

Contemporary Abstract Algebra Theorems and Definitions

Joseph McGuire

August 14th, 2020

1 Groups

1.1 Introduction to Groups

Definition 1 (Partition) Suppose $a, b \in \mathbb{R}$ with $a < b$. A partition of $[a, b]$ is a finite list of the form x_0, x_1, \dots, x_n , where

$$a = x_0 < x_1 < \dots < x_n = b.$$

Definition 2 (Notation for Infimum and Supremum of a Function) If f is a real-valued function and A is a subset of the domain of f , then

$$\inf_A f = \inf\{f(x) : x \in A\} \text{ and } \sup_A f = \sup\{f(x) : x \in A\}.$$

Definition 3 (Lower and Upper Riemann Sums) Suppose $f : [a, b] \rightarrow \mathbb{R}$ is a bounded function and P is a partition x_0, \dots, x_n of $[a, b]$. The lower Riemann sum $L(f, P, [a, b])$ and the upper Riemann sum $U(f, P, [a, b])$ are defined by

$$L(f, P, [a, b]) = \sum_{j=1}^n (x_j - x_{j-1}) \inf_{[x_{j-1}, x_j]} f$$

and

$$U(f, P, [a, b]) = \sum_{j=1}^n (x_j - x_{j-1}) \sup_{[x_{j-1}, x_j]} f.$$

1.2 Groups

Definition 4 (Binary Operations) 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 5 (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 ab . We say that 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's an element $e \in G$ (called the identity) such that $ae = ea = a$, for all $a \in G$.
3. *Inverses.* For each element $a \in G$, there's an element $b \in G$ (called the inverse of a) such that $ab = ba = e$.

Theorem 6 (Uniqueness of the Identity) In a group G , there's only one identity element.

Theorem 7 (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 8 (Uniqueness of Inverses) For each element $a \in G$, there's a unique element $b \in G$ such that $ab = ba = e$.

Theorem 9 (Socks-Shoes Property) For group elements a, b , $(ab)^{-1} = b^{-1}a^{-1}$.

1.3 Finite Groups; Subgroups

Definition 10 (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 11 (Order of an Element) The order of an element $g \in G$ 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 $|g|$.

Definition 12 (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 .

Theorem 13 (One-Step Subgroup Test) Let G be a group and H a nonempty subset of G . If $ab^{-1} \in H$ whenever $a, b \in H$, then H is a subgroup of G . (In additive notation, if $a - b \in H$ whenever $a, b \in H$, then H is a subgroup of G .)

Theorem 14 (Two-Step Subgroup Test) Let G be a group and let H be a nonempty subset of G . If $ab \in H$ whenever $a, b \in H$ (H is closed under the operation), and $a^{-1} \in H$ whenever $a \in H$ (H is closed under taking inverses), then H is a subgroup of G .

Theorem 15 (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 .

Theorem 16 ($\langle a \rangle$ is a Subgroup) Let G be a group, and let $a \in G$. Then $\langle a \rangle$ is a subgroup of G .

Definition 17 (Center of a Group) The center, $Z(G)$, of a group G is a subset of elements in G such that commute with every element of G . In symbols, $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$.

Theorem 18 (Center is a Subgroup) The center of a group G is a subgroup of G .

Definition 19 (Centralizer of a in 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 20 ($C(a)$ is a subgroup) For each a in a group G , the centralizer of a is a subgroup of G .

1.4 Cyclic Groups

Theorem 21 (Criterion for $a^i = a^j$) Let G be a group, and let $a \in G$. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say, n , then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.

Corollary 22 ($|a| = |\langle a \rangle|$) For any group element a , $|a| = |\langle a \rangle|$.

Corollary 23 ($a^k = e$ 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 24 ($\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$) 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 $|a^k| = n/\gcd(n,k)$.

Corollary 25 (Orders of Elements in Finite Cyclic Groups) In a finite cyclic group, the order of an element divides the order of the group.

Corollary 26 (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 27 (Generators for 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 28 (Generators of \mathbb{Z}_n) An integer $k \in \mathbb{Z}_n$ is a generator of \mathbb{Z}_n if and only if $\gcd(n, k) = 1$.

Theorem 29 (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 30 (Subgroups of \mathbb{Z}_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 31 (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 $\phi(d)$. (ϕ is the Euler phi function, the number of positive integers less than a number that are relatively prime to that number)

Corollary 32 (Number of Elements of Order d in a Finite Group) In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

1.5 Permutation Groups

Definition 33 (Permutation of A , Permutation Group of 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.

Theorem 34 (Products of Disjoint Cycles) Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem 35 (Disjoint Cycles Commute) If the pair of cycles $\alpha = (a_1, a_2, \dots, a_m)$ and $\beta = (b_1, b_2, \dots, b_n)$ have no common entries, then $\alpha\beta = \beta\alpha$.

Theorem 36 (Orders 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 37 (Product of 2-Cycles) Every permutation in S_n , $n > 1$, is a product of 2-cycles.

Lemma 38 If $\epsilon = \beta_1\beta_2\cdots\beta_r$, where the β 's are 2-cycles, then r is even.

Theorem 39 (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 $\alpha = \beta_1\beta_2\cdots\beta_r$ and $\alpha = \gamma_1\gamma_2\cdots\gamma_s$, where β 's and the γ 's are 2-cycles, then r and s are both even or both odd.

Definition 40 (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 41 (Even Permutations Form a Group) The set of even permutations in S_n forms a subgroup of S_n .

Definition 42 (Alternating Group of Degree n) The group of even permutations of n symbols is denoted A_n and is called the alternating group of degree n .

Theorem 43 For $n > 1$, A_n has order $n!/2$.

1.6 Isomorphisms

Definition 44 (Group Isomorphism) An isomorphism ϕ from a group G to a group \bar{G} is a one-to-one mapping (or function) from G onto \bar{G} that preserves the group operation. That is, $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. If there's an isomorphism from G onto \bar{G} , we say that G and \bar{G} are isomorphic and write $G = \bar{G}$.

Theorem 45 (Cayley's Theorem) Every group is isomorphic to a group of permutations.

Theorem 46 (Properties of Isomorphisms Acting on Elements) Suppose that ϕ is an isomorphism from a group G onto a group \bar{G} . Then

1. ϕ carries the identity of G to the identity of \bar{G} .
2. For every integer n and for every group elements $a \in G$, $\phi(a^n) = [\phi(a)]^n$.
3. For any elements $a, b \in G$, 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 47 (Properties of Isomorphism Acting on Groups) Suppose that ϕ is an isomorphism from a group G onto a group \bar{G} . Then

1. ϕ^{-1} is an isomorphism from \bar{G} onto 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 $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of \bar{G} .
5. If \bar{K} is a subgroup of \bar{G} , then $\phi^{-1}(\bar{K}) = \{g \in G | \phi(g) \in \bar{K}\}$ is a subgroup of G .
6. $\phi(Z(G)) = Z(\bar{G})$.

Definition 48 (Automorphism) An isomorphism from a group G onto itself is called an automorphism of G .

Definition 49 (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 50 ($\text{Aut}(G)$ and $\text{Inn}(G)$ are Groups) The set of automorphism of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

1.7 Cosets and Lagrange's Theorem

Definition 51 (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 $\{ah | h \in H\}$ is denoted by aH . Analogously, $Ha = \{ha | h \in H\}$ and $aHa^{-1} = \{aha^{-1} | h \in H\}$. When H is a subgroup of G , the set aH is called the left coset of H containing a , whereas Ha is called the right coset of H in G containing a . In the 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 52 (Properties of Cosets) Let H be a subgroup of G , and let $a, b \in G$. Then

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

Theorem 53 (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 $|G|/|H|$.

Corollary 54 ($|G:H| = |G|/|H|$) If G is a finite group and H is a subgroup of G , then $|G:H| = |G|/|H|$.

Corollary 55 ($|a|$ Divides $|G|$) In a finite group, the order of each element of the group divides the order of the group.

Corollary 56 (Groups of Prime Order Are Cyclic) A group of prime order is cyclic.

Corollary 57 ($a^{|G|} = e$) Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.

Corollary 58 (Fermat's Little Theorem) For every integer a and every prime p , $a^p \mod p = a \mod p$.

Theorem 59 ($|HK| = |H||K|/|H \cap K|$) For two finite subgroups H and K of a group, define the set $HK = \{hk | h \in H, k \in K\}$. Then $|HK| = |H||K|/|H \cap K|$.

Theorem 60 (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 .

Definition 61 (Stabilizer of a Point) Let G be a group of permutations of a set S . For each $i \in S$, let $\text{stab}_G(i) = \{\phi \in G | \phi(i) = i\}$. We call $\{\text{stab}_G(i)\}$ the stabilizer of i in G .

Definition 62 (Orbit of a Point) Let G be a group of permutations of a set S . For each $s \in S$, let $\text{orb}_G(s) = \{\phi(s) | \phi \in G\}$. 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 63 (Orbit-Stabilizer Theorem) Let G be a finite group of permutations of a set S . Then, for any i from S , $|G| = |\text{orb}_G(i)||\text{stab}_G(i)|$.

1.8 External Direct Products

Definition 64 (External Direct Product) Let G_1, \dots, G_n be a finite collection of groups. The external direct product of G_1, \dots, G_n , written as $G_1 \oplus G_2 \oplus \dots \oplus G_n$, is the set of all n -tuples for which the i th component is an element of G_i and the operation is component-wise.

Theorem 65 (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, $|(g_1, \dots, g_n)| = \text{lcm}(|g_1|, \dots, |g_n|)$.

Theorem 66 (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 $\gcd(|G|, |H|) = 1$.

Corollary 67 (Criterion for $G_1 \oplus \dots \oplus G_n$ to be Cyclic) An external direct product $G_1 \oplus \dots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $\gcd(|G_i|, |G_j|) = 1$ when $i \neq j$.

Corollary 68 (Criterion for $\mathbb{Z}_{n_1 n_2 \dots n_k} \approx \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k}$) Let $m = n_1 \dots n_k$. Then \mathbb{Z}_m is isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_k}$ if and only if $\gcd(n_i, n_j) = 1$ when $i \neq j$.

Theorem 69 ($U(n)$ as an External Direct Product) Suppose that $\gcd(s, t) = 1$. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. In short, $U(st) \approx U(s)U(t)$. Moreover, $U_s(st)$ is isomorphic to $U(t)$ and $U_t(st)$ is isomorphic to $U(s)$. ($U_k(n) = \{x \in U(n) | x \bmod k = 1\}$)

Corollary 70 Let $m = n_1 \dots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then $U(m) \approx U(n_1) \oplus U(n_2) \oplus \dots \oplus U(n_k)$.

1.9 Normal Subgroups and Factor Groups

Definition 71 (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 72 (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 73 (Factor Groups) Let G be a group and let H be a normal subgroup of G . The set $G/H = \{aH | a \in G\}$ is a group under the operation $(aH)(bH) = (ab)H$.

Theorem 74 (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 75 ($G/Z(G) \approx \text{Inn}(G)$) For any group G , $G/Z(G)$ is isomorphic to $\text{Inn}(G)$.

Theorem 76 (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 77 (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, K are normal subgroups of G and $G = HK$ and $H \cap K = \{e\}$.

Definition 78 (Internal Direct Product $H_1 \times \dots \times H_n$) Let H_1, \dots, H_n be a finite collection of normal subgroups of G . We say that G is the internal direct product of H_1, \dots, H_n and write $G = H_1 \times H_2 \times \dots \times H_n$, if

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

Theorem 79 ($H_1 \times \dots \times H_n \approx H_1 \oplus \dots \oplus H_n$) If a group G is the internal direct product of a finite number of subgroups H_1, \dots, H_n , then G is isomorphic to the external direct product of H_1, \dots, H_n .

Theorem 80 (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 81 If G is a group of order p^2 , where p is a prime, then G is Abelian.

1.10 Groups Homomorphisms

Definition 82 (Group Homomorphism) A homomorphism ϕ from a group G to a group \bar{G} is a mapping from G into \bar{G} that preserves the group operation; that is $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Definition 83 (Kernel of a Homomorphism) The kernel of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G | \phi(x) = e\}$. The kernel of ϕ is denoted $\ker(\phi)$.

Theorem 84 (Properties of Elements Under Homomorphisms) Let ϕ be a homomorphism from a group G to a group \bar{G} and let g be an element of G . Then

1. ϕ carries the identity of G to the identity of \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 $\phi^{-1}(g') = \{x \in G | \phi(x) = g'\} = g\ker(\phi)$

Theorem 85 Let ϕ be a homomorphism from a group G to a group \bar{G} and let H be a subgroup of G . Then

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

Corollary 86 (Kernels Are Normal) Let ϕ be a group homomorphism from G to \bar{G} . Then $\ker \phi$ is a normal subgroup of G .

Theorem 87 (First Isomorphism Theorem) Let ϕ be a group homomorphism from G to \bar{G} . Then the mapping from $G/\ker \phi$ to $\phi(G)$, given by $g\ker \phi \rightarrow \phi(g)$, is an isomorphism. In symbols, $G/\ker \phi \approx \phi(G)$.

Corollary 88 If ϕ is a homomorphism from a finite group G to \bar{G} , then $|\phi(G)|$ divides $|G|$ and $|\bar{G}|$.

Theorem 89 (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 $g \rightarrow gN$ from G to G/N .

1.11 Fundamental Theorem of Finite Abelian Groups

Theorem 90 (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.

Corollary 91 (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 .

Lemma 92 Let G be a finite Abelian group of order $p^n m$, where p is a prime that doesn't divide m . Then $G = H \times K$, where $H = \{x \in G | x^{p^n} = e\}$ and $K = \{x \in G | x^m = e\}$. Moreover, $|H| = p^n$.

Lemma 93 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 94 A finite Abelian group of prime-power order is an internal product of cyclic groups.

Lemma 95 Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \dots \times H_m$ and $G = K_1 \times \dots \times K_n$, where the H 's and K 's are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \dots \geq |H_m|$ and $|K_1| \geq \dots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i .

2 Rings

2.1 Introduction to Rings

Definition 96 (Ring) A ring R is a set with two binary operations, addition (denoted $a + b$) and multiplication (denoted by ab), such that for all $a, b, c \in R$:

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. There's an additive identity 0 . That is, there's an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.
4. There's an element $-a \in R$ such that $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Theorem 97 (Rules of Multiplication) Let a, b, c belong to a ring R . Then

1. $a0 = 0a = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

Furthermore if R has unity element 1 , then

1. $(-1)a = -a$.
2. $(-1)(-1) = 1$.

Theorem 98 (Uniqueness of the Unity and Inverses) If a ring has a unity, it's unique. If a ring element has a multiplicative inverse, it's unique.

Definition 99 (Subring) A subset S of a ring R is a subring of R if S is itself a ring with the operations of R .

Theorem 100 (Subring Test) A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication - that is, if $a - b$ and ab are in S whenever $a, b \in S$.

2.2 Integral Domains

Definition 101 (Zero-Divisors) A zero-divisor is a nonzero element a of a commutative ring R such that there's a nonzero element $b \in R$ with $ab = 0$.

Definition 102 (Integral Domain) An integral domain is a commutative ring with unity and no zero-divisors.

Theorem 103 (Cancellation) Let a, b, c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Definition 104 (Field) A field is a commutative ring with unity in which every nonzero element is a unit.

Theorem 105 (Finite Integral Domains are Fields) A finite integral domain is a field.

Corollary 106 (\mathbb{Z}_p is a Field) For every prime p , \mathbb{Z}_p , the ring of integers modulo p is a field.

Definition 107 (Characteristic of a Ring) The characteristic of a ring R is the least positive integer n such that $nx = 0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0 . The characteristic of R is denoted by $\text{char}R$.

Theorem 108 (Characteristic of an Integral Domain) The characteristic of an integral domain is 0 or prime.

2.3 Ideals and Factor Rings

Definition 109 (Ideal) A subring A of a ring R is called a (two-sided) ideal of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A .

Theorem 110 (Ideal Test) A nonempty subset A of a ring R is an ideal of R if

1. $a - b \in A$ whenever $a, b \in A$.
2. ra and ar are in A whenever $a \in A$ and $r \in R$.

Theorem 111 (Existence of Factor Rings) Let R be a ring and let A be a subring of R . The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations $(s + A) + (t + A) = (s + t) + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R .

Definition 112 (Prime Ideal, Maximal Ideal) A prime ideal A of a commutative ring R is a proper ideal of R such that, $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A maximal ideal of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Theorem 113 (R/A is an Integral Domain if and only if A is Prime) Let R be a commutative ring with unity and let A be an ideal of R . Then R/A is an integral domain if and only if A is prime.

Theorem 114 (R/A is a Field if and only if A is Maximal) Let R be a commutative ring with unity and let A be an ideal of R . Then R/A is a field if and only if A is maximal.

2.4 Ring Homomorphisms

Definition 115 (Ring Homomorphism, Ring Isomorphism) A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all $a, b \in R$, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. A ring homomorphism that is both one-to-one and onto is called a ring isomorphism.

Theorem 116 (Properties of Ring Homomorphisms) Let ϕ be a ring homomorphism from a ring R to a ring S . Let A be a subring of R and let B be an ideal of S .]

1. For any $r \in R$ and any positive integer n , $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.
2. $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S .
3. If A is an ideal and ϕ is onto S , then $\phi(A)$ is an ideal.
4. $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R .
5. If R is commutative, then $\phi(R)$ is commutative.
6. If R has a unity 1 , $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S .
7. ϕ is an isomorphism if and only if ϕ is onto and $\ker(\phi) = \{r \in R \mid \phi(r) = 0\} = \{0\}$.
8. If ϕ is an isomorphism from R onto S , then ϕ^{-1} is an isomorphism from S onto R .

Theorem 117 (Kernels are Ideals) Let ϕ be a ring homomorphism from a ring R to a ring S . Then $\ker(\phi) = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R .

Theorem 118 (First Isomorphism Theorem for Rings) Let ϕ be a ring homomorphism from R to S . Then the mapping from $R/\ker(\phi)$ to $\phi(R)$, given by $r + \ker(\phi) \rightarrow \phi(r)$, is an isomorphism. In symbols, $R/\ker(\phi) \approx \phi(R)$.

Theorem 119 (Ideals are Kernels) Every ideal of a ring R is the kernel of a ring homomorphism of R . In particular, an ideal A is the kernel of the mapping $r \rightarrow r + A$ from R to R/A .

Theorem 120 (Homomorphism from \mathbb{Z} to a Ring with Unity) Let R be a ring with unity 1 . The mapping $\phi : \mathbb{Z} \rightarrow R$ given by $n \rightarrow n \cdot 1$ is a ring homomorphism.

Corollary 121 (A Ring with Unity Contains \mathbb{Z}_n or \mathbb{Z}) If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to \mathbb{Z}_n . If the characteristic of R is 0 , then R contains a subring isomorphic to \mathbb{Z} .

Corollary 122 (\mathbb{Z}_m is a Homomorphic Image of \mathbb{Z}) For any positive integer m , the mapping of $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_m$ given by $x \rightarrow x \pmod{m}$ is a ring homomorphism.

Corollary 123 (A Field Contains \mathbb{Z}_p or \mathbb{Q}) If F is a field of characteristic p , then F contains a subfield isomorphic to \mathbb{Z}_p . If F is a field of characteristic 0, then F contains a subfield isomorphic to the rational numbers.

Theorem 124 (Field of Quotients) Let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D .

2.5 Polynomial Rings

Definition 125 (Ring of Polynomials over R) Let R be a commutative ring. The set of formal symbols $R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in R, n \text{ is a nonnegative integer}\}$ is called the ring of polynomials over R in the indeterminate x . Two elements are considered equal if and only if $a_i = b_i$ for all nonnegative integers i . (Define $a_i = 0$ when $i > n$ and $b_i = 0$, when $i > m$.)

Definition 126 (Addition and Multiplication in R) Let R be a commutative ring and let $f(x) = a_n x^n + \dots + a_1 x + a_0, g(x) = b_m x^m + \dots + b_1 x + b_0$ belong to $R[x]$. Then $f(x) + g(x) = (a_s + b_s)x^s + \dots + (a_1 + b_1)x + a_0 + b_0$, where s is the maximum of $m, n, a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$. Also $f(x)g(x) = c_{m+n}x^{m+n} + \dots + c_1 x + c_0$, where $c_k = a_k b_0 + a_{k-1} b_1 + \dots + a_1 b_{k-1} + a_0 b_k$ for $k = 0, \dots, m+n$.

Theorem 127 (D an Integral Domain Implies $D(\text{Polynomial})$ is an Integral Domain) If D is an integral domain, then $D[x]$ is an integral domain.

Theorem 128 (Division Algorithms for F) Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

Corollary 129 (Remainder Theorem) Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Corollary 130 (Factor Theorem) Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Corollary 131 (Polynomials of Degree n Have at Most n Zeros) A polynomial of degree n over a field has at most n zeros, counting multiplicity.

Theorem 132 ($F(\text{Poly})$ is a PID) Let F be a field. Then $F[x]$ is a principal ideal domain.

Theorem 133 (Criterion for $I = \langle g(x) \rangle$) Let F be a field, I a nonzero ideal in $F[x]$, and $g(x)$ an element of $F[x]$. Then $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I .

2.6 Factorization of Polynomials

Definition 134 (Irreducible Polynomial, Reducible Polynomial) Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unity in $D[x]$ is said to be irreducible over D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero nonunity element of $D[x]$ that's not irreducible over D is called reducible over D .

Theorem 135 (Reducibility Test for Degrees 2 and 3) Let F be a field. If $f(x) \in F[x]$ and $\deg(f(x))$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F .

Definition 136 (Content of a Polynomial, Primitive Polynomial) The content of a nonzero polynomial $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$, where a_i 's are integers, is the greatest common divisor of the integers a_n, a_{n-1}, \dots, a_0 . A primitive polynomial is an element of $\mathbb{Z}[x]$ with content 1.

Lemma 137 (Gauss's Lemma) The product of two primitive polynomials is primitive.

Theorem 138 (Reducibility over \mathbb{Q} implies Reducibility over \mathbb{Z}) Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over \mathbb{Q} , then it's reducible over \mathbb{Z} .

Theorem 139 (\pmod{p} Irreducibility Test) Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg(f(x)) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p . If $\bar{f}(x)$ is irreducible over \mathbb{Z}_p and $\deg(\bar{f}(x)) = \deg(f(x))$, then $f(x)$ is irreducible over \mathbb{Q} .

Theorem 140 (Eisenstein's Criterion) Let $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$. If there's a prime p such that $p \nmid a_n, p \mid a_{n-1}, \dots, p \mid a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over \mathbb{Q} .

Corollary 141 (Irreducibility of p^{th} Cyclotomic Polynomial) For any prime p , the p^{th} cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$ is irreducible over \mathbb{Q} .

Theorem 142 ($\langle p(x) \rangle$ is Maximal if and Only if $p(x)$ is irreducible) Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F .

Corollary 143 ($F[x] / \langle p(x) \rangle$ is a Field) Let F be a field and $p(x)$ be an irreducible polynomial over F . Then $F[x] / \langle p(x) \rangle$ is a field.

Corollary 144 ($p(x) \mid a(x)b(x)$ Implies $p(x) \mid a(x)$ or $p(x) \mid b(x)$) Let F be a field and let $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Theorem 145 (Unique Factorization in $\mathbb{Z}[x]$) Every polynomial in $\mathbb{Z}[x]$ that isn't the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form $b_1 b_2 \dots b_s p_1(x) p_2(x) \dots p_m(x)$, where the b_i 's are irreducible polynomials of degree 0 and the $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore, if $b_1 b_2 \dots b_s p_1(x) p_2(x) \dots p_m(x) = c_1 c_2 \dots c_t q_1(x) q_2(x) \dots q_n(x)$, where the b_i 's and c_i 's are irreducible polynomials of degree 0 and the $p_i(x)$'s and $q_i(x)$'s are irreducible polynomials of positive degree, then $s = t, m = n$, and, after renumbering the c 's and $q(x)$'s, we have $b_i = \pm c_i$ for $i = 1, \dots, s$ and $p_i(x) = \pm q_i(x)$ for $i = 1, \dots, m$.

2.7 Divisibility in Integral Domains

Definition 146 (Associates, Irreducibles, Primes) Elements a, b of an integral domain D are called associates if $a = ub$ where u is a unit in D . A nonzero element a of an integral domain D is called an irreducible if a isn't a unit and, whenever $b, c \in D$ with $a = bc$, then b or c is a unit. A nonzero element a of an integral domain D is called a prime if a isn't a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Theorem 147 (Prime Implies Irreducible) In an integral domain, every prime is an irreducible.

Theorem 148 (PID implies Irreducible Equals Prime) In a principal ideal domain, an element is an irreducible if and only if it's prime.

Definition 149 (Unique Factorization Domain (UFD)) An integral domain D is a unique factorization domain if

1. every nonzero element of D that isn't a unit can be written as a product of irreducibles of D ; and
2. the factorization into irreducibles is unique up to associates and the order in which the factors appear.

Lemma 150 (Ascending Chain Condition for a PID) In a principal ideal domain, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \dots$ must be finite length.

Theorem 151 (PID implies UFD) Every principal ideal domain is a unique factorization domain.

Corollary 152 ($F[x]$ is a UFD) Let F be a field. Then $F[x]$ is a unique factorization domain.

Definition 153 (Euclidean Domain (ED)) An integral domain D is called a Euclidean domain if there's a function d (called the measure) from a nonzero elements of D to the nonnegative integers such that

1. $d(a) \leq d(ab)$ for all nonzero $a, b \in D$; and
2. if $a, b \in D, b \neq 0$, then there exists elements $q, r \in D$ such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Theorem 154 (ED Implies PID) Every Euclidean domain is a principal ideal domain.

Corollary 155 (ED Implies UFD) Every Euclidean domain is a unique factorization domain.

Theorem 156 (D is a UFD implies $D[x]$ a UFD) If D is a unique factorization domain, then $D[x]$ is a unique factorization domain.

3 Fields

3.1 Vector Spaces

Definition 157 (Vector Spaces) A set V is said to be a vector space over a field F if V is an Abelian group under addition (denoted by $+$) and, if for each $a \in F$ and $v \in V$, there's an element $av \in V$ such that the following conditions holds for all $a, b \in F$ and $u, v \in V$.

1. $a(v + u) = av + au$
2. $(a + b)v = av + bv$
3. $a(bv) = (ab)v$
4. $1v = v$

Definition 158 (Subspaces) Let V be a vector space over a field F and let U be a subset of V . We say that U is a subspace of V if U is also a vector space over F under the operations of V .

Definition 159 (Linear Dependent, Linear Independent) A set S of vectors is said to be linearly dependent over a field F if there are vectors v_1, \dots, v_n from S and element a_1, \dots, a_n from F not all zero, such that $a_1v_1 + \dots + a_nv_n = 0$. A set of vectors that's not linearly dependent over F is called linearly independent over F .

Definition 160 (Basis) Let V be a vector space over F . A subset B of V is called a basis for V if B is linearly independent over B and every element of V is a linear combination of elements in B .

Theorem 161 (Invariance of Basis Size) If $\{u_1, \dots, u_m\}$ and $\{w_1, \dots, w_n\}$ are both bases of a vector space V over a field F , then $m = n$.

Definition 162 (Dimension) A vector space that has a basis consisting of n elements is said to have dimension n . For completeness, the trivial vector space $\{0\}$ is said to be spanned by the empty set and to have dimension 0.

3.2 Extension Fields

Definition 163 (Extension Fields) A field E is an extension field of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F ,

Theorem 164 (Fundamental Theorem of Field Theory) Let F be a field and $f(x)$ be a nonconstant polynomial in $F[x]$. Then there's an extension field E of F in which $f(x)$ has a zero.

Definition 165 (Splitting Field) Let E be an extension field of F and let $f(x) \in F[x]$ with degree at least 1. We say that $f(x)$ splits in E if there are elements $a \in F$ and $a_1, a_2, \dots, a_n \in E$ such that $f(x) = a(x - a_1)(x - a_2) \dots (x - a_n)$. We call E a splitting field for $f(x)$ over F if $E = F(a_1, \dots, a_n)$.

Theorem 166 ($F(a) = F[x]/\langle p(x) \rangle$) Let F be a field and let $p(x) \in F[x]$ be irreducible over F . If a is a zero of $p(x)$ in some extension E of F , then $F(a)$ is isomorphic to $F[x]/\langle p(x) \rangle$. Furthermore, if $\deg(p(x)) = n$, then every member of $F(a)$ can be uniquely expressed in the form $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \dots + c_1a + c_0$, where $c_0, \dots, c_{n-1} \in F$.

Corollary 167 ($F(a) \approx F(b)$) Let F be a field and let $p(x) \in F[x]$ be irreducible over F . If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F , then the fields $F(a)$ and $F(b)$ are isomorphic.

Lemma 168 Let F be a field, let $p(x) \in F[x]$ be irreducible over F , and let a be a zero of $p(x)$ in some extension of F . If ϕ is a field isomorphism from F to F' and b is zero of $\phi(p(x))$ in some extension of F' , then there is an isomorphism from $F(a)$ to $F'(b)$ that agrees with ϕ on F and carries a to b .

Theorem 169 (Extending $\phi : F \rightarrow F'$) Let ϕ be an isomorphism from a field F to a field F' and let $f(x) \in F[x]$. If E is a splitting field for $f(x)$ over F and E' is a splitting field of $\phi(f(x))$ over F' , then there is an isomorphism from E to E' that agrees with ϕ on F .

Corollary 170 (Splitting Fields are Unique) Let F be a field and let $f(x) \in F[x]$. Then any two splitting fields of $f(x)$ over F are isomorphic.

Definition 171 (Derivative) Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ belong to $F[x]$. The derivative of $f(x)$, denoted by $f'(x)$, is the polynomial $na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1$ in $F[x]$.

Lemma 172 (Properties of the Derivative) Let $f(x), g(x) \in F[x]$ and let $a \in F$. Then

1. $(f(x) + g(x))' = f'(x) + g'(x)$
2. $(af(x))' = af'(x)$
3. $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$.

Theorem 173 (Criterion for Multiple Zeros) A polynomial $f(x)$ over a field F has a multiple zero in some extension E if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$.

Theorem 174 (Zeros of an Irreducible) Let $f(x)$ be an irreducible polynomial over a field F . If F has characteristic 0, then $f(x)$ has no multiple zeros. If F has characteristic $p \neq 0$, then $f(x)$ has a multiple zero if it's of the form $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Definition 175 (Perfect Field) A field F is called perfect if F has characteristic 0 or if F has characteristic p and $F^p = \{a^p | a \in F\} = F$.

Theorem 176 (Finite Fields Are Perfect) Every finite field is perfect.

Theorem 177 (Criterion for No Multiple Zeros) If $f(x)$ is an irreducible polynomial over a perfect field F , then $f(x)$ has no multiple zeros.

Theorem 178 (Zeros of an Irreducible over a Splitting Field) Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$ over F . Then all the zeros of $f(x)$ in E have the same multiplicity.

Corollary 179 (Factorization of an Irreducible over a Splitting Field) Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$. Then $f(x)$ has the form $a(x - a_1)^n(x - a_2)^n \dots (x - a_t)^n$ where a_1, a_2, \dots, a_t are distinct elements of E and $a \in F$.

3.3 Algebraic Extensions

Definition 180 (Types of Extensions) Let E be an extension field of a field F and let $a \in E$. We call a algebraic over F if a is the zero of some nonzero polynomial in $F[x]$. If a isn't algebraic over F , it's called transcendental over F . An extension E of F is called an algebraic extension of F if every element of E is algebraic over F . If E isn't an algebraic extension of F , it's called a transcendental extension of F . An extension of F of the form $F(a)$ is called a simple extension of F .

Theorem 181 (Characterization of Extensions) Let E be an extension field of the field F and let $a \in E$. If a is transcendental over F , then $F(a) \approx F[x]/\langle p(x) \rangle$, where $p(x)$ is a polynomial in $F[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over F .

Theorem 182 (Uniqueness Property) If a is algebraic over a field F , then there is a unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(a) = 0$.

Theorem 183 (Divisibility Property) Let a be algebraic over F , and let $p(x)$ be the minimal polynomial for a over F . If $f(x) \in F[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $F[x]$.

Definition 184 (Degree of an Extension) Let E be an extension field of a field F . We say that E has degree n over F and write $[E : F] = n$ if E has dimension n as a vector space over F . If $[E : F]$ is finite, E is called a finite extension of F ; otherwise, we say that E is an infinite extension of F .

Theorem 185 (Finite Implies Algebraic) If E is a finite extension of F , then E is an algebraic extension of F .

Theorem 186 ($[K : F] = [K : E][E : F]$) Let K be a finite extension field of the field E and let E be a finite extension field of the field F . Then K is a finite extension field of F and $[K : F] = [K : E][E : F]$.

Theorem 187 (Primitive Element Theorem) If F is a field of characteristic 0, and a and b are algebraic over F , then there's an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.

Theorem 188 (Algebraic over Algebraic is Algebraic) If K is an algebraic extension of E and E is an algebraic extension of F , then K is an algebraic extension of F .

Corollary 189 (Subfield of Algebraic Elements) Let E be an extension field of the field F . Then the set of all elements of E that are algebraic over F is a subfield of E .

3.4 Finite Fields

Theorem 190 (Classification of Finite Fields) For each prime p and each positive integer n , there's, up to isomorphism, a unique finite field of order p^n .

Theorem 191 (Structure of Finite Fields) As a group under addition, $\text{GF}(p^n)$ is isomorphic to $\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p$. (n -times) As a group under multiplication, the set of nonzero elements of $\text{GF}(p^n)$ is isomorphic to \mathbb{Z}_{p^n-1} (and is, therefore, cyclic).

Corollary 192 $[\text{GF}(p^n) : \text{GF}(p)] = n$

Corollary 193 Let a be a generator of the group of nonzero elements of $\text{GF}(p^n)$ under multiplication. Then a is algebraic over $\text{GF}(p)$ of degree n .

Theorem 194 (Subfields of a Finite Field) For each divisor m of n , $\text{GF}(p^n)$ has a unique subfield of order p^m . Moreover, these are the only subfields of $\text{GF}(p^n)$.

3.5 Sylow Theorems

Definition 195 Let a and b be elements of group G . We say that a, b are conjugate in G (and call b a conjugate of a) if $axa^{-1} = b$ for some $x \in G$. The conjugacy class of a is the set $\text{cl}(a) = \{axa^{-1} : x \in G\}$.

Theorem 196 (Number of Conjugates of a) Let G be a finite group and let $a \in G$. Then, $|\text{cl}(a)| = |G : C(a)|$

Corollary 197 ($|\text{cl}(a)|$ Divides $|G|$) In a finite group, $|\text{cl}(a)|$ divides $|G|$.

Corollary 198 (Class Equation) For any finite group G , $|G| = \sum |G : C(a)|$ where the sum runs over one element a from each conjugacy class of G .

Theorem 199 (p – Groups Have Nontrivial Centers) Let G be a nontrivial finite group whose order is a power of a prime p . Then $Z(G)$ has more than one element.

Corollary 200 If $|G| = p^2$, where p is prime, then G is Abelian.

Theorem 201 (Existence of Subgroups of Prime-Power Order (Sylow's First Theorem)) Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k .

Definition 202 (Sylow p -Subgroup) Let G be a finite group and let p be a prime. If p^k divides $|G|$ and p^{k-1} doesn't divide $|G|$, then any subgroup of G of order p^k is called a Sylow p -subgroup of G .

Corollary 203 (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 204 (Conjugate Subgroups) Let H and K be subgroups of a group G . We say that H and K are conjugate in G if there's an element $g \in G$ such that $H = gKg^{-1}$.

Theorem 205 (Sylow's Second Theorem) If H is a subgroup of a finite group G and $|H|$ is a power of a prime p , then H is contained in some Sylow p -subgroup of G .

Theorem 206 (Sylow's Third Theorem) Let p be a prime and let G be a group of order $p^k m$, where p doesn't divide m . Then the number n of Sylow p -subgroups of G is equal to $1 \pmod{p}$ and divides m . Furthermore, any two Sylow p -subgroups of G are conjugate.

Corollary 207 (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's the only Sylow p -subgroup of G .

Theorem 208 (Cyclic Groups of Order pq) If G is a group of order pq , where p and q are primes, $p < q$, and p doesn't divide $q - 1$, then G is cyclic. In particular, G is isomorphic to \mathbb{Z}_{pq} .

3.6 Simple Groups

Definition 209 (Simple Group) *A group is simple if its only subgroups are the identity subgroup and the group itself.*

Theorem 210 (Sylow Test for Nonsimplicity) *Let n be a positive integer that's not a prime, and let p be a prime divisor of n . If 1 is the only divisor of n that's equal to $1 \pmod p$, then there doesn't exist a simple group of order n .*

Theorem 211 (2· Odd Test) *An integer of the form $2 \cdot n$, where n is an odd number greater than 1, is not the order of a simple group.*

Theorem 212 (Generalized Cayley Theorem) *Let G be a group and let H be a subgroup of G . Let S be the group of all permutations of the left cosets of H in G . Then there's a homomorphism from G into S , whose kernel lies in H and contains every normal subgroup of G that's contained in H .*

Corollary 213 (Index Theorem) *If G is a finite group and H is a proper subgroup of G such that $|G|$ doesn't divide $|G : H|!$, then H contains a nontrivial subgroup of G . In particular, G isn't simple.*

Corollary 214 (Embedding Theorem) *If a finite non-Abelian simple group G has a subgroup of index n , then G is isomorphic to a subgroup of A_n .*