb{Z}_n$ is a generator of Z_n if and only if $\gcd(n,k) = 1$.

4.2 Classification of Subgroups of Cyclic Groups

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, $\langle a^{n/k} \rangle$.

Corollary 4.3.1 *Subgroups of* $\mathbb{Z}_\mathbf{n}$
For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.

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 4.4.1 *Number of Elements of Order* $\mathbf{d}$ *in a Finite Group*
In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

5.1 Definition and Notation

Definition 5.1 *Permutation of* $\mathbf{A}$*, Permutation Group of* $\mathbf{A}$
A *permutation* of a set A is a function from A to A that is both one-to-one and onto. A *permutation group* of a set A is a set of permutations of A that forms a group under function composition.

5.2 Cycle Notation

Definition 5.2
Consider the permutation

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

The assignment of values is as follows:

$$1 \mapsto 2 \qquad 2 \mapsto 1 \qquad 3 \mapsto 4 \qquad 4 \mapsto 6 \qquad 5 \mapsto 5 \qquad 6 \mapsto 3$$

Although mathematically satisfactory, such diagrams are cumbersome. Instead, we leave out the arrows and simply write $\alpha = (1, 2)(3, 4, 6)(5)$.

It is also worth noting that an expression of the form $(a_1, a_2, \ldots, a_m)$ is called a *cycle of length* m, or an m*-cycle*.

Example
To multiply cycles, consider the following permutations from S_8. Let $\alpha = (13)(27)(456)(8)$ and $\beta = (1237)(648)(5)$. (When the domain consists of single-digit integers, it is common practice to omit the commas between the digits.) What is the cycle form of $\alpha\beta$? Of course, one could say that $\alpha\beta = (13)(27)(456)(8)(1237)(648)(5)$, but it is usually more desirable to express a permutation in a *disjoint* cycle form (that is, the various cycles have no number in common). Well, keeping in mind that function composition is done from right to left and that each cycle that does not contain a symbol fixes the symbol, we observe that (5) fixes 1; (648) fixes 1; (1237) sends 1 to 2, (8) fixes 2; (456) fixes 2; (27) sends 2 to 7; and (13) fixes 7. So the net effect of $\alpha\beta$ is to send 1 to 7. Thus, we begin $\alpha\beta = (17\ldots)\ldots$. Now, repeating the entire process beginning with 7, we have, cycle by cycle, right to left,

$$7 \to 7 \to 7 \to 1 \to 1 \to 1 \to 1 \to 3,$$

so that $\alpha\beta = (173\ldots)\ldots$. Ultimately, we have $\alpha\beta = (1732)(48)(56)$. The important thing to bear in mind when multiplying cycles is to "keep moving" from one cycle to the next from right to left.

5.3 Properties of Permutations

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 $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Theorem 5.3 ***Order of a Permutation***
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 2-Cycles***
Every permutation in $S_n,\ n > 1$ is a product of 2-cycles.

Lemma
If $\varepsilon = \beta_1\beta_2 \ldots \beta_r$, where the β's are 2-cycles, then r is even.

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

$$\alpha = \beta_1\beta_2 \ldots \beta_r \quad \text{and} \quad \alpha = \gamma_1\gamma_2 \ldots \gamma_s,$$

where the β's and the γ's are 2-cycles, then r and s are both even or both odd.

Definition 5.3 ***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.

Definition 5.4 ***Alternating Group of Degree*** **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 $n!/2$.

6.1 Definition and Examples

Definition 6.1 ***Group Isomorphism***
An *isomorphism* ϕ from a group G to a group $\overline{G}$ is a one-to-one mapping (or function) from G onto $\overline{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b),\ \forall a, b \in G$$

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

6.2 Cayley's Theorem

Theorem 6.1 ***Cayley's Theorem***
Every group is isomorphic to a group of permutations.

6.3 Properties of Isomorphisms

Theorem 6.2 ***Properties of Isomorphisms Acting on Elements***
Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ carries the identity of G to the identity of $\overline{G}$.
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 $\overline{G} = \langle \phi(a) \rangle$.
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 $\overline{G}$.
7. If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

Theorem 6.3 ***Properties of Isomorphisms Acting on Groups***
Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ^{-1} is an isomorphisms from $\overline{G}$ onto G.
2. G is Abelian if and only if $\overline{G}$ is Abelian.
3. G is cyclic if and only if $\overline{G}$ is cyclic.
4. If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.
5. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{g \in G \mid \phi(g) \in \overline{K}\}$ is a subgroup of G.
6. $\phi(Z(G)) = Z(\overline{G})$.

6.4 Automorphisms

Definition 6.2 ***Automorphism***
An isomorphism from a group G onto itself is called an *automorphisms* of G.

Definition 6.3 ***Inner Automorphism Induced by*** **a**
Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ 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.

When G is a group, we use $\mathrm{Aut}(G)$ to denote the set of all automorphisms of G and $\mathrm{Inn}(G)$ to denote the set of all inner automorphisms of G.

Theorem 6.5 ***Aut***$(\mathbb{Z}_\mathbf{n}) \approx \mathbf{U(n)}$
For every positive integer n, $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $U(n)$.

7.1 Properties of Cosets

Definition 7.1 ***Coset of* H *in* G**
Let G be a group and let H be a nonempty 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. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.
4. $aH = bH$ if and only if $a \in bH$.
5. $aH = bH$ or $aH \cap bH = \emptyset$.
6. $aH = bH$ if and only if $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$ if and only if $H = aHa^{-1}$.
9. aH is a subgroup of G if and only if $a \in H$.

7.2 Lagrange's Theorem and Consequences

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 $|G| \,/\, |H|$.

Remark
A special name and notation have been adopted for the number of left (or right) cosets of a subgroup in a group. The *index* of a subgroup H in G is the number of distinct left cosets of H in G. This number is denoted by $|G : H|$.

Corollary 7.1.1 $|\mathbf{G} : \mathbf{H}| = |\mathbf{G}| \,/\, |\mathbf{H}|$
If G is a finite group and H is a subgroup of G, then $|G : H| = |G| \,/\, |H|$.

Corollary 7.1.2 $|\mathbf{a}|$ ***Divides*** $|\mathbf{G}|$
In a finite group, the order of each element of the group divides the order of the group.

Corollary 7.1.3 ***Groups of Prime Order Are Cyclic***
A group of prime order is cyclic.

Corollary 7.1.4 $\mathbf{a^{|G|} = e}$
Let G be a finite group, and let $a \in G$. Then, $a^{|G|} = e$.

Corollary 7.1.5 *Fermat's Little Theorem*
For every integer a and every prime p, $a^p \mod p = a \mod p$.

Theorem 7.2 $\mathbf{|HK| = |H|\,|K| \,/\, |H \cap K|}$
For two finite subgroups H and K of a group, define the set $HK = \{hk \mid h \in H, k \in K\}$. Then $|HK| = |H|\,|K| \,/\, |H \cap K|$.

Theorem 7.3 *Classification of Groups of order 2*p
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.

7.3 An Application of Cosets to Permutation Groups

Definition 7.2 *Stabilizer of a Point*
Let G be a group of permutations of a set S. For each i in S, let $\text{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$. We call $\text{stab}_G(i)$ the *stabilizer of i in G*.

Definition 7.3 *Orbit of a Point*
Let G be a group of permutations of a set S. For each s in S, let $\text{orb}_G(s) = \{\phi(s) \mid \phi \in G\}$. The set $\text{orb}_G(s)$ is a subset of S called the *orbit of s under G*. We use $|\text{orb}_G(s)|$ to denote the number of elements in $\text{orb}_G(s)$.

Theorem 7.4 *Orbit-Stabilizer Theorem*
Let G be a finite group of permutations of a set S. Then, for any i from S, $|G| = |\text{orb}_G(i)|\,|\text{stab}_G(i)|$.

7.4 The Rotation Group of a Cube and a Soccer Ball

Theorem 7.5 *The Rotation Group of a Cube*
The group of rotations of a cube is isomorphic to S_4.

8.1 Definition and Examples

Definition 8.1 *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 $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.

8.2 Properties of External Direct Products

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 component of the element. In symbols,

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

Theorem 8.2 ***Criterion for*** $\mathbf{G \oplus H}$ ***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 8.2.1 ***Criterion for*** $\mathbf{G_1 \oplus G_2 \oplus \cdots \oplus G_n}$ ***to Be Cyclic***
An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ 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 8.2.2 ***Criterion for*** $\mathbb{Z}_{\mathbf{n_1 n_2 \cdots n_k}} \approx \mathbb{Z}_{\mathbf{n_1}} \oplus \mathbb{Z}_{\mathbf{n_2}} \oplus \cdots \oplus \mathbb{Z}_{\mathbf{n_k}}$
Let $m = n_1 n_2 \ldots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

8.3 The Group of Units Modulo n as an External Direct Product

Remark
The U-groups provide a convenient way to illustrate the preceding ideas. We first introduce some notation. If k is a divisor of n, let

$$U_k(n) = \{x \in U(n) \mid x \mod k = 1\}$$

Theorem 8.3 $\mathbf{U(n)}$ ***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 8.3.1
Let $m = n_1 n_2 \ldots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then,

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$$

9.1 Normal Subgroups

Definition 9.1 ***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 $H \triangleleft G$.

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.

9.2 Factor Groups

Theorem 9.2 ***Factor Groups (O. Hölder, 1889)***
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 $(aH)(bH) = abH$.

9.3 Applications of Factor Groups

Theorem 9.3 G/Z *Theorem*
Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.

Theorem 9.4 $\mathbf{G/Z(G) \approx Inn(G)}$
For any group G, $G/Z(G)$ is isomorphic to $\text{Inn}(G)$.

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.

9.4 Internal Direct Products

Definition 9.2 *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 9.3 *Internal Direct Product* $\mathbf{H_1 \times H_2 \times \cdots \times H_n}$
Let $H_1, H_2, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the *internal direct product* of $H_1, H_2, \ldots, H_n$ and write $G = H_1 \times H_2 \times \cdots \times H_n$, if

1. $G = H_1 H_2 \ldots H_n = \{h_1 h_2 \ldots h_n \mid h_i \in H_i\}$,
2. $(H_1 H_2 \ldots H_n) \cap H_{i+1} = e$ for $i = 1, 2, \ldots, n-1$.

Theorem 9.6 $\mathbf{H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n}$
If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \ldots, H_n$, then G is isomorphic to the external direct product of $H_1, H_2 \ldots, H_n$.

Theorem 9.7 *Classification of Groups of Order* $\mathbf{p^2}$
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 9.7.1
If G is a group of order p^2, where p is a prime, then G is Abelian.

10.1 Definition and Examples

Definition 10.1 *Group Homomorphism*
A *homomorphism* ϕ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Definition 10.2 *Kernel of a Homomorphism*
The *kernel* of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by $\ker \phi$.

10.2 Properties of Homomorphisms

Theorem 10.1 ***Properties of Elements Under Homomorphisms***
Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G. Then

1. ϕ carries the identity of G to $\overline{G}$.
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 ϕ be a homomorphism from a group G to a group $\overline{G}$ and let H be a subgroup of G. Then

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.
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 ϕ is an n-to-1 mapping from G onto $\phi(G)$.
6. If $|H| = n$, then $|\phi(H)|$ divides n.
7. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a subgroup of G.
8. If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a normal subgroup of G.
9. If ϕ is onto and $\ker\phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.

Corollary 10.2.1 ***Kernels Are Normal***
Let ϕ be a group homomorphism from G to $\overline{G}$. Then $\ker\phi$ is a normal subgroup of G.

10.3 The First Isomorphism Theorem

Theorem 10.3 ***First Isomorphism Theorem***
Let ϕ be a group homomorphism from G to $\overline{G}$. Then the mapping from $G/\ker\phi$ to $\phi(G)$, given by $g\ker\phi \to \phi(g)$, is an isomorphism. In symbols, $G/\ker\phi \approx \phi(G)$.

Theorem 10.4 ***Second Isomorphism Theorem***
Let G be a group, $K \leq G$ and $H \lhd G$. Then

(a) The set

$$HK = \{hk \mid h \in H,\ k \in K\}$$

is a subgroup of G

(b) $H \cap K$ is a normal subgroup of K.

(c) The groups HK/H and $K/(H \cap K)$ are isomorphic.

Theorem 10.5 ***Third Isomorphism Theorem***
Let G be a group and $H \lhd G$.

(a) If $K \leq G$ and $H \subseteq K \subseteq G$, then K/H is a subgroup of G/H.

(b) Every subgroup of G/H is of the form K/H, for some $K \leq G$ such that $H \subseteq K \subseteq G$.

(c) If $K \lhd G$ and $H \subseteq K \subseteq G$, then K/H is a normal subgroup of G/H.

(d) Every normal subgroup of G/H is of the form K/H, for some $K \lhd G$ such that $H \subseteq K \subseteq G$.

(e) If $K \lhd G$ and $H \subseteq K \subseteq G$, then the groups $(G/H)/(K/H)$ and G/K are isomorphic.

Corollary 10.5.1
If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $\left|\overline{G}\right|$.

Theorem 10.6 ***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.

11.1 The Fundamental Theorem of Finite Abelian Groups

Theorem 11.1 ***Fundamental Theorem of Finite Abelian Groups***
Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

11.2 The Isomorphism Classes of Abelian Groups

Remark ***Greedy Algorithm for an Abelian Group of Order*** $\mathbf{p^n}$
The Fundamental Theorem is extremely powerful. As an application, we can use it as an algorithm for constructing all Abelian groups of any order. Let's look at Abelian groups of a certain order n, where n has two or more distinct prime divisors.

1. Compute the orders of the elements of the group G

2. Select an element a_1 of maximum order and define $G_1 = \langle a_1 \rangle$. Set $i = 1$.

3. If $|G| = |G_i|$, stop. Otherwise, replace i by $i + 1$.

4. Select an element a_i of maximum order p^k such that $p^k \leq |G| / |G_{i-1}|$ and none of $a_i, a_i^p, a_i^{p^2}, \ldots, a_i^{p^{k-1}}$ is in G_{i-1}, and define $G_i = G_{i-1} \times \langle a_i \rangle$.

5. Return to step 3.

Corollary 11.1.1 ***Existence of Subgroups of Abelian Groups***
If m divides the order of a finite Abelian group G, then G has a subgroup of order m.

11.3 Proof of the Fundamental Theorem

Lemma 11.2
Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.

Lemma 11.3
Let G be an Abelian group of prime-power order and let a be an element of maximum order in G. Then G can be written in the form $\langle a \rangle \times K$.

Lemma 11.4
A finite Abelian group of prime-power order is an internal direct product of cyclic groups.

Lemma 11.5
Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the H's and K's are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

24.1 Conjugacy Classes

Definition 24.1 ***Conjugacy Class of*** **a**
Let a and b be elements of a group G. We say that a and b are *conjugate* in G (and call b the *conjugate* of a) if $xax^{-1} = b$ for some x in G. The *conjugacy class of* a is the set $\text{cl}(a) = \{xax^{-1} \mid x \in G\}$.

Theorem 24.1 ***Number of Conjugates of*** **a**
Let G be a finite group and let a be an element of G. Then, $|\text{cl}(a)| = |G : C(a)|$.

Corollary 24.1.1 $|\text{cl}(\mathbf{a})|$ ***Divides*** $|\mathbf{G}|$
In a finite group, $|\text{cl}(a)|$ divides $|G|$.

24.2 The Class Equation

Corollary 24.1.2 ***Class Equation***
For any finite group G,

$$|G| = \sum |G : C(a)|$$

where the sum runs over one element of a from each conjugacy class of G.

Theorem 24.2 p-*Groups Have Nontrivial Centers*
Let G be a nontrivial finite group whose order is a power of a prime p. Then $\mathbb{Z}(G)$ has more than one element.

Corollary 24.2.1 *Groups of Order* $\mathbf{p^2}$ *Are Abelian*
If $|G| = p^2$, where p is prime, then G is Abelian.

24.3 The Sylow Theorems

Theorem 24.3 *Sylow's First Theorem*
Let G finite group and p prime. p^k divides $|G|$
$\implies \exists$ at least one $H \leq G$ such that $|H| = p^k$.

Definition 24.2 *Sylow* p-*Subgroup*
Let G be a finite group and let p be a prime. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a *Sylow p-subgroup of G*.

Corollary 24.3.1 *Cauchy's Theorem*
Let G be a finite group and let p be a prime that divides the order of G. Then G has an element of order p.

Definition 24.3 *Conjugate Subgroups*
Let H and K be subgroups of a group G. We say that H and K are *conjugate* in G if there is an element in G such that $H = gKg^{-1}$.

Theorem 24.4 *Sylow's Second Theorem*
Let G finite group, $H \leq G$, $|H|$ is a power of a prime p
$\implies$ H is contained in some Sylow p-subgroup of G.

Theorem 24.5 *Sylow's Third Theorem*
Let $|G| = p^k m$, p prime where p does not divide m
$\implies$ # of Sylow p-sgp of $G = n_p \equiv 1 \pmod{p}$ and $n_p | m$.
Furthermore, any two Sylow p-sgp of G are conjugate.

Corollary 24.5.1 *A Unique Sylow* p-*Subgroup Is Normal*
A Sylow p-subgroup of a finite group G is a normal subgroup of G if and only if it is the only Sylow p-subgroup of G.

24.4 Applications of Sylow Theorems

Theorem 24.6 *Cyclic Groups of Order* pq
If G is a group of order pq, where p and q are primes, $p < q$, and p does not divide $q - 1$, then G is cyclic. In particular, G is isomorphic to $\mathbb{Z}_{pq}$.