1 Preliminaries

Properties of Integers

DEFINITION ***Well Ordering Principle***
Every nonempty subset of positive integers contains a smallest member.

THEOREM 1.1 ***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 $0 \leq r < b$.

DEFINITION ***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 $gcd(a, b)$. Then $gcd(a, b) = 1$, we say a and b are *relatively prime*.

THEOREM 1.2 ***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 $as + bt4$.

LEMMA ***Euclid's Lemma :*** $p|ab$ ***implies*** $p|a$ ***or*** $p|b$
If p is a prime that divides ab, then p divides a or p divides b.

LEMMA ***Generalized Euclid's Lemma***
If p is a prime and p divides $a_1a_2 \dots a_n$, then p divides a_i for some i.

THEOREM 1.3 ***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. Thus, if $n = p_1p_2 \dots p_2$ and $n = q_1q_2 \dots q_2$, there 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 ***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 $lcm(a, b)$.

Mathematical Induction

THEOREM 1.4 ***First Principal 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 1.5 ***Second Principal of Mathematical Induction***
Let S be a set of integers containing a. Suppose S has the property that h 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.

Equivalence Relations

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

THEOREM 1.6 ***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 elements of P.

Functions (Mappings)

DEFINITION ***Function (Mapping)***
A *function* (or *mapping*) ϕ *from a set* A *to a set* B is a rule that assigns to each element 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 ***Composition of Functions***
Let $\phi : A \to B$ and $\psi : B \to C$. The *composition* $\psi\phi$ is the mapping from A to C define by $(\psi\phi)(a) = \psi(\phi(a))$ for all a in A.

DEFINITION ***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 ***Function 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 1.7 ***Properties of Functions***
Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$, then

1. *Associative.* $\gamma(\beta\alpha) = (\gamma\beta)\alpha$.
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 Groups

Definition and Examples of Groups

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

DEFINITION ***Group***
Let G be a nonempty set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element of 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 ***Multiplicative Group of Integers modulo n***
For each integer $n > 1$ we define $U(n)$ to be the set of all positive integers less than n and relatively prime to n. Note that $U(n)$ is a group under multiplication modulo n called the *multiplicative group of integers modulo n*.

DEFINITION ***Special Linear Group, $SL(2, \mathbb{F})$***
The set of all 2×2 matrices with determinant 1 and entries from $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (p a prime) is a non-Abelian group under matrix multiplication. This group is called the *special linear group* of 2×2 matrices, and is denoted by $SL(2, \mathbb{F})$.

DEFINITION ***General Linear Group, $GL(2, \mathbb{F})$***
Let $\mathbb{F}$ be any of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}_p$ (p a prime). The set $GL(2, \mathbb{F})$ of all 2×2 matrices with nonzero determinants and entries from $\mathbb{F}$ is a non-Abelian group under matrix multiplication. We call this group the *general linear group* of 2×2 matrices.

DEFINITION ***The Dihedral Group of order $2n$, D_n***
The *dihedral group of order* $2n$, sometimes called the *group of symmetries of a regular n-gon*, is the group formed by all possible reflections and rotations that move an n sided regular polygon onto itself. It is denoted $D_n = \langle r, f \mid r^n = f^2 = e, rf = fr^2 \rangle$.

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 $b = c$.

LEMMA ***Cross Cancellation implies Commutativity***
If, whenever $a, b, c \in G$, we have $ab = ca$ implies $b = c$ then G is Abelian.

LEMMA ***Middle Cancellation implies Commutativity***
Suppose G is a group with the property that for every choice of elements in G, $axb = cxd$ implies $ab = cd$. Then G is Abelian.

THEOREM 2.3 ***Uniqueness of Inverses***
For each element a in a group G, there is a unique element B in G such that $ab = ba = e$.

DEFINITION ***Law of Exponents for Abelian Groups***
Let a and b be elements of an Abelian group and let n be any integer. Then $(ab)^n = a^n b^n$.

DEFINITION ***Socks-Shoes Property***
Let a and b be elements of a group, then $(ab)^{-1} = b^{-1}a^{-1}$.

3 Finite Groups; Subgroups

Terminology and Notation

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 is 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 ***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.

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 subgroup 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.

Examples of Subgroups

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

$$Z(G) = \{z \in G \mid ax = xa \text{ for all } x \in G\}.$$

THEOREM 3.5 ***Center 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. Then *centralizer of* a *in* G, $C(a)$, is the set of all elements in G that commute with a. In symbols, $C(a) = \{g \in G \mid ga = ag\}$.

DEFINITION ***Centralizer of*** H ***in*** G
If H is a subgroup of G, then by the *centralizer* $C(H)$ of H we mean the set $\{x \in G \mid xh = hx \text{ for all } h \in H\}$.

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

LEMMA
For each divisor $k > 1$ of n, let $U_k(n) = \{x \in U(n) \mid x \mod k = 1\}$. Then $U_k(n)$ is a group.

DEFINITION ***Conjugate of H***
Let G be a group and H be a subgroup of G. For any fixed x in G, define the *conjugate of* H by $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$.

THEOREM ***Properties of Conjugation***
Let G be a group with $x \in G$ and H be a subgroup of G.

1. xHx^{-1} is a subgroup of G.
2. If H is cyclic, then xHx^{-1} is cyclic.
3. If H is Abelian, then xHx^{-1} is Abelian.

DEFINITION ***Normalizer of H***
Let G be a group and H be a subgroup of G. Define $N(H) = \{x \in G \mid xHx^{-1} = H\}$.

THEOREM Normalizer is a subgroup ***L***
et G be a group and H be a subgroup of G. Then the normalizer of H, $N(H)$ is a subgroup of G.

4 Cyclic Groups

Properties of 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 infintie order, then all distinct powers of a are distinct group elements. If a has finite order, say, n, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^k$ if and only if n divides $i - j$.

COROLLARY 1 $|a| = |\langle a \rangle|$
For any group element a, $|a| = |\langle a \rangle|$.

COROLLARY 2 $a^k = e$ ***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 $|a^k| = n/gcd(n,k)$.

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

COROLLARY 2 ***Generators of Cyclic Groups***
Let $G = \langle a \rangle$ be a cyclic group of order n. Then $G = \langle a^k \rangle$ if and only if $gcd(n, k) = 1$.

COROLLARY 3 ***Generators of $\mathbb{Z}_n$***
In integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $gcd(n, k) = 1$.

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 ***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 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 and Notation

DEFINITION ***Permutations 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 is a set of permutations of A that forms a group under function composition.

DEFINITION ***Symmetric Group of Degree n, S_n***
Let $A = \{1, 2, \ldots, n\}$. The set of all permutations of A is called the *symmetric group of degree* n and is denoted by S_n.

Properties of Permutations

THEOREM 5.1 ***Products of Disjoint Cycles***

Every permutation of a fintie set can be written as a cycle or as a product of disjoint cycles.

THEOREM 5.2 ***Disjoint Cycles Commute***
If the pair $\alpha = (a_1, a_2, \ldots, a_m)$ 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 (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.

DEFINITION ***Transposition***
A permutation of the form (ab) is called a *transposition*, since the effect is to interchange or transpose a and b.

THEOREM 5.4 ***Product of 2-Cycles***
Every permutation in S_n, $n > 1$, is a product of 2-cycles.

LEMMA
If $\epsilon = \beta_1\beta_2 \ldots \beta_r$ where the $\beta's$ are 2-cycles, then r is even.

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

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

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

DEFINITION ***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 ***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 Isomorphism

Definition and Examples

DEFINITION ***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,

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

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

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

Properties of Isomorphism's

THEOREM 6.2 ***Properties of Isomorphism's 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 $\overline{G}$.

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

1. G is Abelian if and only if $\overline{G}$ is Abelian.

2. G is cyclic if and only if $\overline{G}$ is cyclic.

3. ϕ^{-1} is an isomorphism from $\overline{G}$ onto G.

4. If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

Automorphism's

DEFINITION ***Automorphism***
An isomorphism from a group G onto 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 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 automorphism's of a group and the set of inner automorphism's 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 $U(n)$.

DEFINITION ***Characteristic Subgroup***
A subgroup N of a group G is called a *characteristic subgroup* if $\phi(N) = N$ for all automorphisms ϕ of G.

DEFINITION ***Commutator Subgroup***
The *commutator subgroup* G' of a group G is the subgroup generated by the set $\{x^{-1}y^{-1}xy \mid x, y \in G\}$. That is, every element is of the form $a_1^{i_1}a_2^{i^2}\dots a_k^{i_k}$, where each a_j has the form $x^{-1}y^{-1}xy$, each $i_j = \pm 1$, and k is any positive integer.

7 Coset's and Lagrange's Theorem

Properties of Coset's

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 $\{ah \mid a \in H\}$ is denoted by aH. Analogously, $Ha = \{ha \mid m \in H\}$ 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 Coset's***
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. $aH = bH$ or $aH \cap bH = \emptyset$,
4. $aH = bH$ if and only if $a^{-1}b \in H$,
5. $|aH| = |bH|$,
6. $aH = Ha$ if and only if $H = aHa^{-1}$,
7. aH is a subgroup of G if and only if $a \in H$.

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 if distinct left (right) coset's of H in G is $|G|/|H|$.

COROLLARY 1 $|G : H| = |G|/|G|$
If G is a finite group and H is a subgroup of G, then $|G : H| = |G|/|H|$.

COROLLARY 2 $|a|$ divides $|G|$
In a finite group, the order of each element of the group divides the order of the group.

COROLLARY 3 ***Groups of Prime Order are Cyclic***
A group of prime order is cyclic.

COROLLARY 4 $a^{|G|} = e$
Let G be a finite group, and let $a \in G$. Then, $a^{|G|} = e$.

COROLLARY 5 ***Fermat's Little Theorem***
For every integer a and every prime p, $a^p \mod p = a \mod p$.

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.

An Application of Coset's to Permutation Groups

DEFINITION ***Stabilizer of a Point***
Let G be a group of permutations of a set S. For each i in S, let $stab_G(i) = \{\phi \in G \mid \phi(1) = i\}$. We call $stab_G(i)$ the *stabilizer of i in G*.

DEFINITION ***Orbit of a Point***
Let G be a group of permutations of a set S. For each s in S, let $orb_G(s) = \{\phi(s) \mid \phi \in G\}$. The set $orb_G(s)$ is a subset of S called the *orbit of s under G*.

THEOREM 7.3 ***Orbit-Stabilizer Theorem***
Let G be a finite group of permutations of a set S. Then, for any i from S, $|G| = |orb_G(i)||stab_G(i)|$.

THEOREM 7.4 ***The Rotation Group of a Cube***
The group of rotations of a cube is isomorphic to S_4.

8 External Direct Product

Definition and Examples

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 ith component is an element of G_i and the operation is component wise.

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 components of the element. In symbols,

$$|(g_1, g_2, \ldots, g_n)| = lcm(|g_1|, |g_2|, \ldots, |g_n|).$$

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 1 ***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 2 ***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 when $i \neq j$.

The Group of Units Modulo n as an External Direct Product

THEOREM 8.3 ***$U(n)$ as an External Direct Product***
Suppose s and t re relative 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 $m = n_1 n_2 \ldots n_l$, where $gcd(n_i, n_j) = 1$ for $i \neq j$. Then,

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

9 Normal Subgroups and Factor Groups

Normal Subgroups

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 $H \triangleright G$.

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.

Factor Groups

THEOREM 9.2 ***Factor Groups (O. Hölder, 1889)***
Let G be a group and let H be a normal subgroup of G. Then set $G/H = \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$

Applications of Factor Groups

THEOREM 9.3 ***The 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 $G/Z(G) \approx Inn(G)$
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.

Internal Direct Product

DEFINITION ***Internal Direct Products 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

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

DEFINITION ***Internal Direct Product of $H_1 \times H_2 \times \ldots \times H_n$***
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 $H_1 \times H_2 \times \ldots \times H_n$, if

1. $G = H_1 H_2 \ldots H_n = \{h1_h 2 \ldots h_n \mid h_i \in H_i\}$
2. $(H_1 H_2 \ldots H_n) \cap H_{i+1} = \{e\}$ for $i = 1, 2, \ldots, n-1$.

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

10 Group Homomorphism's

Definition and Examples

DEFINITION ***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 ***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 $\ker \phi$.

Properties of Homomorphism's

THEOREM 10.1 ***Properties of Elements Under Homomorphism's***
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 the identity $\overline{G}$.
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 Homomorphism's***
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 $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in K\}\}$ 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 $\overline{G}$.

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, $G/\ker\phi \equiv \phi(G)$.

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

THEOREM ***Second Isomorphism Theorem***
If K is a subgroup of G and N is a normal subgroup of G, then $K/(K \cap N)$ is isomorphic to KN/N.

THEOREM ***Third Isomorphism Theorem***
If M and N are normal subgroups of G and $N \leq M$, then $(G/N)/(M/N) \equiv G/M$.

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

11 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 and terms in the product and the orders of the cyclic groups are uniquely determined by the group.

COROLLARY ***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.

Proof of the Fundamental Theorem

LEMMA 1
Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times X$, where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.

LEMMA 2
Let G be an Abelian group of prime-power order and let a be an element of maximal order in G. Then G can be written in the form $\langle a \rangle \times K$.

LEMMA 3
A finite Abelian group of prime-power order is an internal direct product of cyclic groups.

LEMMA 4
Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \ldots \times H_m$ and $G = K_1 \times K_2 \times \ldots K_n$, where H's and K's are nontrivial cyclic subgroups with $|H_1| \leq |H_2| \leq \ldots \leq |H_m|$ and $|K_1| \leq |H_2| \leq \ldots \leq |H_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

DEFINITION ***Maximal***
A proper subgroup H of a group G is called *maximal* if there is no subgroup K such that $H \subset K \subset G$.

12 Introduction to Rings

DEFINITION ***Ring***
A *ring* R is a nonempty set with two binary operations, addition (denoted by $a + b$) 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 is an additive identity 0. That is, there is an element 0 in R such that $a + 0 = a$ for all a in R.
4. There si an element $-a$ in R such that $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

DEFINITION ***Unity***
A *unity* (or *identity*) in a ring is a nonzero element that is an identity under multiplication.

DEFINITION ***Unit***
A nonzero element of a commutative ring with unity need not have an inverse. When it does, we say that it is a *unit* of the ring.

Properties of Rings

THEOREM 12.1 ***Rules of Multiplication***
Let a, b and 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 a unity element 1, then
5. $(-1)a = -a$.
6. $(-1)(-1) = 1$.

THEOREM 12.2 ***Uniqueness of the Unity and Inverses***
If a ring has a unity, it is unique. If a ring has a multiplicative inverse, it is unique.

Subrings

DEFINITION ***Subring***
A subset S of a ring R is a *subring of* R if S is itself a ring with the operation R.

THEOREM 12.3 ***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 in S whenever a and b are in S.

DEFINITION ***Gaussian Integers***
The set of *Gaussian integers*

$$Z[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

is a subring of the complex numbers $\mathbb{C}$.

DEFINITION ***Group of Units of R***
Let R be a commutative ring with unity and let $U(R)$ denote the set of units in R. Then $U(R)$ is a group under the multiplication of R and is called the *group of units of* R.

DEFINITION ***Boolean Ring***
Suppose that R is a ring and that $a^2 = a$ for all a in R. Then R is a commutative ring called a *Boolean ring*.

13 Integral Domains

13.1 Definition and Examples

DEFINITION ***Zero-Divisors***
A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

DEFINITION ***Integral Domain***
An *integral domain* is a commutative ring with unity and no zero-divisors.

THEOREM 13.1 ***Cancellation***
Let a, b and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Fields

DEFINITION ***Field***
A *field* is a commutative ring with unity in which ever nonzero element is a unit.

THEOREM Finite Subring Test ***A***
finite subset of a field is a subfield if it contains a nonzero element and is closed under addition and multiplication.

THEOREM 13.2 ***Finite Integral Domains are Fields***
A finite integral domain is a field.

COROLLARY $\mathbb{Z}_p$ ***Is a Field***
For every prime p, $\mathbb{Z}_p$, the ring of integers modulo p, is a field.

Characteristic of a Ring

DEFINITION ***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 char R.

THEOREM 13.4 ***Characteristic of an Integral Domain***
The characteristic of an integral domain is 0 or prime.

DEFINITION ***Nilpotent***
Let a belong to a ring R with unity and suppose $a^n = 0$ for some positive integer n. Such an element is called *nilpotent*.

DEFINITION ***Idempotent***
A ring element a is called *idempotent* if $a^2 = a$. In an integral domain, only 0 and 1 can be idempotent.

14 Ideals and Factor Rings

Ideals

DEFINITION ***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.

DEFINITION ***Proper Ideal***
An ideal A of R is called a *proper ideal* of R if A is a proper subset of R.

DEFINITION ***Trivial Ideal***
For any ring R, $\{0\}$ and R are ideals of R. The ideal $\{0\}$ is called the *trivial* ideal.

THEOREM 14.1 ***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 in A whenever $a \in A$ and $r \in R$.

DEFINITION ***Trivial Ideal***
For any ring R, $\{0\}$ is an ideal of R called the *trivial idea*.

DEFINITION ***Principal Ideal Generated by a***
Let R be a commutative ring with unity and let $a \in R$. The set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of R called the *principal ideal generated by* a.

DEFINITION ***Ideal Generated by $a_1, a_2, \ldots, a_n$***
Let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n$ belong to R. Then $I = \langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_i \in R\}$ is an ideal or R called the *ideal generated by* $a_1, a_2, \ldots, a_n$.

Factor Rings

THEOREM 14.2 ***Existence of Factor Groups***
Let R be a ring and let A be a subring of R. The set of coset's $\{r + a \mid r \in R\}$ is a rung under the operation $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R.

DEFINITION ***Prime Ideal, Maximal Ideal***
A *prime ideal* 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 proper ideal A of a commutative ring R is a *maximal ideal* of R if, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

THEOREM 14.3 *R/A is an Integral Domain if and only if A is a 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 14.4 *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.

LEMMA
Let n be an integer greater than 1. Then, in the ring of integers, the ideal $n\mathbb{Z}$ is prime if and only if n is prime ($\{0\}$ is also prime).

LEMMA
Consider the ideal $\langle x^2+1\rangle$ in $\mathbb{R}[x]$. This ideal is maximal and the quotient ring

$$\mathbb{R}[x]/\langle x^2+1\rangle \approx \mathbb{C}$$

is ring isomorphic to the complex numbers $\mathbb{C}$.

LEMMA
Let R be a ring and let $\{I_1, I_2, \ldots, I_n\}$ be any set of ideals of R. Then the intersection $I = \bigcap\{I_1, I_2, \ldots, I_n\}$ is an ideal of R.

DEFINITION ***Sum***
If A and B are ideals of a ring, their *sum*, $A+B = \{a+b \mid a \in A, b \in B\}$ is an ideal.

DEFINITION ***Product***
If A and B are ideals of a ring, their *product*, $AB = \{a_1b_1+a_2b_2+\ldots+a_nb_n \mid a_i \in A, b_i \in B\}$ is an ideal.

LEMMA
Let A and B be ideals of a ring R, then $AB \subseteq A \cap B$.

LEMMA
Let R be a ring and let A be an ideal of R. If u is a unit and R and u belongs to A, then $A = R$.

LEMMA
If R is a commutative ring with unity and A is a proper ideal of R, the factor ring R/A is a commutative ring with unity.

LEMMA
The ring $\mathbb{F}$ is a field if and only if its only ideals are the trivial ideal, $\{0\}$, and itself, $\mathbb{F}$.

LEMMA

Let R be a ring and let p be a fixed prime. Then the set

$$I_p = \{r \in R \mid \text{ additive order of } r \text{ is a power of } p\}$$

is an ideal of R.

DEFINITION ***Principal Ideal Domain***
An integral domain D is called a *principal ideal domain* if every ideal of D has the form $\langle a \rangle = \{ad \mid d \in D\}$ for some a in D.

LEMMA
If R is a principal ideal domain and I is an ideal of R, then every ideal of R/I is a principal ideal.

DEFINITION ***Annihilator***
Let R be a commutative ring and let A be any subset of R. The *annihilator* of A, $\text{Ann}(A) = \{r \in R \mid ra = 0 \text{ for all } a \in A\}$ is an ideal.

DEFINITION ***Nil Radical***
Let R be a commutative ring and let A be any ideal of R. The *nil radical* of A, $N(A) = \{r \in R \mid r^n \in A \text{ for some positive integer } n\}$ is an ideal. Note that n depends in r.

DEFINITION ***Nil Radical of R***
The nil radical $N(\langle 0 \rangle)$ is called the *nil radical of* R.

LEMMA
Let R be a commutative ring. Then the factor group $R/N(\langle 0 \rangle)$ has no nonzero nilpotent elements.

LEMMA
Let A be an ideal of a commutative ring, then $N(N(\langle A \rangle)) = N(\langle A \rangle)$.

LEMMA
Let R be a commutative ring with more than one element. If, for every nonzero element a of R, we have $aR = R$ then R is a field.

LEMMA ***Euclid's Lemma for Prime Ideals***
Let A, B and C be ideals of a ring R. If $AB \subseteq C$ and C is a prime ideal of R, then $A \subset C$ or $B \subset C$.

LEMMA
Let A, B and C be subrings of a ring R. IF $A \subseteq B \cup C$ then $A \subseteq B$ or $A \subseteq C$.

LEMMA
Let R be an integral domain with nonzero characteristic. If A is a proper ideal of R, then R/A has the same characteristic as R.

15 Ring Homomorphism's

DEFINITION ***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 $a, b \in R$,

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism that is both one-to-one and onto is called a *ring homomorphism.*

THEOREM ***Second Isomorphism Theorem for Rings***
Let A be a subring of R and let B be an ideal of R. Then $A \cap B$ is an ideal of A and $A/(A \cap B)$ is isomorphic to $(A + B)/B$.

THEOREM ***Third Isomorphism Theorem for Rings***
Let A and B be ideals of a ring R with $B \subseteq A$. Then A/B is an ideal of R/B and $(R/B)/(A/B)$ is isomorphic to R/A.

DEFINITION ***Natural Homomorphism***
For any positive integer n, the mapping $k \to e \mod n$ is a ring homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}_n$. This mapping is called the *natural homomorphism* from $\mathbb{Z}$ to $\mathbb{Z}_n$.

Properties of Ring Homomorphism's

THEOREM 15.1 ***Properties of Ring Homomorphism's***
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 onto, then $\phi(1)$ is the unity of S.
7. ϕ is an isomorphism if and only if ϕ is onto and $\text{Ker}\phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.
8. If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.

THEOREM 15.2 ***Kernels Are Ideals***
Let ϕ be a homomorphism from a ring R to a ring S. Then $\text{Ker}\phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

THEOREM 15.3 ***First Isomorphism Theorem***
Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\text{Ker}\phi$ to $\phi(R)$, given by $r+\text{Ker}\phi \to \phi(R)$, is an isomorphism. In symbols, $R/\text{Ker}\phi \approx \phi(R)$.

THEOREM 15.4 ***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 $r \to r + A$ from R to R/A (the natural homomorphism from R to R/A).

THEOREM 15.5 ***Homomorphism from $\mathbb{Z}$ to a Ring with Unity***
Let R be a ring with unity 1. The mapping $\phi : \mathbb{Z} \to R$ given by $n \to n \cdot 1$ is a ring homomorphism.

COROLLARY ***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 ***$\mathbb{Z}_m$ is a Homomorphic Image of $\mathbb{Z}$***
For any positive integer m, the mapping $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \to x \mod m$ is a ring homomorphism.

COROLLARY ***A Field Contains $\mathbb{Z}_p$ or $\mathbb{Q}$ (Steinz, 1910)***
If $\mathbb{F}$ is a field of characteristic p, then $\mathbb{F}$ contains a subfield isomorphic to $\mathbb{Z}_p$. If $\mathbb{F}$ is a field of characteristic 0, then $\mathbb{F}$ contains a subfield isomorphic to the rational numbers.

DEFINITION ***Prime Subfield***
The intersection of all subfields (hence, the smallest subfield) of a field of characteristic p called the *prime subfield* of the field and is isomorphic to $\mathbb{Z}_p$.

The Field of Quotients

THEOREM Existence of Field of Quotients ***L***
et D be an integral domain. Then there exists a field $\mathbb{F}$ (called the *field of quotients* of D) that contains a subring isomorphic to D.

DEFINITION ***Field of Quotients***
The *field of quotients* of an integral domain D, $\{(a, b) \mid a, b \in D, b \neq 0\}$ is the smallest field containing D. If $D = \mathbb{F}$ is a field, then the field of quotients of $\mathbb{F}[x]$ is denoted by $\mathbb{F}(x)$.

LEMMA
Let $\mathbb{F}$ be a field. Then the field of quotients of $\mathbb{F}$ is a field that is ring-isomorphic to $\mathbb{F}$.

LEMMA
Let D be an integral domain and let $\mathbb{F}$ be the field of quotients of D. Then if E is any field that contains D, then E contains a subfield that is ring-isomorphic to $\mathbb{F}$.

COROLLARY
The field of quotients of an integral domain D is the smallest field containing D.

LEMMA
Let ϕ be a ring homomorphism from R to S and let a be an idempotent in R. Then the image of a, $\phi(a)$ is an idempotent in S.

LEMMA
Let p be a prime. Then the field of quotients $\mathbb{Z}_p(x) = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{Z}_p[x], g(x) \neq 0\}$ is an infinite field of characteristic p.

LEMMA ***Test for Divisibility by 3***
Let n be an integer with decimal representation $a_k a_{k-1} \ldots a_1 a_0$. Then n is divisible by 3 if and only if $a_0 + a_1 + \ldots + a_k$ is divisible by 3.

LEMMA ***Test for Divisibility by 4***
Let n be an integer with decimal representation $a_k a_{k-1} \ldots a_1 a_0$. Then n is divisible by 4 if and only if $a_0 a_1$ is divisible by 4.

LEMMA ***Test for Divisibility by 9***
An integer n with decimal representation $a_k a_{k-1} \ldots a_0$ is divisible by 9 if and only if $a_k + a_{k-1} + \ldots + a_0$ is divisible by 9.

LEMMA ***Test for Divisibility by 11***
Let n be an integer with decimal representation $a_k a_{k-1} \ldots a_1 a_0$. Then n is divisible by 11 if and only if $a_0 - a_1 + \ldots (-1)^k a_k$ is divisible by 11.

THEOREM ***Theorem of Gersonides (Special case of the so-called "abc Conjecture")***
The only four solutions to the expression $2^m = 3^n \pm 1$ are $1, 2$; $2, 3$; $3, 4$; and $8, 9$.

DEFINITION ***Frobenius Map***
Let R be a commutative ring of prime characteristic p. The *Frobenius* map $x \to x^p$ is a ring homomorphism from R to R.

DEFINITION ***Principal Ideal Ring***
A *principal ideal ring* is a ring with the property that every ideal has the form (a).

16 Polynomial Rings

Notation and Terminology

DEFINITION ***Ring of Polynomials over R***
Let R be a commutative ring. The set of formal symbols $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \mid a_i \in R, n \text{ a nonnegative integer}\}$ is called the *ring of polynomials over R in the indeterminate x*. Two elements

$$x_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

and

$$b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$$

of $R[x]$ 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 ***Addition and Multiplication in $R[x]$***
Let R be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$$

belong to $R[x]$. Then

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0),$$

where s is the maximum of m and n, $a_i = 0$ for all $i > n$, and $b_i = 0$ for $i > m$. Also,

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \ldots + c_1 x + c_0,$$

where

$$c_k = a_k b_0 + a_{k-1}b_i + \ldots + a_1 b_{k-1} + a_0 b_k$$

for $k = 0, \ldots, m + n$.

DEFINITION ***Degree of a polynomial, Leading coefficient, Monic polynomials***
If

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

where $a_n \neq 0$, we say that $f(x)$ has *degree* n, denoted $\deg f = n$. The term a_n is called the *leading coefficient* of $f(x)$, and if the leading coefficient is the multiplicative identity element of R, we say that $f(x)$ is a *monic* polynomial. The polynomial $f(x) = 0$ has no degree, and polynomials of the form $f(x) = a_0$ are called *constant*.

THEOREM 16.1 ***D an Integral Domain Implies $D[x]$ an Integral Domain***
If D is an integral domain, then $D[x]$ is an integral domain.

The Division Algorithm and Consequences

THEOREM 16.2 ***Division Algorithm for*** $\mathbb{F}[x]$
Let $\mathbb{F}$ be a field and let $f(x)$ and $g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $f(x) = q(x)g(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. The polynomials $q(x)$ and $r(x)$ are called the *quotient* and *remainder* in the division of $f(x)$ by $g(x)$.

DEFINITION ***Polynomial Division***
Let D be an integral domain. If $f(x)$ and $g(x) \in D[x]$, we say that $g(x)$ *divides* $f(x)$ in $D[x]$ (and write $f(x)|g(x)$) if there exists an $h(x) \in D[x]$ such that $f(x) = g(x)h(x)$. In this case, we also call $g(x)$ a *factor* of $f(x)$.

DEFINITION ***Zero, Root, Zero of Multiplicity*** k
An element a is a *zero* (or a *root*) of a polynomial $f(x)$ if $f(a) = 0$. When $\mathbb{F}$ is a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$, we say that a is a *zero of multiplicity* k ($k \geq 1$) if $(x - a)^k$ is a factor of $f(x)$ but $(x - a)^{k+1}$ is not a factor of $f(x)$.

COROLLARY ***The Remainder Theorem***
Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

COROLLARY ***The Factor Theorem***
Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, 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 ***Polynomials of Degree*** n ***Have at Most*** n ***Zeros***
A polynomial of degree n over a field has at most n zeros, counting multiplicity.

LEMMA ***The Complex Zeros of*** $x^n - 1$
Let $\omega = \cos(360°)/n) + i\sin(360°)/n)$. It follows from DeMoivre's Theorem that $\omega^n = 1$ and $\omega^k \neq 1$ for $a \leq k < n$. Thus, each of $1, \omega^2, \ldots, \omega^{n-1}$ is a zero of $x^n - 1$. The complex number ω is called a *primitive nth root of unity.*

DEFINITION ***Principal Ideal Domain***
A *principal ideal domain* is an integral domain R where every ideal has the form $\langle a \rangle \{ra \mid r \in R\}$.

THEOREM 16.3 $\mathbb{F}[x]$ ***is a Principal Ideal Domain***
Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a principal ideal domain.

THEOREM 16.4 ***Criterion for*** $I = \langle g(x) \rangle$
Let $\mathbb{F}$ be a field, I a nonzero ideal in $\mathbb{F}[x]$, and $g(x)$ an element of $\mathbb{F}[x]$. Then, $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.

LEMMA
If R is a commutative ring, then the characteristic of $R[x]$ is the same as the characteristic of R.

LEMMA
Let R be a commutative ring, then $R[x]$ has a subring isomorphic to R.

LEMMA
If R and S are rings that are isomorphic, then $R[x]$ and $S[x]$ are isomorphic.

LEMMA ***Degree Rule***
Let D be an integral domain and $f(x), g(x) \in D[x]$. Then, deg($f(x)g(x)$)=deg $f(x)$ + deg $g(x)$.

LEMMA
For every prime p, it follows that

$$x^{p-1} - 1 = (x-1)(x-2)\dots[x-(p-1)]$$

in $\mathbb{Z}_p[x]$.

LEMMA
Wilson's Theorem For ever integer $n > 1$, $(n-1)!$ mod $n = n-1$ if and only if n is prime.

LEMMA
If I is an ideal of R, then $I[x]$ is an ideal of $R[x]$.

LEMMA
Let R be a commutative ring with unity. If I is a prime ideal of R, then $I[x]$ is a prime ideal of $R[x]$.

DEFINITION ***Relatively Prime Polynomials***
Let $\mathbb{F}$ be a field, and let $f(x)$ and $g(x)$ belong to $\mathbb{F}[x]$. If there is no polynomial of positive degree in $\mathbb{F}[x]$ that divides both $f(x)$ and $g(x)$, we say that $f(x)$ and $g(x)$ are *relatively prime*.

LEMMA
Let $f(x), g(x) \in \mathbb{F}[x]$. If $f(x)$ and $g(x)$ are relatively prime, then there exist polynomials $h(x)$ and $k(x)$ in $\mathbb{F}[x]$ such that $f(x)h(x) + g(x)k(x) = 1$.

17 Factorization of Polynomials

Reducibility Tests

DEFINITION ***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 unit 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 is not irreducible over D is called *reducible over* D.

THEOREM 17.1 ***Reducibility Test for Degrees 2 and 3***
Let $\mathbb{F}$ be a field. If $f(x) \in \mathbb{F}[x]$ and $\deg f(x) = 2$ or 3, then $f(x)$ is reducible over $\mathbb{F}$ if and only if $f(x)$ has a zero in $\mathbb{F}$.

DEFINITION ***Content of a Polynomial, Primitive Polynomial***
The *content* of a nonzero polynomial $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, where the a's are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, \ldots, a_1, a_0$. A *primitive polynomial* is an element in $\mathbb{Z}[x]$ with content 1.

LEMMA ***Gauss's Lemma***
The product of two primitive polynomials is primitive.

THEOREM 17.2 ***Over $\mathbb{Q}$ implies over $\mathbb{Z}$***
Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Irreducibility Tests

THEOREM 17.3 ***Mod p Irreducibility Test***
Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $f(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $f(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg f(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

THEOREM 17.4 ***Eisenstein's Criterion (1850)***
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there is a prime p such that $p \nmid a_n$, $p|a_{n-1}, \ldots, p|a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

COROLLARY ***Irreducibility of pth Cyclotomic Polynomial***
For any prime p, the pth cyclotomic polynomial,

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over $\mathbb{Q}$.

THEOREM 17.5 *$\langle p(x)\rangle$ Is Maximal if and only if $p(x)$ is Irreducible*
Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$. Then $\langle p(x)\rangle$ is a maximal ideal in $\mathbb{F}[x]$ if and only if $p(x)$ is irreducible over $\mathbb{F}$.

COROLLARY 1 *$\mathbb{F}[x]/\langle p(x)\rangle$ is a Field*
Let $\mathbb{F}$ be a field and $p(x)$ an irreducible polynomial over $\mathbb{F}$. Then $\mathbb{F}[x]/\langle p(x)\rangle$ is a field.

COROLLARY 2 *$p(x)|a(x)b(x)$ implies $p(x)|a(x)$ or $p(x)|b(x)$*
Let $\mathbb{F}$ be a field and let $p(x)$, $a(x)$, $b(x) \in \mathbb{F}[x]$. If $p(x)$ is irreducible over $\mathbb{F}$ and $p(x)|a(x)b(x)$, then $p(x)|a(x)$ or $p(x)|b(x)$.

Unique Factorization in $\mathbb{Z}[x]$

THEOREM 17.6 *Unique Factorization in $\mathbb{Z}[x]$*
Every polynomial in $\mathbb{Z}[x]$ that is not 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

$$b_1 b_2 \dots b_s p_1(x 0 p_2(x) \dots p_m(x) = c_1 c_2 \dots c_t q_1(x) q_2(x) \dots q_n(x),$$

where the b's and c's are irreducible polynomials of degree 0, and the $p(x)$'s and $q(x)$'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 $i = 1, \dots, m$.

LEMMA
Any nonconstant polynomial from $\mathbb{Z}[x]$ that is irreducible over $\mathbb{Z}$ is primitive.

LEMMA *Properties of Irreducibility*
Let $\mathbb{F}$ be a field and let a be a nonzero element of $\mathbb{F}$.

a. If $af(x)$ is irreducible over $\mathbb{F}$, then $f(x)$ is irreducible over $\mathbb{F}[x]$.
b. If $f(ax)$ is irreducible over $\mathbb{F}$, then $f(x)$ is irreducible over $\mathbb{F}[x]$.
c. If $f(x + a)$ is irreducible over $\mathbb{F}$, then $f(x)$ is irreducible over $\mathbb{F}[x]$.

LEMMA
Suppose that $f(x) \in \mathbb{Z}_p[x]$ and is irreducible over $\mathbb{Z}_p$, where p is a prime. If $\deg f(x) = n$, then $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field with p^n elements.

LEMMA *Rational Root Theorem*
Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

and $a_n \neq 0$. If r and s are relatively prime integers and $f(r/s) = 0$, then $r|a_0$ or $s|a_0$.

18 Divisibility in Integral Domains

Irreducibles, Primes

DEFINITION ***Associates, Irreducibles, Primes***
Elements a and b of an integral domain D are called *associates* if $a = ub$, where u is a unit of D. A nonzero element a of an integral domain D is called an *irreducible* if a is not 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 is not a unit and $a|bc$ implies $a|b$ or $a|c$.

DEFINITION ***Norm***
A function N from an integral domain of the form $\mathbb{Z}[\sqrt{d}]$ into the nonnegative integers defined by $N(a + b\sqrt{d}) = |a^2 - db^2|$ is called the *norm* of $a + b\sqrt{d}$ in $\mathbb{Z}[\sqrt{d}]$.

LEMMA ***Properties of a Norm***
Let $\mathbb{Z}[\sqrt{d}]$ be an integral domain and N the norm function from $\mathbb{Z}[\sqrt{d}]$ to the nonnegative integers. Then, the follow statements are always true

1. $N(x) = 0$ if and only if $x = 0$;
2. $N(xy) = N(x)N(y)$, for all x and y;
3. x is a unit if and only if $N(x) = 1$; and,
4. if $N(x)$ is a prime, then x is irreducible in $\mathbb{Z}[\sqrt{d}]$.

THEOREM 18.1 ***Prime Implies Irreducible***
In an integral domain, every prime is irreducible.

THEOREM 18.2 ***PID Implies Irreducible Equals Prime***
In a principal ideal domain, an element is an irreducible if and only if it is a prime.

THEOREM ***Fermat's Last Theorem***
Let x, y, z, n be any nonzero integers with $n > 2$. Then, $x^n + y^n \neq z^n$.

Unique Factorization Domains

DEFINITION ***Unique Factorization Domain (UFD)***
An integral domain D is a *unique factorization domain* if

1. every nonzero element of D that is not 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 ***Ascending Chain Condition for a PID***

In a principal ideal domain, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \ldots$ must be finite in length.

DEFINITION ***Noetherian Ring***
A ring is called *Noetherian* if it does not contain any infinite ascending chain of ideals. In this case, the ring in question is said to satisfy the ascending chain condition.

THEOREM 18.3 ***PID implies UFD***
Every principal ideal domain is a unique factorization domain.

COROLLARY $\mathbb{F}[x]$ ***is a UFD***
Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a unique factorization domain.

Euclidean Domains

DEFINITION ***Euclidean Domain***
An integral domain D is called a *Euclidean domain* if there is a function d (called the *measure*) from the 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 and r in D such that $a = bq + r$, where $r = 0$ and $d(r) < d(b)$.

LEMMA
Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a Euclidean domain with $d(f(x)) = \deg f(x)$.

THEOREM 18.4 ***ED (Euclidean Domain) Implies PID***
Every Euclidean domain is a principal ideal domain.

COROLLARY ***ED Implies UFD***
Every Euclidean domain is a unique factorization domain.

THEOREM 18.5 D ***a UFD Implies*** $D[x]$ ***a UFD***
If D is a unique factorization domain, then $D[x]$ is a unique factorization domain.

LEMMA
In an integral domain, the elements a and b are associates if and only if $\langle a \rangle = \langle b \rangle$.

LEMMA
The union of a chain $I_1 \subset I_2 \subset \ldots$ of ideals of a ring R is an ideal of R.

LEMMA
In an integral domain, the product of an irreducible and a unit is an irreducible.

LEMMA

Let a and b belong to an integral domain D, such that $b \neq 0$ and a is not a unit. Then, $\langle ab \rangle$ is a proper subring of $\langle b \rangle$.

LEMMA
Let D be an integral domain. The relation on R defined by $a\ b$ if and only if a and b are associates, is an equivalent relation on D.

LEMMA
Let D be an integral domain with measure d. Then u is a unit in D if and only of $d(u) = 1$.

LEMMA
Let D be an integral domain with measure d. If a and b are associates then $d(a) = d(b)$.

LEMMA
Let D be a principal ideal domain and let $p \in D$. Proive that $\langle p \rangle$ is a maximal ideal in D if and only if p is irreducible.

LEMMA
Let D be a principal ideal domain. Then every proper ideal of D is contained in a maximal ideal of D.

LEMMA
Let d be an integer less than -1 that is not divisible by the square of a prime. Then the only units in $\mathbb{Z}[\sqrt{d}]$ are 1 and -1.

LEMMA
Let p be a prime in an integral domain. If $p|a_1a_2 \ldots a_n$ then p divides some a_i.

LEMMA
Let D be a principal ideal domain and p an irreducible element of D. Then $D/\langle p \rangle$ is a field.

DEFINITION ***Finitely Generated***
An ideal A of a commutative ring R with unity is said to be *finitely generated* if there exist elements $a_1, a_2, \ldots, a_n$ of A such that $A = \langle a_1, a_2, \ldots, a_n \rangle$.

THEOREM Finitely Generated Equals Ascending Chain ***A***
n integral domain R satisfies the ascending chain condition if and only if it is finitely generated.

LEMMA
In a unique factorization domain, an element is irreducible if and only if it is prime.

THEOREM ***Chinese Remainder Theorem for Rings***
If R is a commutative ring and I and J are two proper ideals with $I+J = R$, show $R/(I \cap J)$ is isomorphic to $R/I \oplus R/J$.

LEMMA
Suppose that R is a commutative ring and I is an ideal of R. Then $R[x]/I[x]$ is isomorphic to $(R/I)[x]$.

19 Vector Spaces

Definitions

DEFINITION ***Vector Space***
A set V is aid to be a *vector space* over a field $\mathbb{F}$ if V is an abelian group under addition (denoted by $+$) and, if for each $a \in \mathbb{F}$ and $v \in V$, there is an element av in V such that the following conditions hold for all $a, b \in \mathbb{F}$ and $u, v \in V$:

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

The member of the vector space are called *vectors* and the members of the field are called *scalars*. The operation that combines a scalar a and a vector v to form a vector av is called *scalar multiplication*.

LEMMA
Let $\mathbb{F}$ be a field and E be a subfield of $\mathbb{F}$. Then $\mathbb{F}$ is a vector space over E. The operations are the operations of E.

Subspaces

DEFINITION ***Subspace***
Let V be a vector space over a field $\mathbb{F}$ 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 $\mathbb{F}$ under the operations of V.

DEFINITION ***Subspace of V spanned by $v_1, v_2, \ldots, v_n$, Linear Combination***
Let V be a vector space over $\mathbb{F}$ and let $v_1, v_2, \ldots, v_n$ be (not necessarily distinct) elements of V. Then the subset

$$\langle v_1, v_2, \ldots, v_n \rangle = \{a_1v_1 + a_2v_2 + \ldots + a_nv_n \mid a_1, a_2, \ldots, a_n \in \mathbb{F}\}$$

is called the *subspace of V spanned by* $v_1, v_2, \ldots, v_n$. Any summand of the form $a_1v_1 + a_2v_2 + \ldots + a_nv_n$ is called a *linear combination of* $a_1v_1 + a_2v_2 + \ldots + a_nv_n$. If $\langle a_1v_1 + a_2v_2 + \ldots + a_nv_n \rangle = V$ we say that $\{a_1v_1 + a_2v_2 + \ldots + a_nv_n\}$ *spans* V.

THEOREM ***Subspace Test***
Let U be a nonempty subset of a vector space V over a field $\mathbb{F}$. Then U is a subspace of V if, for every u and u' in U and every a in $\mathbb{F}$, $u + u' \in U$ and $au \in U$.

DEFINITION ***Subspace Spanned by $v_1, v_2, \ldots, v_n$, Linear Combination***
Let V be a vector space over $\mathbb{F}$ and let $v_1, v_2, \ldots, v_n$ be (not necessarily distinct) elements of V. Then the subset $\langle v_1, v_2, \ldots, v_n \rangle = \{a_1v_1 + a_2v_2 + \ldots + a_nv_n \mid a_1, a_2, \ldots, a_n \in \mathbb{F}\}$ is called the *subspace of V spanned by* $v_1, v_2, \ldots, v_n$. Any summand of the form $a_1v_1 + a_2v_2 + \ldots + a_nv_n$ is called a *linear combination* of $v_1, v_2, \ldots, v_n$.

Linear Independence

DEFINITION ***Linearly Dependent, Linearly Independent***
A set S of vectors is said to be *linear dependent* over the field $\mathbb{F}$ if there are vectors $v_1, v_2, \ldots, v_n$ from S and scalars $a_1, a_2, \ldots, a_n$ from $\mathbb{F}$, not all zero, such that $a_1v_1 + a_2v_2 + \ldots + a_nv_n = 0$. A set of vectors that is not linearly dependent over $\mathbb{F}$ is called *linearly independent* over $\mathbb{F}$.

DEFINITION ***Basis***
Let V be a vector space over $\mathbb{F}$. A subset B of V is called a *basis* for V if B is linearly independent over $\mathbb{F}$ and every element of V is a linear combination of elements of B.

THEOREM 19.1 ***Invariance of Basis Size***
If $\{u_1, u_2, \ldots, u_n\}$ and $\{w_0, w_1, \ldots, w_n\}$ are both bases of a vector space V, then $m = n$.

DEFINITION ***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. A vector that has a finite basis is called *finite dimensional*; otherwise, it is called *infinite dimensional*.

LEMMA
Let V be a vector space and let $\{v_1, v_2, \ldots\}$ be an infinite dimensional basis for V. Then every basis for V has infinite dimension.

THEOREM ***Every Spanning Collection Contains a Basis***
If $\{v_1, v_2, \ldots, v_n\}$ spans a vector space V, then some subset of the v's is a basis for V.

THEOREM ***Every Independent Set is Contained in a Basis***
Let V be a finite-dimensional vector space and let $\{v_1, v_2, \ldots, v_n\}$ be a linearly independent subset of V. Then, there are vectors $w_1, w_2, \ldots, w_m$ such that $\{v_1, v_2, \ldots, v_n, w_1, \ldots, w_m\}$ is a basis for V.

LEMMA
If U is a proper subsace of a finite-dimensional vector space V, then the dimension of U is less than the dimension of V.

DEFINITION ***Linear Transformation***
A *linear transformation* between two vector spaces V and W is a map $T : V \to W$ such that the following hold:

1. $T(v_1 + v_2) = T(v_1) + T(v_2)$ for any vectors $v_1, v_2 \in V$; and,
2. $T(\alpha v) = \alpha T(v)$ for any scalar α.

LEMMA
Let V and W be vector spaces and let T be a linear transformation from V go W. Then $T(V)$, the image of V under T, is a subspace of W.

DEFINITION ***Kernel of a Linear Transformation***
Let T be a linear transformation of a vector space V. The set $\{v \in V \mid T(v) = 0\}$ is called the *kernel* of T and is a subspace of V.

THEOREM ***Basis maps to Basis***
Let T be a linear transformation of V onto W. If $\{v_1, v_2, \ldots, v_n\}$ spans V then $\{T(v_1), T(v_2), \ldots, T$
spans W.

20 Extension Fields

The Fundamental Theorem of Field Theory

DEFINITION ***Extension Field***
A field E is an *extension field* of a field $\mathbb{F}$ if $\mathbb{F} \subset E$ and the operations of $\mathbb{F}$ are those of E restricted to $\mathbb{F}$.

THEOREM 20.1 ***Fundamental Theorem of Field Theory (Kronecker's Theorem, 1887)***
Let $\mathbb{F}$ be a field and let $f(x)$ be a nonconstant polynomial in $\mathbb{F}[x]$. Then there is an extension field E of $\mathbb{F}$ in which $f(x)$ has a zero.

Splitting Fields

DEFINITION ***Splitting Field***
Let E be an extension field of $\mathbb{F}$ and let $f(x) \in \mathbb{F}[x]$. We say that $f(x)$ *splits* in E if $f(x)$ can be factored as a product of linear factors in $E[x]$. We call E a *splitting field for* $f(x)$ *over* $\mathbb{F}$ if $f(x)$ splits in E but in no proper subfield of E.

THEOREM 20.2 ***Existence of Splitting Fields***
Let $\mathbb{F}$ be a field and let $f(x)$ be a nonconstant element of $\mathbb{F}[x]$. Then there exists a splitting field E for $f(x)$ over $\mathbb{F}$.

THEOREM 20.3 $F(a) \approx F[x]/\langle p(x)\rangle$
Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$. If a is a zero of $p(x)$ in some extension E of $\mathbb{F}$, then $\mathbb{F}(a)$ is isomorphic to $\mathbb{F}/\langle p(x)\rangle$. Furthermore, if $\deg p(x) = n$, then every member of $\mathbb{F}(a)$ can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + c_{n-1}a^{n-2} + \ldots + c_1 a + c_0,$$

where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}$.

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

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

THEOREM 20.4 ***Extending $\phi : F \to F'$***
Let ϕ be an isomorphism from a field F to a field F' and let $f(x) \in \mathbb{F}[x]$. If E is a splitting field for $f(x)$ over $\mathbb{F}$ and E' is a splitting field for $\phi(f(x))$ over $\mathbb{F}'$, then there is an isomorphism from E to E' that agrees with ϕ on $\mathbb{F}$.

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

DEFINITION ***The Splitting Field of $x^n - a$ over $\mathbb{Q}$***
Let a be a positive rational number and let ω be a primitive nth root of unity. Then each of

$$a^{1/n}\omega a^{1/n}, \omega^2 a^{1/n}, \ldots, w^{n-1}a^{1/n}$$

is a zero of $x^n - a$ in $\mathbb{Q}(\sqrt[n]{a}, \omega)$.

Zeros of an Irreducible Polynomial

DEFINITION ***Derivative of a Polynomial***

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + 0$ belong to $\mathbb{F}[x]$. The *derivative* of $f(x)$, denoted by $f'(x)$, is the polynomial $na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a1$ in $\mathbb{F}[x]$.

LEMMA ***Properties of the Derivative***
Let $f(x)$ and $g(x) \in \mathbb{F}[x]$ and let $a \in \mathbb{F}$. Then
- **a.** $(f(x) + g(x))' = f'(x) + g'(x)$
- **b.** $(af(x))' = af'(x)$
- **c.** $(f(x)g(x))' = f(x)g'(x) + g(x)f'(x)$.

THEOREM 20.5 ***Criterion for Multiple Zeros***
A polynomial $f(x)$ over a field $\mathbb{F}$ 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 $\mathbb{F}[x]$.

THEOREM 20.6 ***Zeros of an Irreducible***
Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$. If $\mathbb{F}$ has characteristic 0, then $f(x)$ has no multiple zeros. If $\mathbb{F}$ has characteristic $p \neq 0$, then $f(x)$ has a multiple zero only if it is of the form $f(x) = g(x^p)$ for some $g(x)$ in $\mathbb{F}[x]$.

DEFINITION ***Perfect Field***
A field $\mathbb{F}$ is called *perfect* if $\mathbb{F}$ has characteristic 0 or if $\mathbb{F}$ has characteristic p and $\mathbb{F}^p - \{a^p | a \in \mathbb{F}\} = \mathbb{F}$.

THEOREM 20.7 ***Finite Fields are Perfect***
Every finite field is perfect.

THEOREM 20.8 ***Criterion for No Multiple Zeros***
If $f(x$ is an irreducible polynomial over a perfect field $\mathbb{F}$, then $f(x)$ has no multiple zeros.

THEOREM 20.9 ***Zeros of an Irreducible over a Splitting Field***
Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$ and let E be a splitting field of $f(x)$ over $\mathbb{F}$. Then all zeros of $f(x)$ in E have the same multiplicity.

COROLLARY ***Factorization of an Irreducible over a Splitting Field***
Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$ and let E be a splitting field of $f(x)$. Then $f(x)$ has the form

$$a(x - a_1)^n (x - a_2)^n \ldots (x - a_t)^n$$

where $a_1, a_2, \ldots, a_t$ are distinct elements of E and $a \in \mathbb{F}$.

THEOREM ***$\mathbb{F}$ absorbs its own elements.***
Let $\mathbb{F}$ be a field and let a and b belong to $\mathbb{F}$ with $a \neq 0$. If c belongs to some extension of $\mathbb{F}$, then $\mathbb{F}(c) = \mathbb{F}(ac + b)$.

LEMMA
Let $f(x) \in \mathbb{F}[x]$ and let $a \in \mathbb{F}$. Then, $f(x)$ and $f(x + a)$ have the same splitting field over

$\mathbb{F}$.

LEMMA
Let E be an extension of $\mathbb{F}$ and let a and b belong to E. Then, $\mathbb{F}(a,b) = \mathbb{F}(a)(b) = \mathbb{F}(b)(a)$.

LEMMA
Let $\mathbb{F}$ be a field of characteristic $p \neq 0$. Then the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{F}$ has distinct zeros.

21 Algebraic Extensions

Characterization of Extensions

DEFINITION ***Types of Extensions***
Let E be an extension field of a field $\mathbb{F}$ and let $a \in E$. We call a *algebraic over* $\mathbb{F}$ if a is a zero of some nonzero polynomial in $\mathbb{F}[x]$. If a is not algebraic over $\mathbb{F}$, it is called *transcendental over* $\mathbb{F}$. An extension E of $\mathbb{F}$ is called an *algebraic extension* of $\mathbb{F}$ if every element of E is algebraic over $\mathbb{F}$. If E is not an algebraic extension of $\mathbb{F}$, it is called a *transcendental extension* of $\mathbb{F}$. An extension of $\mathbb{F}$ of the form $\mathbb{F}(a)$ is called a *simple* extension.

THEOREM 21.1 ***Characterization of Extensions***
Let E be an extension field of the field $\mathbb{F}$ andlet $a \in E$. If a is transcendental over $\mathbb{F}$, then $\mathbb{F}(a) \approx F(x)$ If a is algebraic over $\mathbb{F}$, then $\mathbb{F}(a) \approx \mathbb{F}[x]/\langle p(x)\rangle$, where $p(x)$ is a polynomial in $\mathbb{F}[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over $\mathbb{F}$.

THEOREM 21.2 ***Uniqueness Property***
If a is algebraic over a field $\mathbb{F}$, then there is a unique monic irreducible polynomial $p(x)$ in $\mathbb{F}[x]$ such that $p(a) = 0$.

DEFINITION ***Minimal Polynomial for a over $\mathbb{F}$***
The polynomial with the property in Theorem 1.2 is called the *minimal polynomial for a over* $\mathbb{F}$.

THEOREM 21.3 ***Divisibility Property***
Let a be algebraic over $\mathbb{F}$, and let $p(x)$ be the minimal polynomial for a over $\mathbb{F}$. If $f(x) \in \mathbb{F}[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $\mathbb{F}[x]$.

DEFINITION ***Degree n over $\mathbb{F}$***
If a is algebraic over $\mathbb{F}$ and its minimal polynomial over $\mathbb{F}$ has degree n, then $\{1, a \ldots, a^{n-1}\}$ is a basis for $\mathbb{F}(a)$ over $\mathbb{F}$; and therefore, $[\mathbb{F}(a) : \mathbb{F}] = n$. In this case, we say that a has *degree n over* $\mathbb{F}$.

Finite Extensions

DEFINITION ***Degree of an Extension***
Let E be an extension field of $\mathbb{F}$. We say that E *has degree* n *over* $\mathbb{F}$ and write $[E:\mathbb{F}] = n$ if E has dimension n as a vector space over $\mathbb{F}$. If $[E:\mathbb{F}]$ is finite, E is called a *finite extension* of $\mathbb{F}$; otherwise, we say thta E is an *infinite extension* of $\mathbb{F}$.

THEOREM 21.4 ***Finite Implies Algebraic***
If E is a finite extension of $\mathbb{F}$, then E is an algebraic extension of $\mathbb{F}$.

THEOREM 21.5 $[K:\mathbb{F}] = [K:E][E:\mathbb{F}]$
Let K be a finite extension field of the field E and let E be a finite extension field of the field $\mathbb{F}$. Then K is a finite extension of $\mathbb{F}$ and $[K:\mathbb{F}] = [K:E][E:\mathbb{F}]$.

THEOREM 21.6 ***Primitive Elements Theorem (Steinitz, 1910)***
If $\mathbb{F}$ is a field of characteristic 0, and a and b are algebraic over $\mathbb{F}$, then there is an element c in $\mathbb{F}(a,b)$ such that $\mathbb{F}(a,b) = \mathbb{F}(c)$.

DEFINITION ***Primitive Element***
An element a with the property that $E = \mathbb{F}(a)$ is called a *primitive element* of E.

DEFINITION ***Algebraic Closure of*** $\mathbb{F}$ ***in*** E
For any extension of a field $\mathbb{F}$, the subfield of E of the elements that are algebraic over $\mathbb{F}$ is called the *algebraic closure of* $\mathbb{F}$ *in* E.

DEFINITION ***Algebraically Closed***
A field that has no proper algebraic extension is called *algebraically closed*. This field is called the *algebraic closure of* $\mathbb{F}$.

THEOREM ***Complex Numbers Algebraically Closed (Gauss, 1799)***
The set $\mathbb{C}$ of complex numbers is algebraically closed.

LEMMA
Let E be the algebraic closure of $\mathbb{F}$. Then every polynomial in $\mathbb{F}[x]$ splits in E.

LEMMA
Let E be an algebraic extension of $\mathbb{F}$. If every polynomial in $\mathbb{F}[x]$ splits in E, then E is algebraically closed.

LEMMA
Suppose that $f(x)$ and $g(x)$ are irreducible over $\mathbb{F}$ and deg $f(x)$ and deg $g(x)$ are relatively prime. If a is a zero of $f(x)$ in some extension of $\mathbb{F}$, then $g(x)$ is irreducible over $\mathbb{F}(a)$.

LEMMA
Suppose that E is an extension of $\mathbb{F}$ of prime degree. Then, for every a in E, $\mathbb{F}(a) = \mathbb{F}$ or

$\mathbb{F}(a) = E$.

LEMMA
Suppose that E is an extension of $\mathbb{F}$ and $a, b \in E$. If a is algebraic over $\mathbb{F}$ of degree m, and b is algebraic over $\mathbb{F}$ of degree n, where m and n are relatively prime, then $[\mathbb{F}(a, b) : \mathbb{F}] = mn$.

LEMMA
Let E be a field extension of $\mathbb{F}$. Then $[E : \mathbb{F}]$ is finite if and ony if $E = \mathbb{F}(a_1, a_2, \ldots, a_n)$, where $a_1, a_2, \ldots, a_n$ are algebraic over $\mathbb{F}$.

LEMMA
If α and β are real numbers and α and β are transcendental over $\mathbb{Q}$, then either $\alpha\beta$ or $\alpha + \beta$ is also transcendental over $\mathbb{Q}$.

LEMMA
Let $f(x)$ be a nonzero element of $\mathbb{F}[x]$. If a belongs to some extension of $\mathbb{F}$ and $f(a)$ is algebraic over $\mathbb{F}$, then a is algebraic over $\mathbb{F}$.

LEMMA
Let a and b belong to some extension of $\mathbb{F}$ and let b be algebraic over $\mathbb{F}$. Then $[\mathbb{F}(a, b) : \mathbb{F}(a)] \leq [\mathbb{F}(a, b) : \mathbb{F}]$.

Properties of Algebraic Extensions

THEOREM 21.7 ***Algebraic over Algebraic Is Algebraic***
If K is an algebraic extension of E and E is an algebraic extension of $\mathbb{F}$, then K is an algebraic extension of $\mathbb{F}$.

COROLLARY ***Subfield of Algebraic Elements***
Let E be an extension field of the field $\mathbb{F}$. Then the set of all elements of E that are algebraic over $\mathbb{F}$ is a subfield of E.

DEFINITION ***Algebraic Closure***
For any extension E of a field $\mathbb{F}$, the subfield of E of the elements that are algebraic over $\mathbb{F}$ is called the *algebraic closure of* $\mathbb{F}$ *in* E.

22 Finite Fields

Classification of Finite Fields

THEOREM 22.1 ***Classification of Finite Fields***

For each prime p and each positive integer n, there is, up to isomorphism, a unique finite field of order p^n.

Structure of Finite Fields

DEFINITION ***Galois Field***
Because there is only one field for each prime-power p^n, we may unambiguously denote it by $GF(p^n)$ and call it the *Galois field of order* p^n.

THEOREM 22.2 ***Structure of Finite Fields***
As a group under addition, $GF(p^n)$ is isomorphic to

$$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p.$$

As a group under multiplication, the set of nonzero elements of $GF(p^n)$, denoted $GF(p^n)^*$, is isomorphic to $\mathbb{Z}_{p^n-1}$ (and is, therefore, cyclic).

COROLLARY 1
$[GF(p^n) : GF(p)] = n$.

COROLLARY 2 $GF(p^n)$ ***Contains an Element of Degree*** n
Let a be a generator of the group of nonzero elements of $GF(p^n)$ under multiplication. Then a is algebraic over $GF(p)$ of degree n.

Subfields of a Finite Field

THEOREM 22.3 ***Subfields of a Finite Field***
For each divisor m of n, $GF(p^n)$ has a unique subfield of order p^n. Moreover, these are the only subfields of $GF(p^n)$.

LEMMA
If m divides n, then $[GF(p^n) : GF(p^m)] = n/m$.

DEFINITION ***Frobenius Mapping***
The mapping $\phi : GF(p^n) \to GF(p^n)$ given by $a \mapsto a^p$ is a ring automorphism of order n called the *Frobenius mapping*.

LEMMA
Let K be a finite extension field of a finite field $\mathbb{F}$. Then there exists some element $a \in K$ such that $K = \mathbb{F}(a)$.

LEMMA
Any finite subgroup of the multiplicative group of a field is cyclic.

LEMMA
If $g(x)$ is irreducible over $GF(p)$ and $g(x)$ divides $x^{p^n} - x$ then deg $g(x)$ divides n.

LEMMA
If $p(x)$ is a polynomial in $\mathbb{Z}_p[x]$ with no multiple zeros, then $p(x)$ divides $x^{p^n} - x$ for some n.

LEMMA
Any element of $GF(p^n)$ can be written in the form a^p for some unique a in $GF(p^n)$.

LEMMA
Show that no finite field is algebraically closed.

LEMMA
Let E be a splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. The set of zeros of $f(x)$ in E is closed under addition, subtraction, multiplication and division (by nonzero elements).

LEMMA
If $p(x) \in \mathbb{F}[x]$ and deg $p(x) = n$, then the splitting field for $p(x)$ over $\mathbb{F}$ has degree at most $n!$.

LEMMA
Let a be a nonzero algebraic element over $\mathbb{F}$ of degree n. Then a^{-1} is algebraic and of degree n.

LEMMA
If ab is algebraic over $\mathbb{F}$ and $b \neq 0$, then a is algebraic over $\mathbb{F}(b)$.

LEMMA
Let E be an algebraic extension of a field $\mathbb{F}$. If R is a ring and $\supseteq R \supseteq \mathbb{F}$ then R is a field.

LEMMA
If a is transcendental over $\mathbb{F}$, then every element of $\mathbb{F}(a)$ that is not in $\mathbb{F}$ is transcendental over $\mathbb{F}$.

LEMMA
Any finite extension of a finite field is a simply extension.

LEMMA
Let R be an integral domain that contains a field $\mathbb{F}$ as a subring. If R is finite-dimensional when viewed as a vector space over $\mathbb{F}$, then R is a field.

LEMMA
If $a \neq 0$ belongs to a field $\mathbb{F}$ and $x^n - a$ splits in some extension E of $\mathbb{F}$, then E contains all the nth roots of unity.