Math 402/403/404 Notes

Brett Saiki

April 2023

These are notes based on the University of Washington modern algebra sequence (Math 402, 403, and 404) taught by Minseon Shin. The course loosely followed Thomas W. Hungerford's *Abstract Algebra: An Introduction.* These notes mainly contain definitions, propositions, theorems, etc. For proofs and detailed explanations, refer to the actual text.

Contents

1 Arithmetic in $\mathbb{Z}$ Revisited

1.1 The Division Algorithm

Axiom 1.1 (Well-Ordering Axiom). Every nonempty subset of the set of nonnegative integers contains a smallest element.

Theorem 1.2 (The Division Algorithm). Let a, b be integer with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < b.$$

1.2 Divsibility

Definition 1.3. Let a and b be integers with $b \neq 0$. We say that b *divides* a (or that b *is a divisor of* a, or that b *is a factor of* a), if $a = bc$ for some integer c. We denote "b divides a" by $b \mid a$ and "b does not divide a" by $b \nmid a$.

Lemma 1.4. Suppose a, b are integers. Then

(i) a and $-a$ have the same divisors;

(ii) $a \mid 0$ for all $a \in \mathbb{Z}$;

(iii) $1 \mid a$ for all $a \in \mathbb{Z}$;

(iv) if $a \neq 0$ and $b \mid a$, then $|b| \leq |a|$;

Corollary 1.5. Every integer $a \neq 0$ has only finitely many divisors.

Definition 1.6. Let a, b, c be integers. If $c \mid a$ and $c \mid b$ then we say c is a *common divisor* of a and b.

Lemma 1.7. Let $a, b, d \in \mathbb{Z}$ be integers. If $d \mid a$ and $d \mid b$, then $d \mid ma + nb$ for any $m, n \in \mathbb{Z}$.

Definition 1.8. Let a, b are integers such that not both are zero. The *greatest common divisor (gcd)* of a and b is the integer d that divides both a and b. In other words, d is the gcd of a and b provided that

(i) $d \mid a$ and $d \mid b$;

(ii) if $c \mid a$ and $c \mid b$, then $c \leq d$.

The greatest common divisor of a and b is denoted by (a, b).

Theorem 1.9. Let a, b are integers such that not both are zero, and let d be their greatest common divisor. Then there exist integers u and v such that $d = au + bv$.

Corollary 1.10. Let a, b are integers such that not both are zero, and let d be a positive integer. Then d is the greatest common divisor of a and b if and only if d satisfies:

(i) $d \mid a$ and $d \mid b$;

(ii) if $c \mid a$ and $c \mid b$, then $c \mid d$.

Theorem 1.11. If $a \mid bc$ and $(a, c) = 1$ then $a \mid c$.

Definition 1.12. We say that $a, b \in \mathbb{Z}$ are *relatively prime* if $\gcd(a, b) = 1$.

1.3 Primes and Unique Factorization

Definition 1.13. An integer p is said to be *prime* if $p \neq 0, \pm 1$ and the only divisors of p are ± 1 and $\pm p$. If p is not $0, \pm 1$, or prime, then it is *composite*.

Lemma 1.14. Let p, q be integers. Then the following are true:

(i) p if prime if and only if $-p$ is prime;

(ii) if p and q are prime and $p \mid q$, then $p = \pm q$.

Theorem 1.15. Let p be an integer with $p \neq 0, \pm 1$. Then p is prime if and only if p has the following property: whenever $p \mid bc$ for integers b, c, then $p \mid b$ or $p \mid c$.

Corollary 1.16. If p is prime and $p \mid a_1 a_2 \cdots a_n$, then p divides at least one of the a_i.

Theorem 1.17. Every integer n, except $0, \pm 1$, is a product of primes.

Theorem 1.18 (The Fundamental Theorem of Arithmetic). Every integer n except $0, \pm 1$ is a product of primes. This prime factorization is unique in the following sense: if $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ where each p_i, q_j are prime, then $r = s$ and the q's can be reordered (and relabeled) such that $p_1 = \pm q_1, p_2 = \pm q_2, \ldots, p_r = \pm q_r$.

Corollary 1.19. Every integer $n > 1$ has a unique form $n = p_1 p_2 \cdots p_r$, where each p_i is positive and prime and $p_1 \leq p_2 \leq \cdots \leq p_r$.

Theorem 1.20. Let $n > 1$. If n has no positive prime factor p such that $p < \sqrt{n}$, then n is prime.

2 Congruence in $\mathbb{Z}$ and Modular Arithmetic

2.1 Congruence and Congruence Classes

Definition 2.1. Let a, b, n be integer with $n > 0$. Then *a is congruent to b modulo n* provided that n divides $a - b$. In that case, we'd write $a \equiv b \pmod{n}$.

Theorem 2.2. Let n be a positive integer. For all $a, b, c \in \mathbb{Z}$,

(i) $a \equiv a \pmod{n}$;

(ii) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Theorem 2.3. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

(i) $a + c \equiv b + d \pmod{n}$;

(ii) $ac \equiv bd \pmod{n}$.

Definition 2.4. Let a and n be integers with $n > 0$. The *congruence class of a modulo n*, denoted $[a]$, is the set of all integers that are congruent to a modulo n, that is,

$$[a] = \{b \mid b \in \mathbb{Z} \text{ and } b \equiv a \,(\text{mod } n)\}.$$

Theorem 2.5. Let a, c, n be integers with $n > 0$. Then $a \equiv c \,(\text{mod } n)$ if and only if $[a] = [c]$.

Corollary 2.6. Two congruence classes modulo n are either disjoint or identical.

Corollary 2.7. Let $n > 1$ be an integer and consider congruence modulo n.

(i) If a is any integer and r is the remainder when a is divided by n, then $[a] = [r]$.

(ii) There are exactly n distinct congruence classes, namely, $[0], [1], \ldots, [n-1]$.

Definition 2.8. The set of all congruence classes modulo n is denoted $\mathbb{Z}/n\mathbb{Z}$ (read "$\mathbb{Z} \bmod n$").

Lemma 2.9. The set $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements.

2.2 Modular Arithmetic

Theorem 2.10. If $[a] = [b]$ and $[c] = [d]$ in $\mathbb{Z}/n\mathbb{Z}$, then

$$[a+c] = [b+d] \qquad \text{and} \qquad [ac] = [bd].$$

Definition 2.11. Addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ are defined by

$$[a] \oplus [c] = [a+c] \qquad \text{and} \qquad [a] \odot [c] = [ac].$$

Theorem 2.12. For any classes $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$,

(1) if $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, then $[a] \oplus [b] \in \mathbb{Z}^n$ (closed under addition);

(2) $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$ (associative addition);

(3) $[a] \oplus [b] = [b] \oplus [a]$ (commutative addition);

(4) $[a] \oplus [0] = [0] + [a] = [a]$ ($[0]$ is the additive identity);

(5) For each $[a] \in \mathbb{Z}/n\mathbb{Z}$, the equation $[a] \oplus x = [0]$ has a solution in Z_n (additive inverse);

(6) if $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, then $[a] \odot [b] \in \mathbb{Z}^n$ (closed under multiplication);

(7) $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$ (associative multiplication);

(8) $[a] \odot [b] = [b] \odot [a]$ (commutative multiplication);

(9) $[a] \odot ([b] \oplus [c]) = [a] \odot [b] \oplus [a] \odot [c]$ (multiplication distributes);

(10) $[a] \cdot [1] = [1] \cdot [a] = [a]$ ($[1]$ is the multiplicative identity).

Definition 2.13. The same exponent notation used in oridinary arithmetic is also used in $\mathbb{Z}/n\mathbb{Z}$. If $[a] \in \mathbb{Z}/n\mathbb{Z}$, and k is a positive integer, then

$$[a]^k = [a] \odot [a] \odot \cdots \odot [a] \qquad (k \text{ factors}).$$

2.3 $\mathbb{Z}/n\mathbb{Z}$ is an Integral Domain

Lemma 2.14. Let $a, n \in \mathbb{Z}$ with $n > 0$. The element $[a] \in \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if $(a, n) = 1$.

Definition 2.15. Let R be a ring. For any element $r \in \mathbb{R}$, let $\mu_r : R \to R$ be the "multiplication-by-r map", i.e. $\mu_r(x) = rx$ for all $x \in \mathbb{R}$. We say that r is a *non-zero divisor* if μ_r is injective; otherwise r is a *zero divisor*.

Lemma 2.16. Let $r \in \mathbb{Z}/n\mathbb{Z}$ and let $f(x) = rx$ for all $x \in \mathbb{Z}/n\mathbb{Z}$. The following are equivalent:

(i) r is a unit;

(ii) f is bijective;

(iii) f is surjective.

Lemma 2.17. In a finite ring R, every non-zero divisor is a unit.

Definition 2.18. Let R be a ring. We say that R is an *integral domain* if every non-zero element is a non-zero divisor. We say that R is a *field* if every non-zero element is a unit.

Theorem 2.19. Let $n > 1$. The following are equivalent:
(i) n is prime;
(ii) $\mathbb{Z}/n\mathbb{Z}$ is an integral domain;
(iii) $\mathbb{Z}/n\mathbb{Z}$ is a field.

2.4 Chinese Remainder Theorem

Definition 2.20. Given two rings R, S, their *product ring* is the set

$$R \times S = \{(r, s) : r \in R, s \in S\}$$

with addition and multiplication defined by

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

for all $r_i \in \mathbb{R}$ and $s_i \in S$.

Definition 2.21. Given a, n with $n > 0$, we let $[a]_n$ be a congruence class modulo n. If $m \mid n$, there is a ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ sending $[a]_n \to [a]_m$ for all $a \in \mathbb{Z}$. For any integers $m, n > 0$, we define the ring homomorphism

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}n\mathbb{Z}$$

sending

$$[a]_{mn} \to ([a]_m, [a]_n)$$

for all $a \in \mathbb{Z}$.

Theorem 2.22 (Chinese Remainder Theorem). The map φ is bijective if and only if $(m, n) = 1$.

Corollary 2.23. If $n = p_1^{e_1} \cdots p_r^{e_r}$ where p_i are distinct primes, then there is an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

of rings.

3 Rings

3.1 Definition and Properties Rings

Definition 3.1. A *ring* is a nonempty set R equipped with two operations (usually written as addition and multipication) that satisfy the following axioms. For all $a, b, c \in R$:
(1) if $a \in R$ and $b \in R$, then $a + b \in R$ (closure of addition);
(2) $a + (b + c) = (a + b) + c$ (associative addition);

(3) $a + b = b + a$ (commutative addition);

(4) there is an element $0 \in R$ such that $a + 0 = a + 0 = a$ for every $a \in R$ (additive identity);

(5) for each $a \in R$, the equation $a + x = 0$ has a solution in R (existence of additive inverse);

(6) if $a \in R$ and $b \in R$, then $ab \in R$ (closure of multiplication);

(7) $a(bc) = (ab)c$ (associative multiplication);

(8) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (distributive laws);

Definition 3.2. A *commutative ring* is a ring R that satisfies:

$$ab = ba \text{ for all } a, b \in \mathbb{R} \qquad \text{(commutative multiplication).}$$

Definition 3.3. A *ring with identity* is a ring R that contains an element 1 that satisfies:

$$a1 = 1a = a \text{ for all } a \in \mathbb{R} \qquad \text{(multiplicative identity).}$$

Definition 3.4. A *division ring* is a ring with identity R that satisfies the following: for each $a \in R$, the equation $ax = 1$ has a solution in R (existence of the multiplicative inverse);

Definition 3.5. A *field* is a division ring that also satisfies commutative multiplication.

3.2 Example of Rings

Definition 3.6. Let R be a ring. We say that an element $l \in R$ is a *left identity* if $lx = x$ for all $x \in R$. We say that an element $r \in R$ is a *right identity* if $xr = x$ for all $x \in R$. We say that an element $1 \in R$, is a identity if it is both an left and right identity.

Definition 3.7. Let R be a ring with identity and let $a, b \in R$ be elements. We say that a is a *left inverse* to b (and b is a *right inverse* to a) if $a \cdot b = 1$. We say that u is *unit* if it has both a left inverse and right inverse.

Definition 3.8. Let R be a ring, and let $a \in R$ be an element. Let $\mu : R \to R$ be the left multiplication-by-a map, i.e. $\mu(x) = a \cdot x$. Let $\nu : R \to R$ be the right multipication-by-a map, i.e. $\mu(x) = x \cdot a$. We say that a is a *non-zero divisor* if both μ and ν are injective.

Lemma 3.9. The additive identity 0 is unique. The multiplicative identity 1 is unique (if it exists).

Lemma 3.10. The additive inverse $-a$ is unique. If R is commutative, then multiplicative inverses are unique (if they exists).

Lemma 3.11. Let R be a ring,

(i) if $a + b = a + c$, then $b = c$;

(ii) $a \cdot 0 = 0 \cdot a = 0$;

(iii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;

(iv) $-(-a) = a$;

(v) $-(a + b) = (-a) + (-b)$;

(vi) $(-a) \cdot (-b) = ab$.

If R has the identity element, then $(-1) \cdot a = -a$.

Remark. Examples of rings:

(i) The rings $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ are commutative with identity.
(ii) The zero ring $R = 0$ contains only one element 0.
(iii) For $n \in \mathbb{Z}$, the set $R = n\mathbb{Z}$ is a commutative ring with identity if and only if $|n| \leq 1$.
(iv) For a set X and ring R, the set of functions $f : X \to R$ such that $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$ is a ring.
(v) Given a commutative ring R with identity, the set $S = R[x_1, \ldots, x_n]$ of (multivariate) polynomials in variables $x_1, \ldots, x_n$ with coefficients in R is a commutative rings with identity.
(vi) Given a ring R, the set $M_n(R)$ of $n \times n$ matrices with entries in R is a ring using the usual matrix addition and matrix multiplication. The additive identity is the zero matrix. If R has identity, then the multiplicative identity is the identity matrix.

Lemma 3.12. Let R be a commutative ring with identity and set $S = M_n(R)$. If $u, v \in S$ such that $u \cdot_S v = id_n$, then $v \cdot_S u = id_n$.

Definition 3.13. Let R be a ring and let $S \subset R$ be a subset. We say that S is a *subring* of R if
(i) if $a, b \in S$, then $a + b \in S$ (closed under addition);
(ii) if $a, b \in S$, then $a \cdot b \in S$ (closed under multiplication);
(iii) $0 \in S$;
(iv) if $a \in S$; then $-a \in S$.

3.3 Ring Homomorphisms

Definition 3.14. Let R, S be rings and let $f : R \to S$ be a function. We say that f is a *ring homomorphism* if
(i) $f(a +_R b) = f(a) +_S f(b)$,
(ii) $f(a \cdot_R b) = f(a) \cdot_S f(b)$
for all $a, b \in R$. A bijective ring homomorphism is called a *ring isomorphism*. If R, S have identity and f satisfies
(iii) $f(1_R) = 1_S$,
then f is a *unital ring homomorphism*.

Lemma 3.15. If f is a ring isomorphism, then the inverse function f^{-1} is also a ring isomorphism.

Lemma 3.16. Let $f : R \to S$ be a ring homomorphism.
(i) $f(0_R) = 0_S$.
(ii) $f(-a) = -f(a)$.
(iii) $f(R)$ is a subring of S.
If R has identity:
(iv) $f(R)$ has identity;
(v) $f(1_R) = 1_{f(R)}$;
(vi) if in addition f is surjective, then $f(1_R) = 1_S$.

Lemma 3.17. Let R, S be commutative rings with identity, let $\varphi : R \to S$ be a ring isomorphism.
(i) $a \in R$ is a unit if and only if $\varphi(a) \in S$ is a unit.
(ii) $a \in R$ is irreducible if and only if $\varphi(a) \in S$ is irreducible.

(iii) $a \in R$ is prime if and only if $\varphi(a) \in S$ is prime.

Remark. There are a few techniques to show that two rings are not isomorphic. Cardinality: if the number of objects in each ring are different, then the rings are not isomorphic. Number of units: if the number of units in a ring are different, then the rings are not isomorphic. Number of solutions to equations: if an equation (meaningful in both rings) yields a different number of solutions.

4 Arithmetic in $F[x]$

4.1 The Polynomial Ring

Definition 4.1. Let R be a ring. A *polynomial* with coefficients in R is an infinite vector

$$a = (a_0, a_1, a_2, \ldots)$$

where each $a_i \in R$ and there exists an n such that $a_i = 0_R$ for $i > n$. The set of all polynomials with coefficients is the polynomial ring $R[x]$. Given $a = (a_0, a_1, a_2, \ldots)$ and $b = (b_0, b_1, b_2, \ldots)$ in $R[x]$, their sum is defined as

$$a +_{R[x]} b = (a_0 +_R b_0, a_1 +_R b_1, a_2 +_R b_2, \ldots)$$

and their product

$$a \cdot_{R[x]} b = ((a \cdot_{R[x]} b)_0, (a \cdot_{R[x]} b)_1, (a \cdot_{R[x]} b)_2, \ldots)$$

has kth coordinate

$$(a \cdot_{R[x]} b)_k = \sum_{i+j=k} a_i \cdot_R b_k + a_1 \cdot_R b_{k-1} + \ldots + a_k \cdot_R b_0.$$

for all $k \geq 0$. In terms of notation, the expression $a_0 + a_1 x + \cdots + a_n x^n$ is equivalent to $(a_0, a_1, \ldots, a_n, 0_R, \ldots)$.

Lemma 4.2. Let R be a ring.

(i) The set $R[x]$ is a ring under $+_R$ and $\cdot_R$ and the additive identity is $0_{R[x]} = (0_R, 0_R, \ldots)$.

(ii) If R is commutative, then $R[x]$ is commutative.

(iii) If R has identity, then $R[x]$ also has identity and $1_{R[x]} = (1_R, 0_R, 0_R, \ldots)$.

Lemma 4.3. If $a, b \in R[x]$ and $a_i = 0$ for $i > 0$, then

$$a \cdot_{R[x]} b = (a_0, 0_R, \ldots) \cdot_{R[x]} (b_0, b_1, b_2, \ldots) = (a_0 \cdot b_0, a_0 \cdot b_1, a_0 \cdot b_2, \ldots).$$

Lemma 4.4. The function $R \to R[x]$ defined by $f(a) = (a, 0_R, \ldots)$ is an injective ring homomorphism.

Definition 4.5. A polynomial a satisfying $a_i = 0$ for $i > 0$ is called *constant*. By Lemma 4.4, the constant polynomials form a subring of $R[x]$ that is isomorphic to R.

Lemma 4.6. Let x^n be the polynomial with 1_R in the nth position and 0_R elsewhere, i.e. $(x^n)_n = 1_R$ and $(x^n)_i = 0_R$ if $i \neq n$. For any $a = (a_0, a_1, a_2, \ldots) \in R[x]$, we have

$$x^n \cdot_{R[x]} a = (0_R, \ldots, 0_R, a_0, a_1, a_2, \ldots)$$

where, on the right side, each a_i is in the $(n+1)$th position.

Remark. Polynomials should not be thought of as functions. For $R = \mathbb{Z}/2\mathbb{Z}$, the polynomials x and x^2 define the same function $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, but they are considered different since their coefficients are different. More generally, if R is a finite ring, there are finitely many functions $R \to R$ but infinitely many elements in $R[x]$ so by the Pigeonhole Principle there must exist a function $f : R \to R$ such that there are infinitely many polynomials whose corresponding function is f.

Lemma 4.7. Let R, S be commutative rings with identity and let $\varphi : R \to S$ be a (unital) ring homomorphism. For every $s \in S$, there exists a unique (unital) ring homomorphism $\varphi_s : R[x] \to S$ such that $\varphi_s(x) = s$ and $\varphi_s(r) = \varphi(r)$ for all $r \in R$.

4.2 Division Algorithm for Polynomials

Definition 4.8. Let $a \in R[z] \setminus \{0_{R[x]}\}$ The *degree* of a, denoted $\deg(a)$, is the largest n for which $a_n \neq 0_R$; this a_n is called the *leading coefficient* of a, denoted $\mathrm{lc}(a)$. If $\mathrm{lc}(a) = 1_R$, then a is *monic*. By definition,

$$\mathrm{lc}(a) = a_{\deg(a)} \neq 0_R$$

for all $a \neq 0_{R[x]}$.

Lemma 4.9. Let R be a commutative ring with identity and let $a, b \in R[z] \setminus \{0_{R[x]}\}$.

(i) If $a +_{R[x]} b \neq 0_{R[x]}$, then $\deg(a +_{R[x]} b) \leq \max(\deg(a), \deg(b))$.

(ii) If $a \cdot_{R[x]} b \neq 0_{R[x]}$, then $\deg(a \cdot_{R[x]} b) \leq \deg(a) + \deg(b)$.

(iii) If $\mathrm{lc}(a) \cdot_R \mathrm{lc}(b) \neq 0_R$, then $a \cdot_{R[x]} b \neq 0_{R[x]}$ and $\deg(a \cdot_{R[x]} b) = \deg(a) + \deg(b)$ and $\mathrm{lc}(a \cdot_{R[x]} b) = \mathrm{lc}(a) \cdot_R \mathrm{lc}(b)$.

Lemma 4.10. Let R be a ring and let $a, b \in R[x] \setminus \{0_{R[x]}\}$. If $\mathrm{lc}(b)$ is a non-zero divisor and $\deg(b) > \deg(a)$, then b does not divide a.

Lemma 4.11. If R is an integral domain, then $R[x]$ is an integral domain.

Theorem 4.12 (Division Algorithm for Polynomials). Let R be a commutative ring with identity, let $a, b \in R[x]$ with $b \neq 0_{R[x]}$. If $\mathrm{lc}(b)$ is a unit (of R), then exist unique $q, r \in R[x]$ such that:

(i) $a = bq + r$,

(ii) either $r = 0$ or $\deg(r) < \deg(b)$.

Theorem 4.13. Let F be a field, let $a, b \in F[x]$ be polynomials (not both 0). There exists a unique polynomial $g \in F[x]$ such that:

(i) g is monic ($\mathrm{lc}(g) = 1$);

(ii) g is a common divisor of a, b

(iii) g is a $F[x]$-linear combination of a, b.

Definition 4.14. Let F be a field and let $a, b \in F[x]$ (not both 0). The polynomial g in Theorem 4.13 is called the *greatest common divisor* of a, b, denoted $\gcd(a, b)$.

Remark. The Euclidean algorithm for integers also works for $F[x]$.

Lemma 4.15. Let F be a field, and let $a, b, c \in F[x]$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

4.3 Unique Factorization in $F[x]$

Lemma 4.16. Let R be an integral domain and let $a \in R[x]$ be a polynomial. Then a is a unit (of $R[x]$) if and only if $\deg(a) = 0$ and a_0 is a unit (of R).

Lemma 4.17. Let F be a field, let $a \in F[x]$ be a nonzero polynomial. Then a is a unit if and only if $\deg(a) = 0$.

Lemma 4.18. Let F be a field and let $p \in F[x]$ be a polynomial. The following are equivalent:

(i) p is irreducible;

(ii) p is prime;

(iii) there does not exist $b, c \in F[x]$ such that $p = bc$ and $\deg(b), \deg(c) \geq 1$.

Lemma 4.19. Let F be a field, and let $p \in F[x]$ be a polynomial.

(i) If $\deg(p) = 1$, then p is irreducible.

(ii) If $\deg(p) = 2$ or 3, then p is irreducible if and only if p does not have a factor of degree 1.

Definition 4.20. Let R be a commutative ring with identity, and let $a, b \in R$. We say that a and b are *associates* if there exists a unit $u \in R$ such that $a = ub$.

Lemma 4.21. Let R be a commutative ring with identity and suppose a and b are associates. For any $c \in R$, we have:

(i) $c \mid a \Leftrightarrow c \mid b$, i.e. a, b have the same divisors;

(ii) $a \mid c \Leftrightarrow b \mid c$, i.e. a, b have the same multiples.

Lemma 4.22. Let R be an integral domain. If a is a non-zero prime element, then a is irreducible.

Lemma 4.23. Let R be an integral domain, and let $a, b \in R$ be non-zero elements. If $a \mid b$ and $b \mid a$, then a and b are associates.

Remark. In $\mathbb{Z}$, every non-zero integer is associates with a unique positive integer (divide by the sign of the integer). In $F[x]$, every non-zero polynomial is associates with a unique monic polynomial (dividing by the leading coefficient).

Lemma 4.24. Let F be a field. Every monic polynomial in $F[x]$ is a product of monic irreducible polynomials.

Definition 4.25. Let F be a field, let M_F be the set of monic polynomials in $F[x]$. Let $P_F \subset M_F$ be the subset of monic irreducible polynomials in $F[x]$. Define

$$S_F = \{\text{functions } e : P_F \to \mathbb{Z}_{\geq 0} \text{ such that } e^{-1}(\mathbb{Z}_{\geq 1}) \text{ is finite}\},$$

and define the function $\varphi : S_F \to M_F$ by

$$\varphi(e) = \prod_{p \in e^{-1}(\mathbb{Z}_{\geq 1})} p^{e(p)}$$

for all $e \in S_F$.

Lemma 4.26. We have

$$\varphi(e + f) = \varphi(e) \cdot \varphi(f)$$

for all $e, f \in S_F$.

Theorem 4.27 (Unique factorization in F[x]). The map φ is a bijection.

Corollary 4.28. Let F be a field and let $a, b \in M_F$. Let $e, f \in S_F$ such that $\varphi(e) = a$ and $\varphi(f) = b$. Then $b \mid a$ if and only if $e(p) \leq f(p)$ for all $p \in P_F$.

4.4 Factors of Degree One

Definition 4.29. Let R be a commutative ring with identity, let $a \in R$. There is a ring homomorphism $ev_a : R[x] \to R$ defined by

$$ev_a\left(\sum_{i\geq 0} f_i x^i\right) = \sum_{i\geq 0} f_i a^i$$

for all $f = \sum_{i\geq 0} f_i x^i \in R[x]$. This is called the *evaluation map* at $x = a$. The expression is denoted $f(a)$.

Lemma 4.30. Let R be a commutative ring with identity. Let $f \in R[x]$ and let $a \in R$. Then

(i) $x - a \mid f - f(a)$;

(ii) the remainder upon dividing f by $x - a$ is $f(a)$;

(iii) $x - a \mid f$ if and only if $f(a) = 0$.

Definition 4.31. If condition (iii) is true in Lemma 4.30, we say that a is a *root* (or *zero*) of f.

Lemma 4.32. Let R be an integral domain, and let $f \in R[x] \mid \{0\}$, and let $n = \deg(f)$. Then

(i) f has at most n distinct roots;

(ii) if f has exactly n distinct roots $r_1, \ldots, r_n$, then

$$f = \operatorname{lc}(f) \cdot (x - r_1) \cdots (x - r_n).$$

Lemma 4.33. Let F be a field, and let $f \in F[x] \mid \{0\}$.

(i) If f is irreducible and $\deg(f) \geq 2$, then f has no root in F.

(ii) If f has no root in F and $\deg(f) = 2$ or 3, then f is irreducible.

Remark. There's no systematic way of finding roots of a polynomial that works for every field F and every polynomial $f \in F[x]$. There exist quadratic, cubic, and quartic formulas that give expressions for the roots of f, but a caveat is that these work only when 2, 6, 6 are units of F, respectively.

4.5 Factoring in $\mathbb{Q}[x]$

Remark. For every $f \in \mathbb{Q}[x]$, there exists $n \in \mathbb{Z}_{n\geq 1}$ such that $nf \in \mathbb{Z}[x]$ (where n is the least common multiple of the denominators of the coefficients of f). Note that n is a unit of $\mathbb{Q}[x]$, so f, nf are associates in $\mathbb{Q}[x]$, so they have the same factors in $\mathbb{Q}[x]$.

To factor a polynomial $f \in \mathbb{Q}[x]$ of degree 2 or 3, it is enough to check whether it has any roots in $\mathbb{Q}$.

Theorem 4.34. Let $f = f_0 + f_1 x + \cdots + f_n x^n \in \mathbb{Z}[x]$, and let $r \in \mathbb{Q}$ be a non-zero root of f. If $r = p/q$ for some $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$, then $q \mid f_n$ and $p \mid f_0$.

Lemma 4.35. Let R be a commutative ring with identity. If $p \in R$ is prime, then p is prime in $R[x]$.

Definition 4.36. Let $f = f_0 + f_1 x + \cdots f_n x^n \in \mathbb{Z}[x]$ be a polynomial. We say that f is primitive if $\gcd(f_0, f_1, \ldots, f_n) = 1$.

Lemma 4.37. If $f, g \in \mathbb{Z}[x]$ are primitive, then $f \cdot g$ is primitive.

Lemma 4.38. Let $f, g \in \mathbb{Z}[x]$ and suppose $n \in \mathbb{Z}_{\geq 1}$ such that $n \mid fg$. Then there exist $a, b \in \mathbb{Z}_{\geq 1}$ such that $n = ab$ and $a \mid f$ and $b \mid g$ (in $\mathbb{Z}[x]$).

Lemma 4.39. Let $f \in \mathbb{Z}[x]$ be a polynomial and let $m, n \in \mathbb{Z}_{\geq 0}$. The following are equivalent:
(i) There exist $g, h \in \mathbb{Z}[x]$ such that $f = gh$ and $\deg(g) = m$ and $\deg(h) = n$.
(ii) There exist $g', h' \in \mathbb{Q}[x]$ such that $f = g'h'$ and $\deg(g') = m$ and $\deg(h') = n$.

Theorem 4.40. Let $f \in \mathbb{Z}[x]$ be a primitive polynomial. Then f is irreducible in $\mathbb{Z}[x]$ if and only if f is irreducible in $\mathbb{Q}[x]$.

Remark. In Theorem 4.40, the hypothesis "primitive" is required because there are non-units of $\mathbb{Z}[x]$ that becomes units in $\mathbb{Q}[x]$, namely the non-units of $\mathbb{Z}$, viewed as constant polynomials in $\mathbb{Z}[x]$. Moreover, "prime" and "irreducible" are relative properties, i.e. we must always specify what ring we're considering.

Theorem 4.41 (Eisenstein's Criterion). Let $f = f_0 + f_1x + \cdots + f_nx^n \in \mathbb{Z}[x]$ be a polynomial with $\deg(f) = n$. If there exists a prime $p \in \mathbb{Z}$ such that
(i) $p \nmid f_n$,
(ii) $p \mid f_i$ for all $i = 0, \ldots, n-1$, and
(iii) $p^2 \nmid f_0$,
then f is irreducible in $\mathbb{Q}[x]$.

Lemma 4.42. The function $f : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ sending

$$f = f_0 + f_1x + \cdots + f_nx^n \to \overline{f} = [f_0] + [f_1]x + \cdots + [f_n]x^n.$$

Theorem 4.43. Let $f \in \mathbb{Z}[x]$ and suppose there exists a prime $p \in \mathbb{Z}$ such that $p \nmid \mathrm{lc}(f)$ and $\overline{f} \in (\mathbb{Z}/p\mathbb{Z})[x]$ is irreducible. Then f is irreducible in $\mathbb{Q}[x]$.

Remark. The Theorem 4.43 is not always enough, i.e. there are polynomials $f \in \mathbb{Z}[x]$ which are irreducible in $\mathbb{Q}[x]$ but not irreducible in $(\mathbb{Z}/p\mathbb{Z})[z]$ for all primes $p \in \mathbb{Z}$.

4.6 Factoring in $\mathbb{C}[x]$

Definition 4.44. A field F is called *algebraically closed* if every non-constant polynomial $f \in F[x]$ has a root.

Theorem 4.45 (Fundamental Theorem of Algebra). The field $\mathbb{C}$ is algebraically closed.

Lemma 4.46. Let F be an algebraically closed field.
(i) A polynomial $f \in F[x]$ is irreducible if and only if $\deg(f) = 1$.
(ii) Every polynomial $f \in F[x]$ factors as

$$f = \mathrm{lc}(f) \cdot (x - r_1) \cdots (x - r_n)$$

for some $r_1, \ldots, r_n \in F$.

4.7 Factoring in $\mathbb{R}[x]$

Remark. To factor $f \in \mathbb{R}[x]$, we first factor f in $\mathbb{C}[x]$, then map back to $\mathbb{R}[x]$.

Definition 4.47. Let $\sigma : \mathbb{C} \to \mathbb{C}$ denote the *complex conjugate* map, defined by $\sigma a + bi = a - bi = \overline{a + bi}$ for any $a, b \in \mathbb{R}$. For any $x \in \mathbb{C}$, we denote $\sigma(x)$ by $\overline{x}$.

Lemma 4.48. The complex conjugate map is a ring isomorphism. For any $x \in \mathbb{C}$, we have $x = \overline{x}$ if and only if $x \in \mathbb{R}$.

Lemma 4.49. Let $f \in \mathbb{R}[x]$ and let $r \in \mathbb{C}$. Then r is a root of f if and only if $\overline{r}$ is a root of f.

Theorem 4.50. If a polynomial $f \in \mathbb{R}[x]$ satisfies one of
(i) $\deg(f) = 1$,
(ii) $\deg(f) = 2$ and $f = a_2x^2 + a_1x + a_0$ where $a_1^2 - 4a_2a_0 < 0$.
then f is irreducible (in $\mathbb{R}[x]$). Futhermore, every irreducible polynomial in $\mathbb{R}[x]$ satisfies (i) or (ii).

Lemma 4.51. If $f \in \mathbb{R}[x]$ has odd degree, then f has a root (in $\mathbb{R}$).

5 The Ring $F[x]/p$

5.1 Congruence $\bmod p$ and the Definition of $F[x]/p$

Definition 5.1. We say $f, g \in F[x]$ are *congruent modulo* p, written $f \equiv g \pmod p$, if $p \mid f - g$ in $F[x]$.

Lemma 5.2. Congruence modulo p defines an equivalence relation on $F[x]$, i.e.
(i) $f \equiv f \pmod p$;
(ii) $f \equiv g \pmod p$ if and only if $g \equiv f \pmod p$;
(iii) if $f \equiv g \pmod p$, $g \equiv h \pmod p$, then $f \equiv h \pmod p$.

Definition 5.3. The *congruence class of* f mod p is

$$[f] = \{g \in F[x] : g \equiv f \pmod p\}.$$

Lemma 5.4. Let $f, g \in F[x]$. Then
(i) $f \equiv g \pmod p$ if and only if $[f] = [g]$;
(ii) either $[f] \cap [g] = \emptyset$ or $[f] = [g]$.

Definition 5.5. We define $F[x]/p$ be the set of congruence classes $\bmod p$. We define the addition and multiplication laws on $F[x]/p$ to be:

$$[f] +_{F[x]/p} [g] = [f + g] \qquad [f] \cdot_{F[x]/p} [g] = [f \cdot g]$$

for any $f, g \in F[x]$. This is well-defined by similar argument to Theorem 2.10.

5.2 Description of $F[x]/p$

Definition 5.6. For any $n \geq 0$, let $F[x]_{<n}$ denote the set of polynomials $f \in F[x]$ such that $f_i = 0$ for all $i \geq n$.

Theorem 5.7. Let $n = \deg(p)$, and let

$$\varphi : F[x]_{<n} \to F[x]/p$$

be the function defined by $\varphi(a) = [a]$ or all $a \in F[x]_{<n}$. Then φ is an isomorphism of F-vector spaces.

Remark. Note that $F[x]_{<1}$ are just constant polynomials of $F[x]$. In particular if $\deg(p) \geq 1$, the composition

$$F \simeq F[x]_{<1} \subseteq F[x]_{<\deg(p)} \simeq F[x]/p$$

gives an injective function $F \to F[x]/p$ which is in fact a ring homomorphism.

5.3 Conditions when $F[x]/p$ is an Integral Domain / Field

Lemma 5.8. For $f \in F[x]$, the following are equivalent:
(i) $\gcd(f, p) = 1$;
(ii) $[f]$ is a non-zero divisor of $F[x]/p$;
(iii) f is a unit of $F[x]/p$.

Lemma 5.9. The following are equivalent:
(i) p is irreducible;
(ii) $F[x]/p$ is an integral domain;
(iii) $F[x]/p$ is a field.

5.4 Field Extensions and Roots

Lemma 5.10. The ring $K = F[x]/p$ contains a root of p.

Definition 5.11. If $F \to K$ is a unital ring homomorphism of fields, we say that K is a *field extension* of F.

Lemma 5.12. Let F be a field, and let $f \in F[x] \setminus \{0\}$ be a monic polynomial with $\deg(f) \geq 1$.
(i) There exists a field extension K of F such that f has root in K.
(ii) There exists a field extension K of F such that there exist $r_1, \ldots, r_n \in K$ with

$$f = (x - r_1) \cdots (x - r_n)$$

in $K[x]$.

6 Ideals and Quotient Rings

6.1 Ideals

Definition 6.1. Let R be a ring, and let I be a nonempty subset of R. We say that I is an *ideal* (of R) if it satisfies the following conditions:
(i) if $a_1, a_2 \in I$, then $a_1 + a_2 \in I$;
(ii) if $r \in R$ and $a \in I$, then $ra \in I$.

Lemma 6.2. Let R be a ring, and let I be an ideal of R. If $r_1, \ldots, r_n \in R$, and $a_1, \ldots, a_n \in I$, then

$$r_1 a_1 + \cdots + r_n a_n \in I.$$

Lemma 6.3. Let R be a ring, and let $a_1, \ldots, a_n \in R$ be elements of R. Then the subset

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R\}$$

is an ideal of R.

Definition 6.4. Let R be a ring, and let I be an ideal of R. If there exist elements $a_1, \ldots, a_n \in I$ such that

$$I = (a_1, \ldots, a_n)$$

then we say that I is *finitely generated*, and that I is *generated by* $a_1, \ldots, a_n$ and $\{a_1, \ldots, a_n\}$ is a *generating set* of I. If there exists a single $a \in R$ such that $I = (a)$, we say that I is a *principal ideal*.

Definition 6.5. If R is a ring for which every ideal is finitely generated, we say that R is a *Noetherian ring*.

Lemma 6.6. Let R be an integral domain, and let $a, b \in R$ be nonzero elements.
(i) We have $(a) \subseteq (b) \Leftrightarrow a \in (b) \Leftrightarrow b \mid a$.
(ii) We have $(a) = (b) \Leftrightarrow a, b$ are associates.

Lemma 6.7 ($\mathbb{Z}$ is a Principal Ideal Domain). Consider the ring $R = \mathbb{Z}$.
(i) Every ideal I of $\mathbb{Z}$ is a principal ideal.
(ii) For any $a_1, \ldots, a_n \in \mathbb{Z}$, we have

$$(a_1, \ldots, a_n) = (\gcd(a_1, \ldots, a_n))$$

as ideals of $\mathbb{Z}$.

Lemma 6.8 ($F[x]$ is a Principal Ideal Domain). Let F be a field, and consider the ring $R = F[x]$.
(i) Every ideal I of $F[x]$ is a principal ideal.
(ii) For any $a_1, \ldots, a_n \in F[x]$, we have

$$(a_1, \ldots, a_n) = (\gcd(a_1, \ldots, a_n))$$

as ideals of $F[x]$.

Lemma 6.9. Let R be a ring. Let $\{a_1, \ldots, a_n\}$, $\{a'_1, \ldots, a'_n\} \subset R$ be two subset of R such that $\{a'_1, \ldots, a'_n\}$ is obtained from $\{a_1, \ldots, a_n\}$ by doing a finite number of elementary operations:
(i) multiply some a_i by a unit $u \in R$;
(ii) switch a_i and a_j for some $i, j \in \{1, \ldots, n\}$;
(iii) replace a_j by $a_j + ra_i$ for distinct $i, j \in \{1, \ldots, n\}$ and $r \in R$.
Then

$$(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n)$$

as ideals of R, i.e. the ideals generated by $\{a_1, \ldots, a_n\}$ and $\{a'_1, \ldots, a'_n\}$ are equal.

Remark. An ideal I often has more than one generating set, so the general goal is to find the "minimal" generating set of an ideal. To reduce a generate, eliminate any element of the generating set that is zero or a linear combination of others.

Lemma 6.10. Let R be a ring, and let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be an infinite sequence of inclusions of ideals of R. Then the union

$$I = \bigcup_{n \in \mathbb{N}} I_N$$

is an ideal of R.

6.2 Congruence $\pmod{I}$ and the Definition of R/I

Definition 6.11. Let R be a ring, and let I be an ideal of R. We say that a, b are *congruent modulo* I, written $a \equiv b \pmod{I}$ if $a - b \in I$.

Lemma 6.12. Congruence modulo I defines an equivalence relation of R, i.e.

(i) $a \equiv a \pmod{I}$;

(ii) $a \equiv b \pmod{I}$ if and only if $b \equiv a \pmod{I}$;

(iii) if $a \equiv b \pmod{I}$, $b \equiv c \pmod{I}$, then $a \equiv c \pmod{I}$.

Definition 6.13. The *congruence class of a modulo I* is the set

$$a + I = \{b \in R : b \equiv a \pmod{I}\}.$$

Lemma 6.14. Let $a, b \in R$.

(i) We have $a \equiv b \pmod{I}$ if and only if $a + I = b + I$.

(ii) Either $a + I \cap b + I = \emptyset$ or $a + I = b + I$.

Definition 6.15. For a ring R and ideal I of R, the quotient ring of R by I is

$$R/I = \{\text{congruence classes modulo } I\}.$$

The addition and multiplication in R/I is defined as follows:

$$(a + I) +_{R/I} (b + I) = (a +_R b) + I$$
$$(a + I) \cdot_{R/I} (b + I) = (a \cdot_R b) + I$$

for any $a, b \in R$. This is well-defined by a similar argument to Theorem 2.10. In R/I, the additive identity is $0_{R/I} = 0 + I$, and the multiplicative identity $1_{R/I} = 1 + I$. Furthermore, R/I is commutative.

Definition 6.16. The quotient ring R/I comes with a special ring homomorphism

$$\pi : R \to R/I$$

defined by $\pi(r) = r + I$. This is called the *natural homomorphism* from R to R/I.

Lemma 6.17. Let $f : R \to S$ be a ring homomorphism. If J is an ideal of S, then the preimage $f^{-1}(J)$ is an ideal (of R).

Definition 6.18. Let $f : R \to S$ be a ring homomorphism. The *kernel* of f is $\ker(f) = f^{-1}(\{0_S\})$.

Lemma 6.19. Let $f : R \to S$ be a ring homomorphism. Then $\{0_R\} \subset \ker(f)$, and f is injective if and only if $\ker(f) = \{0_R\}$.

Theorem 6.20. Let $f : R \to S$ be a ring homomorphism with kernel $K = \ker(f)$.

(i) There exists a unique ring homomorphism

$$\overline{f} : R/K \to S$$

such that $\overline{f}(a + K) = f(a)$ for all $a \in R$.

(ii) The ring homomorphism $\overline{f}$ is injective.

(iii) If f is surjective, then $\overline{f}$ is an isomorphism.

Remark. There exists a bijective correspondence between:

(i) ideals of R, and

(ii) equivalence classes of pairs (S, f) where S is ring and $f : R \to S$ is a surjective ring homomorphism, where two pairs (S_1, f_1) and (S_2, f_2) are defined to be equivalent if there exists a ring isomorphism $\varphi : S_1 \to S_2$ such that $\varphi f_1 = f_2$.

6.3 Prime and Maximal Ideals

Definition 6.21. Let R be a ring, and let P be an ideal of R such that $P \neq R$. We say that P is *prime ideal* if $bc \in P$ implies either $b \in P$ or $c \in P$.

Lemma 6.22. Let R be a ring. Let $p \in R$ be an element, and let $P = (p)$ be the ideal generated by p. The following are equivalent:

(i) P is a prime ideal;

(ii) p is prime element.

Definition 6.23. Let R be a ring, and let M be an ideal of R such that $M \neq R$. We say that M is a *maximal ideal* if the only ideals J of R satisfying $M \subseteq J \subseteq R$ are $J = M$ and $J = R$.

Lemma 6.24. Let R be a ring, and let I be an ideal of R such that $I \neq R$.

(i) I is a prime ideal if and only if R/I is an integral domain;

(ii) I is a maximal ideal if and only if R/I is a field.

Lemma 6.25. Let R be a non-zero ring, and let $\{0_R\}$ denote the zero ideal of R.

(i) $\{0_R\}$ is a prime ideal if and only if R is an integral domain.

(ii) $\{0_R\}$ is a maximal ideal if and only if R is a field.

Lemma 6.26. In a ring R, every maximal ideal is a prime ideal.

Definition 6.27. Let R be a ring. The *dimension* of R, written $\dim(R)$ is the largest nonnegative integer d for which there exists a stricting increasing sequence

$$P_0 \subset P_1 \subset \cdots \subset P_{d-1} \subset P_d$$

of prime ideal of R. It is often convenient to defined the dimension of the zero ring to be $-\infty$.

Remark. As a converse to Lemma 6.26, we have $\dim(R) = 0$ if and only if every prime ideal of R is a maximal ideal.

7 Groups

7.1 Definition

Definition 7.1. A *group* is a set G equipped with a function

$$*_G : G \times G \to G$$

satisfying the following conditions:

(i) (associative) For all $g_1, g_2, g_3 \in G$,

$$(g_1 *_G g_2) *_G g_3 = g_1 *_G (g_2 *_G g_3).$$

(ii) (identity) There exists $e \in G$ such that

$$e_G *_G g = g *_G e_G = g$$

for all $g \in G$.

(iii) (inverse) For all $g \in G$, there exists $h \in G$ such that

$$g *_G h = h *_G g = e_G$$

in G.

The function $*_G$ is called the *group law* (or *law of composition*). We say that G is an *abelian group* if, in addition, $*_G$ satisfies

(iv) (commutative) For all $g_1, g_2 \in G$, we have

$$g_1 *_G g_2 = g_2 *_G g_1.$$

Remark. A goal in group theory is to classify/enumerate all groups of a given order (up to isomorphism).

Definition 7.2. If the set G (in definition 7.1) is finite, we say that G is a *finite group.* The number of elements in G is called the *order* and is denoted $|G|$. If G is not finite, it is called an *infinite group.*

7.2 Examples

Example 7.3. The *trivial group* (or *zero group*) contains just one element.

Example 7.4. Let X be a set. A *permutation* of X is a bijective function $\sigma : X \to X$. The *symmetric group* associated to X (denoted $S(X)$) is the set of all permutations of X, with the group law given by composition of functions, i.e., $\sigma *_{S(X)} \sigma_2 = \sigma_1 \cdot \sigma_2$. The identity $e_{S(X)}$ is the identity function $\mathrm{id}_X : X \to X$. If X is finite, then $|S(X)| = |X|!$. If X is infinite, then $S(X)$ is an uncountably infinite set.

Example 7.5. As a special case of example 7.4, let n be a positive integer; then the group of permutations of the set $X = 1, \ldots, n$ is called the *symmetric group* of degree n (denoted S_n). Since X contains n elements, we have $|S_n| = n!$ for all n.

Example 7.6. Let P_n be a regular n-gon, which we can view as the convex hull of the nth roots of unity $e^{\frac{2\pi i}{n}k}$ for $k = 0, 1, \ldots, n-1$. The group of symmetries of P_n is called the *dihedral group* of degree n (and denoted D_n). There are two symmetries that can generate all other symmetries of P: (i) rotatie by $2\pi/n$ radians, or (ii) reflect across the x-axis.

Example 7.7. For a (possibly noncommutative) ring R, we can view R as a group under the addition law. Since the addition law of a ring is always commutative, the group $(R, +_R)$ is an abelian group.

Example 7.8. For a (possibly noncommutative) ring R, the units of R, $R^\times$ is a group under the multiplication law $\cdot_R$ of R.

Example 7.9. For a commutative ring R with identity, the set of units of $\mathrm{Mat}_{n\times n}(R)$, i.e., the set of invertible $n \times n$ matrices with entries in R, is denoted

$$\mathrm{GL}_n(R) = (\mathrm{Mat}_{n\times n}(R))^\times,$$

and called the *general linear group of degree* n associated to R. If $n \geq 2$, then $\mathrm{GL}_n(R)$ is non-abelian.

Example 7.10. Given two groups $(G, *_G)$ and $(H, *_H)$, the Cartesian product

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

has a natural group law, given by

$$(g, h) *_{G \times H} (g', h') = (g *_G g', h \cdot_H h')$$

for all $g, g' \in G$ and $h, h' \in H$. More generally, for any collection of groups $G_1, \ldots, G_n$, the group law on the direct product $G = G_1 \times \cdots \times G_n$ is defined by

$$(g_1, \ldots, g_n) *_G (g_1', \ldots, g_n') = (g_1 *_{G_1} g_1', \ldots, g_n *_{G_n} g_n')$$

for all $g_i, g_i' \in G$. As a special case, for any group G and any positive integer n, we define G^n to be the n-fold direct product $G \times \cdots \times G$.

7.3 Properties

Lemma 7.11. Let G be a group.

(i) (uniqueness of identity) There exists only one element $e \in G$ satisfying (ii) in definition 7.1.

(ii) (uniqueness of inverse) For any $g \in G$, there exists only one element $h \in G$ satisfying (iii) in definition 7.1.

We denote the element of G satisfying (iii) in definition 7.1 by g^{-1}.

Lemma 7.12. Let G be a group and $g, h \in G$. We have

(i) $(gh)^{-1} = h^{-1}g^{-1}$;

(ii) $(g^{-1})^{-1} = g$.

We can generalize (i):

$$(g_1 g_2 \cdots g_n)^{-1} = g_n^{-1} \cdots g_2^{-1} g_1^{-1}$$

for any $g_1, \ldots, g_n \in G$.

Remark. Let G be a group and $g \in G$. If n is a positive integer, then

$$g^n = g \cdot g \cdots g \ (n \text{ factors}).$$

We also define $g^0 = e$ and

$$g^{-n} = g^{-1} \cdot g^{-1} \cdots g^{-1} \ (n \text{ factors}).$$

Lemma 7.13. Let G be a group and let $g \in G$. Then for all $m, n \in \mathbb{Z}$,

$$a^m a^n = a^{m+n} \qquad \text{and} \qquad (a^m)^n = a^{mn}.$$

Lemma 7.14. Let G be a group and $g_1, g_2, h \in G$ be elements.

(i) If $g_1 h = g_2 h$, then $g_1 = g_2$;

(ii) If $h g_1 = h g_2$, then $g_1 = g_2$.

Definition 7.15. Let G be a group and $g \in G$ be an element. If there exists a positive integer $n \in \mathbb{Z}_{\geq 1}$ such that $g^n = e$, then g is said to have *finite order*; the smallest n satisfying $g^n = e$ is called the *order* of g and is denoted $\mathrm{ord}(g)$. If g does not have finite order, we say that g has *infinite order*.

Lemma 7.16. Let G be a group and $g \in G$ be an element. If there exist distinct $i, j \in \mathbb{Z}$ such that $g^i = g^j$, then g has finite order.

Lemma 7.17. If G is a finite group, every element of G has finite order.

Lemma 7.18. Let G be a group and let $g \in G$ be an element of order $\operatorname{ord}(g) = n$.

(i) For an integer $k \in \mathbb{Z}$, we have $g^k = e \Leftrightarrow n \mid k$.

(ii) For any integers $i, j \in \mathbb{Z}$, we have $g^i = g^j \Leftrightarrow i \equiv j \pmod{n}$.

(iii) For any positive integer $t \in \mathbb{Z}_{\geq 1}$, we have $\operatorname{ord}(g^t) = n/\gcd(n, t)$.

Lemma 7.19. Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If $\gcd(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$, then $\operatorname{ord}(ab) = \operatorname{ord}(a) \cdot \operatorname{ord}(b)$.

Remark. If $ab \neq ba$, then it can happen that a and b have finite order, but ab has infinite order.

Lemma 7.20. Let G be an abelian group such that every element of G has finite order. If there exists an element $c \in G$ such that $\operatorname{ord}(g) \leq \operatorname{ord}(c)$ for all $g \in G$, then in fact $\operatorname{ord}(g) \mid \operatorname{ord}(c)$ for all $g \in G$.

Theorem 7.21. Let G and H be groups. Define an operation $*_{G\times H}$ by

$$(g, h) *_{G\times H} (g', h') = (g *_G g', h *_H h').$$

Then $G \times H$ is a group. If G and H are abelian, then so is $G \times H$. If G and H are finite, then so is $G \times H$ and $|G \times H| = |G||H|$.

7.4 Subgroups

Definition 7.22. Let G be a group and let $H \subset G$ be a subset. We say that H is a *subgroup* of G if is satisfies the following conditions:

(i) (identity) $e_G \in H$;

(ii) (closed under multiplication) If $h_1, h_2 \in H$, then $h_1 *_G h_2 \in H$;

(iii) (closed under inverse) If $h \in H$, then $h^{-1} \in H$.

Every subgroup H of G is itself a group, where the group law $*_H : H \times H \to H$ is inherited from, i.e., equal to, that of G.

Lemma 7.23. Let G be a group. Then the subset

$$Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$$

is a subgroup, called the *center* of G.

7.5 Homomorphisms

Definition 7.24. Let $(G, *_G)$ and $(H, *_H)$ be groups. A function $\varphi : G \to H$ is a *group homomorphism* if

$$\varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$$

for all $g_1, g_2 \in G$.

Example 7.25. If H is a subgroup of G, we have a group homomorphism $H \to G$ defined by $h \to h$.

Example 7.26. If G is an abelian group, then the nth power map $\mu_n : G \to G$ defined by $\mu_n(g) = g^n$ is a group homomorphism.

Lemma 7.27. Let $\varphi : G \to H$ be a group homomorphism.

(i) $\varphi(e_G) = e_H$;

(ii) For all $g \in G$, we have $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

Lemma 7.28. If $\varphi : G \to H$ and $\psi : H \to K$ are group homomorphisms, then the composition $\psi \circ \varphi : G \to K$ is a group homomorphism.

Lemma 7.29. Let $\varphi : G \to H$ be a group homomorphism.

(i) For any subgroup $G' \subseteq G$, the image

$$\varphi(G') = h \in H : h = \varphi(g') \text{ for some } g' \in G'$$

is a subgroup of H.

(ii) For any subgroup $H' \subseteq H$, the preimage

$$\varphi^{-1}(H') = \{g \in G : \varphi(g) \in H'\}$$

is a subgroup of G.

Lemma 7.30. Let $\varphi : G \to H$ be a group homomorphism.

(i) The image

$$\mathrm{im}\varphi = \varphi(G) = \{h \in H : h = \varphi(g) \text{ for some } g \in G\}$$

is a subgroup of H.

(ii) The kernel

$$\ker \varphi = \varphi^{-1}(e_H) = \{g \in G : \varphi(g) = e_H\}$$

is a subgroup of G.

Definition 7.31. A bijective group homomorphism is called an *isomorphism.* If $G = H$, then φ is an endomorphism of G; a bijective endomorphism is an *automorphism.* The set of automorphisms of a group is itself a group, denoted Aut(G).

Lemma 7.32. If $\varphi : G \to H$ is an isomorphism, then the inverse function $\varphi^{-1} : H \to G$ is also an isomorphism.

Theorem 7.33. Let G be a group. There exists an injective group homomorphism $G \to S(G)$.

7.6 Generators

Definition 7.34. Let G be a group, $g \in G$ be an element, and

$$\epsilon_g : \mathbb{Z} \to G$$

be the function defined by $\epsilon_g(n) = g^n$. Then ϵ_g is a group homomorphism because

$$\epsilon_g(n_1 + n_2) = g^{n_1+n_2} = g^{n_1} \cdot g^{n_2} = \epsilon_g(n_1) \cdot \epsilon_g(n_2)$$

for all $n_1, n_2 \in \mathbb{Z}$. By lemma 7.30, the image

$$\langle g \rangle = \mathrm{im}\, \epsilon_g = \{\dots, g^{-2}, g^{-1}, g_0, g_1, g_2, \dots\}$$

is a subgroup of G called the *cyclic subgroup* generated by g. We say that G is a *cyclic group* if $G = \langle g \rangle$ for some $g \in G$, i.e., every element of G is of the form g^n for some n, i.e., ϵ_g is surjective; in this case g is called a *generator* of G.

Lemma 7.35. Let G be a group, $H \subseteq G$ be a subgroup, and $g \in G$ be an element. Then $g \in H$ if and only if $\langle g \rangle \subseteq H$.

Lemma 7.36. If G is a cyclic group and $H \subseteq G$ is a subgroup, then H is cyclic.

Lemma 7.37. Let G be a group, and let $g \in G$ be an element. Then:

(i) g has finite order if and only if ϵ_g is not injective;

(ii) g has infinite order if and only if ϵ_g is injective.

Lemma 7.38. Let G be a group and let $g \in G$ be an element.

(i) If g has finite order, then $\langle g \rangle \cong \mathbb{Z}/(\mathrm{ord}(g))$.

(ii) If g has infinite order, then $\langle g \rangle \cong \mathbb{Z}$.

Lemma 7.39. Every cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/(n)$ for some n.

Lemma 7.40. If g has finite order, then $\langle g \rangle = \{g^0, g^1, \ldots, g^{\mathrm{ord}(g)-1}\}$, so in particular $|\langle g \rangle| = \mathrm{ord}(g)$.

Lemma 7.41. Let G be a finite group. Then G is cyclic if and only if there exists $g \in G$ with $\mathrm{ord}(g) = |G|$.

Lemma 7.42. If g has finite order, then g^k is a generator of $\langle g \rangle$ if and only if $\gcd(k, \mathrm{ord}(g)) = 1$.

Lemma 7.43. Let F be a field and let G be a finite subgroup of $F^\times$. Then G is cyclic.

Lemma 7.44. For any prime $p \in \mathbb{Z}$, the group of units $(\mathbb{Z}/(p))^\times$ is cyclic, i.e., there is an isomorphism

$$\mathbb{Z}/(p-1) \cong (\mathbb{Z}/(p))^\times$$

of groups.

Remark. In lemma 7.44, a generator of $(\mathbb{Z}/(p))^\times$ is called a *primitive root* $\mod p$ because it is a root of the polynomial $x^{p-1} - 1$ whose powers generate all other roots.

Lemma 7.45. Let G be a group and let $S \subset G$ be a subset. Let $\langle S \rangle$ be the set of all elements of G of the form $g = g_1 \cdots g_n$ where, for each i, either g_i or g_i^{-1} is contained in S (if $n = 0$, we define $g = e$). Then $\langle S \rangle$ is a subgroup of G.

Definition 7.46. In lemma 7.45, we call $\langle S \rangle$ the *subgroup generated by S*.

7.7 Symmetric, Alternating Groups

Definition 7.47. For a set X and any permutation $\sigma \in S(X)$, we define the *support* of σ to be the (possibly empty) subset

$$\mathrm{Supp}(\sigma) = \{x \in X : \sigma(x) \neq x\}$$

of X, i.e., the elements of X changed by σ.

Lemma 7.48. Let X be a set. For any permutation $\sigma \in S(X)$, we have

$$\sigma(\operatorname{Supp}(\sigma)) = \operatorname{Supp}(\sigma)$$
$$\sigma(X \setminus \operatorname{Supp}(\sigma)) = X \setminus \operatorname{Supp}(\sigma)$$

in X.

Definition 7.49. We say that two permutations $\sigma, \tau \in S(X)$ are *disjoint* if $\operatorname{Supp}(\sigma) \cap \mathrm{S}(\tau) = \emptyset$, i.e., their supports are disjoint, as subsets of X.

Lemma 7.50. Let X be a set and let $\sigma, \tau \in S(X)$.

(i) If σ, τ are disjoint, then for any $x \notin \operatorname{Supp}(\tau)$, we have $\sigma(\tau(x)) = \tau(\sigma(x)) = \sigma(x)$.

(ii) If σ, τ are disjoint, then $\sigma\tau = \tau\sigma$.

(iii) We have $\operatorname{Supp}(\sigma\tau) \subseteq \operatorname{Supp}(\sigma) \cup \operatorname{Supp}(\tau)$. If σ, τ are disjoint, then $\operatorname{Supp}(\sigma\tau) = \operatorname{Supp}(\sigma) \cup \operatorname{Supp}(\tau)$.

Definition 7.51. Let X be a set. We say that a permutation $\sigma \in S(X)$ is a *k-cycle* if there exists a k-element subset $T = \{a_1, \ldots, a_k\}$ of X such that

$$\sigma(a_1) = a_2, \ldots, \sigma(a_{k-1}) = a_k, \sigma_{a_k} = a_1$$

and $\sigma(x) = x$ if $x \notin T$; in this case, we denote $\sigma = (a_1 \cdots a_k)$; here k is the *length* of σ. Note that "0-cycles" and "1-cycles" are just the identity e. If $k = 2$, then σ is called a *transposition*, i.e., a 2-cycle.

Theorem 7.52. Let X be a finite set. For any $\sigma \in S(X)$, there exist pairwise disjoint cycles $\tau_1, \ldots, \tau_m \in S(X)$ (of possibly different lengths) such that $\sigma = \tau_1 \cdots \tau_m$ and $\operatorname{Supp}(\sigma) = \operatorname{Supp}(\tau_1) \cup \cdots \cup \operatorname{Supp}(\tau_m)$.

Lemma 7.53. If $\tau_1, \ldots, \tau_m \in S_n$ are pairwise disjoint, then

$$\operatorname{ord}(\tau_1 \cdots \tau_m) = \operatorname{lcm}(\operatorname{ord}(\tau_1), \ldots, \operatorname{ord}(\tau_m)).$$

Lemma 7.54. If $\sigma \in S(X)$ is a k-cycle (with $k \geq 2$) then $\operatorname{ord}(\sigma) = k$.

Theorem 7.55. If $\tau_1, \ldots, \tau_m$ are pairwise disjoint cycles of length $k_1, \ldots, k_m$, then

$$\operatorname{ord}(\tau_1 \cdots \tau_m) = \operatorname{lcm}(k_1, \ldots, k_m).$$

Lemma 7.56. For any $k \geq 2$ and $a_1, \ldots, a_k \in X$, we have

$$(a_1 \cdots a_k) = (a_1 a_2) \cdots (a_{k-1} a_k)$$

in $S(X)$.

Theorem 7.57. For any $\sigma \in S_n$, there exist transpositions $\tau_1, \ldots, \tau_m \in S_n$ such that $\sigma = \tau_1 \cdots \tau_m$, that is, every permutation is a product of transpositions.

Definition 7.58. For a permutation $\sigma \in S_n$, an *inversion* of σ is a pair of indices (i, j) satisfying $1 \leq i \leq j \leq n$ and $\sigma(i) > \sigma(j)$. We denote $\operatorname{inv}(\sigma)$ the number of inversions of σ. (Note that $0 \leq \operatorname{inv}(\sigma) \leq n(n-1)/2$ for all $\sigma \in S_n$.)

Lemma 7.59. Let $\sigma, \tau \in S_n$. If τ is a transposition, then $\operatorname{inv}(\tau\sigma) = \operatorname{inv}(\sigma) + 1 \pmod 2$.

Lemma 7.60. If $\tau_1, \ldots, \tau_m \in S_n$ are transpositions, then $\operatorname{inv}(\tau_1 \cdots \tau_m) \equiv m \pmod 2$.

Theorem 7.61. The function sgn : $S_n \to \{\pm 1\}$ defined by $\text{sgn}(\sigma) = (-1)^{\text{inv}(\sigma)}$ is a group homomorphism.

Definition 7.62. If $\text{sgn}(\sigma) = 1$, we say σ is an *even* permutation; if $\text{sgn}(\sigma) = -1$, we say that σ is an *odd* permutation. The *alternating group* of degree n (denoted A_n) is the set of even permutations in S_n, i.e. $A_n = \ker(\text{sgn})$.

8 Normal Subgroups and Quotient Groups

8.1 Cosets

Definition 8.1. Let G be a group, and let H be a subgroup of G. A subset of G is called the *left coset* of H if it is of the form $aH = \{ah : h \in H\}$ for some $a \in G$. The set of left cosets of H in G is denoted G/H. The *index* of H in G is the cardinality $[G : H] = |G/H|$, i.e., the number of distinct left cosets of H in G.

Lemma 8.2. Let G be a group, and let H be a subgroup of G. Every element of G is contained in a left coset of H.

Lemma 8.3. Let G be a group and let H be a subgroup of G. If a_1H, a_2H are two left cosets of H, then either $a_1H \cap a_2H = \emptyset$ of $a_1H = a_2H$.

Lemma 8.4. Let G be a group, and let H be a subgroup of G. Given elements $a, b \in G$, the following are equivalent:

(i) $aH = bH$;

(ii) $aH \cap bH = \emptyset$;

(iii) $a \in bH$;

(iv) $a = bh$ for some $h \in H$;

(v) $b^{-1}a \in H$.

Lemma 8.5. Let G be a group, and let H be a subgroup of G. If a_1H, a_2H are two left cosets of H, then $|a_1H| = |a_2H|$.

Theorem 8.6 (Lagrange's Theorem). Let G be a finite group, and let H be a subgroup of G. Then we have $|G| = |H| \cdot [G : H]$ in $\mathbb{Z}$.

Theorem 8.7. If G is a finite group and $g \in G$, then $\text{ord}(g)$ divides $|G|$.

Theorem 8.8. If p is a prime and $|G| = p$, then $G \cong \mathbb{Z}/(p)$.

Corollary 8.9. If $|G| = 4$, then $G \cong \mathbb{Z}/(4)$ or $G \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

Corollary 8.10. If $|G| = 6$, then $G \cong \mathbb{Z}/(6)$ or $G \cong S_3$.

8.2 Normal Subgroups

Lemma 8.11. Let G be a group, and let N be a subgroup of G. The following are equivalent:

(i) for all $g \in G$, we have $gNg^{-1} \subseteq N$;

(ii) for all $g \in G$, we have $gNg^{-1} = N$;

(iii) for all $g \in G$, we have $gN = Ng$.

Definition 8.12. If a subgroup $N \subseteq G$ satisfies the conditions in Lemma 8.11, then N is called a *normal subgroup* of G.

Lemma 8.13. Let G be a finite group, and let N be a subgroup, and suppose that $G/N = \{g_1N, \ldots, g_mN\}$. If $g_iNg_i^{-1} \subseteq N$ for all $i = 1, \ldots, m$, then N is normal in G.

Lemma 8.14. Let G be a group, and let N be a subgroup of G of index 2. Then N is normal in G.

Lemma 8.15. If G is an abelian group, then every subgroup of G is a normal subgroup of G.

Lemma 8.16. Let G be a group. Then any subgroup N of the center $Z(G)$ is a normal subgroup of G.

Lemma 8.17. Let $\varphi : G \to H$ be a group homomorphism. Let $N \subseteq H$ be a normal subgroup of H. Then the preimage $\varphi^{-1}(N)$ is a normal subgroup of G. In particular, $\ker\varphi = \varphi^{-1}(e_H)$ is a normal subgroup of G.

8.3 Quotient Groups

Lemma 8.18. Let G be a group, and let N be a normal subgroup of G. Then the operation $aN *_{G/N} bN = abN$ is well-defined, and G/N is a group under $*_{G/N}$. The function $\pi : G \to G/N$ defined by $\pi(g) = gN$ is a group homomorphism, called the *natural homomorphism*.

Lemma 8.19. If G is abelian, then G/N is abelian.

Lemma 8.20. Let G be a group such that $G/Z(G)$ is cyclic. Then G is abelian.

8.4 Isomorphism Theorems

Lemma 8.21. Let $\varphi : G \to H$ be a group homomorphism, and let N be a normal subgroup of G such that $N \subseteq \ker\varphi$. Let $\pi : G \to G/N$ be the natural homomorphism.

(i) There exists a unique group homomorphism $\overline{\varphi} : G/N \to H$ such that $\varphi = \overline{\varphi} \circ \pi$.

(ii) $N = \ker\varphi$ if and only if $\overline{\varphi}$ is injective.

(iii) φ is surjective if and only if $\overline{\varphi}$ is surjective.

Theorem 8.22 (1st Isomorphism Theorem). Let $\varphi : G \to H$ be a surjective group homomorphism. Then there exist a group isomorphism $\overline{\varphi} : G/\ker\varphi \to H$ satisfying $\varphi = \overline{\varphi}\pi$.

Theorem 8.23 (2nd Isomorphism Theorem). Let G be a group, and let H, N be subgroups of G. If N is normal in G, then HN is a subgroup of G and there exists and isomorphism

$$\overline{\varphi} : H/(H \cap N) \to HN/N$$

of quotient groups.

Lemma 8.24. Let $\varphi : G \to H$ be a surjective group homomorphism. Then there is a bijective correspondence between the subgroups of G containing $\ker\varphi$ and the subgroups of H. Moreover, if N is a subgroup of H, then N is normal in H if and only if $\varphi^{-1}(N)$ is normal in G.

Theorem 8.25 (3rd Isomorphism Theorem). Let G be a group, and let N be a normal subgroup of G.

(i) Every subgroup of G/N is of the form H/N for subgroup H of G such that $N \subseteq H$.

(ii) If $N \subseteq H$ and H is normal in G, then there exists an isomorphism

$$\varphi : (G/N)/(H/N) \to G/H$$

of quotient groups.

Definition 8.26. A group G is *simple* if it does not have any proper normal subgroups, i.e., normal subgroups N such that $\{e\} \subset N \subset G$.

Remark. Given a group G, we can take a proper normal subgroup G_1 and study the properties of G_1 and G/G_1. We may split G_1 and G/G_1 further, recursing until we get a tree of subgroup relations such that the "leaves" of the tree have no proper normal subgroups. We call the simple subgroups the *composition factors* of G.

Theorem 8.27. Every finite simple group is isomorphic to one of the following classes of groups:

(i) $\mathbb{Z}/(p)$ for some prime p,

(ii) A_n for some $n \neq 4$,

(iii) "groups of Lie type",

(iv) "sporadic groups",

(v) "Tits group".

Theorem 8.28. If G is a simple abelian group, then $G \cong \mathbb{Z}/(p)$ for some prime p.

8.5 Alternating Groups are Simple

Lemma 8.29. Let $\sigma \in S_n$ and let $(a_0 a_1 \cdots a_{k-1}) \in S_n$ be a k-cycle. Then

$$\sigma \cdot (a_0 a_1 \cdots a_{k-1}) \cdots \sigma^{-1} = (\sigma(a_0)\sigma(a_1) \cdots \sigma(a_{k-1}))$$

in S_n.

Theorem 8.30. For $n \neq 4$, the alternating group A_n is simple.

Theorem 8.31. For $n \geq 5$, the normal subgroups of S_n are $\{e\}, A_n, S_n$.

9 Topics in Group Theory

9.1 Direct Products

Remark. If $G = G_1 \times G_2$, then G has subgroups $G_1 \times \{e\}$, $\{e\} \times G_2$ isomorphic to G_1, G_2 respectively; these are normal subgroups. Moreover, every $g \in G$ is equal to a product $(g_1, e) \cdot (e, g_2)$ for a unique $(g_1, e) \in G_1 \times \{e\}$ and $(e, g_2) \in \{e\} \times G_2$. In fact, these properties are enough to show that G is a product.

Theorem 9.1. Let G be a group, and suppose there exist normal subgroups $N_1, \ldots, N_k$ such that the function $f : N_1 \times \cdots \times N_k \to G$ defined by $f((n_1, \ldots, n_k)) = n_1 \cdots n_k$ is bijective. Then f is an isomorphism.

9.2 Finite Abelian Groups

Definition 9.2. Let G be an abelian group. For a positive integer $n \in \mathbb{Z}_{\geq 1}$, we say that an element $a \in G$ is *n-torsion* if $na = 0$.

Lemma 9.3. Let G be an abelian group.

(i) If $a \in G$ is n-torsion, then $ma = n/\gcd(m,n)$ for any $m \in \mathbb{Z}$.

(ii) If $a_1 \in G$ is n_1-torsion and $a_2 \in G$ is n_2-torsion, then $a_1 + a_2$ is $\operatorname{lcm}(n_1, n_2)$-torsion.

Lemma 9.4. Let G be an abelian group. Let $m, n \in \mathbb{Z}$ be positive integers such that $\gcd(m,n) = 1$.

(i) If $a \in G$ is m-torsion and n-torsion, then $a = 0$.

(ii) If $a \in G$ is mn-torsion, then there exists $b, c \in G$ such that b is m-torsion, c is n-torsion, and $a = b + c$.

Definition 9.5. Let G be an abelian group. Given a prime p, we define

$$G(p) = \{a \in G : p^r a = 0 \text{ for some } r \geq 0\}.$$

Lemma 9.6. Let G be a finite abelian group of order $|G| = p_1^{e_1} \cdots p_r^{e_r}$. Then the function $f : G(p_1) \times \cdots \times G(p_r) \to G$ defined by $f((a_1, \ldots, a_r)) = a_1 + \cdots + a_r$ is an isomorphism.

Definition 9.7. We say that a group G is a *p-group* if every element of G has order p^r for some $r \geq 0$.

Lemma 9.8. Let G be a finite abelian p-group, and let $a \in G$ be an element of maximal order. Then there exists a subgroup $K \subseteq G$ such that $G \cong \langle a \rangle \times K$.

Lemma 9.9. Every finite abelian p-group is isomorphic to

$$\mathbb{Z}/(p^{m_1}) \times \cdots \times \mathbb{Z}/(p^{m_r})$$

for some $r \geq 0$ and positive integers $m_1 \geq \cdots \geq m_r$.

Lemma 9.10. Let G, H be abelian groups. Then $p(G \times H) \cong pG \times pH$.

Lemma 9.11. For any $m \geq 1$, we have an isomorphism $p(\mathbb{Z}/(p^m)) \cong \mathbb{Z}/(p^{m-1})$.

Lemma 9.12. Let G, H be abelian groups, and let $f : G \to H$ be a group homomorphism. For any prime p, we have $f(G(p)) \subseteq H(p)$.

Lemma 9.13. Let p, q be distinct primes. If G is abelian q-group, we have $G(p) = 0$.

Lemma 9.14. Let G, H be abelian groups. Then $(G \times H)(p) \cong G(p) \times H(p)$.

Theorem 9.15. Let G be a finite abelian group of order $n = p_1^{e_1} \cdots p_r^{e_r}$. Then there exist unique partitions $e_i = e_{i,1} + \cdots + e_{i,\lambda_i}$ such that

$$G \cong \prod_{i=1}^{r} \prod_{j=1}^{\lambda_i} \mathbb{Z}/(p_i^{e_{i,j}}).$$

Lemma 9.16. For any positive integer $n = p_1^{e_1} \cdots p_r^{e_r}$, the number of isomorphism classes of finite abelian groups of order n is

$$N(e_1) \cdots N(e_r)$$

where $N(e)$ denotes the number of partitions of e.

9.3 Group Actions

Definition 9.17. Let G be a group and let X be a set. A *group action* of G on X is a function $\rho : G \times X \to X$ satisfying the following:

(i) We have
$$\rho(g_1g_2, x) = \rho(g_1, \rho(g_2, x))$$
for all $g_1, g_2 \in G$ and $x \in X$.

(ii) We have
$$\rho(e, x) = x$$
for all $x \in X$.

If X is a set equipped with an action of G, we sometimes say that X is a *G-set*. If X_1, X_2 are two G-sets, a function $\varphi : X_1 \to X_2$ is called *G-equivariant* if $\varphi(gx_1) = g\varphi(x_1)$ for all $x_1 \in X_1$ and $g \in G$. We will also write "$g \cdot x$" or gx to mean $\rho(g, x)$. We will say g *fixes* x if $gx = x$.

Definition 9.18. For any set X, let
$$\mathcal{P}_k(X) = \{S \in \mathcal{P}(X) : |X| = k\}$$
be the set of subsets of X of size k. Note that we have
$$|\mathcal{P}_k(X)| = \binom{|X|}{k}$$
for any $0 \leq k \leq |X|$.

Definition 9.19. Given a group G and any $0 \leq k \leq |G|$, there are three natural actions on G on $\mathcal{P}_k(G)$:

(i) The function $\rho : G \times \mathcal{P}_k(G) \to \mathcal{P}_k(G)$ defined by
$$\rho(G, S) = gS = \{gs : s \in S\}$$
is called the *left multiplication action* on G on $\mathcal{P}_k(G)$. If S is a left coset of some subgroup H of order $|H| = k$, then so is gS.

(ii) The function $\rho : G \times \mathcal{P}_k(G) \to \mathcal{P}_k(G)$ defined by
$$\rho(G, S) = Sg^{-1} = \{sg^{-1} : s \in S\}$$
is called the *right multiplication action* on G on $\mathcal{P}_k(G)$. If S is a right coset of some subgroup H of order $|H| = k$, then so is Sg^{-1}.

(iii) The function $\rho : G \times \mathcal{P}_k(G) \to \mathcal{P}_k(G)$ defined by
$$\rho(G, S) = gSg^{-1} = \{gsg^{-1} : s \in S\}$$
is called the *conjugation action* of G on $\mathcal{P}_k(G)$. If S is a subgroup of G, then so is gSg^{-1}.

Remark. Let $\rho : G \times X \to X$ be an action G on X. Given an element $g \in G$, we can define a function $\alpha_g : X \to X$ by $\alpha_g(x) = gx$. Given $g_1, g_2 \in G$, we have
$$\alpha_{g_1}(\alpha_{g_2}(x)) = g_1(g_2(x)) = (g_1g_2)(x) = \alpha_{g_1g_2}(x),$$
so
$$\alpha_{g_1} \circ \alpha_{g_2} = \alpha_{g_1g_2}$$
in $S(X)$; since
$$\alpha_g \circ \alpha_{g^{-1}} = \alpha_{g^{-1}} \circ \alpha_g = \alpha_e = \mathrm{id}_X,$$
each α_g is a bijection, and moreover the function
$$\alpha : G \to S(X)$$

defined by $g \to \alpha_g$ is a group homomorphism.

Conversely, given a group homomorphism $\alpha : G \to S(X)$, we can construct an action of G on X defined by $\rho(g, x) = \alpha(g)(x)$ for all $g \in G$ and $x \in X$, and one can show that these constructions are inverse to ecah other, i.e., there is a bijective correspondence

$$\{\text{group actions } G \times X \to X\} \Longleftrightarrow \{\text{group homomorphism } G \to S(X)\}.$$

Definition 9.20. Let G be a group acting on X. For any $x \in X$, let $\epsilon_x : G \to X$ be the function defined by $\epsilon_x(g) = gx$. The *orbit* of x is the image

$$\text{orb}_G(x) = \epsilon_x(G) = \{x' \in X : x' = gx \text{ for some } g \in G\}.$$

The set of orbits of this action is denoted X/G. The *stabilizer* of x is the preimage

$$\text{stab}_G(x) = \epsilon_x^{-1}(x) = \{g \in G : gx = x\}.$$

The stabilizer of any $x \in X$ is a subgroup of G.

Lemma 9.21. Let G be a group acting on X. The stabilizer of any $x \in X$ is a subgroup of G.

Lemma 9.22. Let G be a group acting on X. Every element of X is in an orbit, and distinct orbits are either equal or disjoint. Thus X is a disjoint union of orbits

$$X = \bigcup_{\mathcal{O} \in X/G} \mathcal{O}$$

and

$$|X| = \sum_{\mathcal{O} \in X/G} |\mathcal{O}|$$

if X is finite.

Theorem 9.23 (The Orbit-Stabilizer Theorem). Let G be a group acting on X. For any $x \in X$, there exists a bijection

$$G/\text{stab}_G(x) \to \text{orb}_G(x)$$

of sets. In particular, we have

$$|G| = |\text{stab}_G(x)| \cdot |\text{orb}_G(x)|$$

if $|G|$ is finite.

Lemma 9.24 (Burnside's Lemma). Let G be a finite group acting on a finite set X. Then

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

where $X^g = \{x \in X : gx = x\}$ denotes the set of $x \in X$ fixed by g.

9.4 Sylow Theorems

Definition 9.25. For any action G on X, let

$$\text{Fix}_G(X) = \{x \in X : gx = x \text{ for all } g \in G\}$$

be the set of elements of X that are fixed by every $g \in G$. In other words, for any $x \in X$, we have

$$x \in \mathrm{Fix}_G(X) \quad \Leftrightarrow \quad \mathrm{stab}_G(x) = G \quad \Leftrightarrow \quad |\mathrm{orb}_G(x)| = 1$$

where the second equivalence is by Theorem 9.23. Thus we have an equality

$$\mathrm{Fix}_G(X) = \bigcup_{\mathcal{O} \in X/G, |\mathcal{O}|=1} \mathcal{O}$$

of subsets of X.

Lemma 9.26. Let p be a prime, and suppose G is a group of order $|G| = p^n$ acting on a finite set X. Then

$$|X| \equiv |\mathrm{Fix}_G(X)| \pmod{p}.$$

Theorem 9.27 (Cauchy's Theorem). Let G be a finite group. For any prime p dividing $|G|$, there exists an element $g \in G$ with $\mathrm{ord}(g) = p$.

Lemma 9.28. If G is a finite p-group, then $|G| = p^k$ for some k.

Definition 9.29. Let G be a group, let p be prime dividing $|G|$. Suppose $|G| = p^k n$ where $\gcd(p, n) = 1$. A subgroup H of G is called a *Sylow p-subgroup* of G if $|H| = p^k$. We denote by $\mathrm{Syl}_p(G) \subset \mathcal{P}_{p^k}(G)$ the set of Sylow p-subgroups of G.

Theorem 9.30 (Sylow's Theorem). Let G be a group, and let p be a prime dividing $|G|$, and say $|G| = p^k n$ where $\gcd(p, n) = 1$.

(i) For any $0 \leq i \leq k-1$ and any subgroup H with $|H| = p^i$, there exists a subgroup H' satisfying $|H'| = p^{i+1}$ and $H \subset H'$. In particular, $\mathrm{Syl}_p(G) \neq \emptyset$.

(ii) For any two $H_1, H_2 \in \mathrm{Syl}_p(G)$, there exists $g \in G$ such that $gH_2g^{-1} = H_1$.

(iii) Let $n_p = |\mathrm{Syl}_p(G)|$ denote the number of Sylow p-subgroups of G. Then n_p divides $|G|$ and $n_p \equiv 1 \pmod{p}$. Furthermore, for any Sylow p-subgroup H, we have $n_p = [G : N_G(H)]$.

Lemma 9.31. Let G be a finite group, and let p be a prime dividing $|G|$. Then $n_p = 1$ if and only if there is a normal Sylow p-subgroup.

9.5 Applications of Sylow Theorems

Lemma 9.32. If $|G| = 63$, then G is not simple.

Lemma 9.33. Let p, q be distinct primes and let G be a group of order $|G| = pq^s$ for some s. If $n_p = q^s$, then $n_q = 1$.

Lemma 9.34. If $|G| = 56$, then G is not simple.

Lemma 9.35. Let $|G| = pq$ for distinct primes p, q such that $p \nmid q-1$ and $q \nmid p-1$, then $G \cong \mathbb{Z}/(pq)$.

Lemma 9.36. Let $|G| = p^n$ for some prime p and $n \geq 1$, then the center $Z(G)$ is nontrivial.

Lemma 9.37. If $|G| = p^n$ for some prime p and $n \geq 2$, then G is not simple.

Lemma 9.38. If $|G| = p^2$ for some prime p, then G is abliean. Hence either $G \cong \mathbb{Z}/(p^2)$ or $G \cong \mathbb{Z}/(p) \times \mathbb{Z}/(p)$.

Lemma 9.39. If $|G| = p^2q$ for distinct primes p, q such that $q \not\equiv 1 \pmod p$ and $p^2 \not\equiv 1 \pmod q$, then either $G \cong \mathbb{Z}/(p^2q)$ or $G \cong \mathbb{Z}(p) \times \mathbb{Z}/(pq)$.

Lemma 9.40. If $|G| = p^2q$ for distinct primes p, q, then G is not simple.

10 Arithmetic in Integral Domains

10.1 Euclidean Domains

Definition 10.1. Let R be an integral domain. We say that R is a *Euclidean domain (ED)* if there exists a function

$$\delta : R \setminus \{0_R\} \to \mathbb{Z}_{\geq 0}$$

satisfying

(i) if $a, b \in \mathbb{R} \setminus \{0_R\}$ and $b \mid a$, then $\delta(b) \leq \delta(a)$;

(ii) if a, b and $b \neq 0_R$, then there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$.

The function δ is called a *Euclidean function* for R.

Remark. If δ is a Euclidean function of the integral domain R, then we can generate infinitely more Euclidean function on R as follows: let $\kappa : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ be any injective function which is order-preserving, i.e. if $n_1 < n_2$ then $\kappa(n_1) < \kappa(n_2)$. Then the composition

$$k \cdot \delta : R \setminus \{0_R\} \to \mathbb{Z}_{\geq 0}$$

is also a Euclidean function for R. In general, we prefer the "simplest" Euclidean function.

Lemma 10.2. For any commutative ring R has any elements $x_1, y_1, x_2, y_2, A \in R$, we have

$$(x_1^2 - Ay_1^2)(x_2^2 - Ay_2^2) = (x_1x_2 + Ay_1y_2)^2 - A(x_1y_2 + x_2y_1)^2$$

in R.

10.2 Principal Ideal Domains

Definition 10.3. Let R be an integral domain. We say that R is a *principal ideal domain (PID)* if every ideal of R is a principal ideal.

Theorem 10.4. If R is an ED, then R is a PID.

Lemma 10.5. Let R be a PID and $a \in R$ be a nonzero element. Then a is prime if and only if a is irreducible.

Lemma 10.6. Let R be a PID and P be a nonzero prime ideal of R. Then P is a maximal ideal.

10.3 Unique Factorization Domains

Definition 10.7. Let R be an integral domain. We say that R is a *unique factorization domain (UFD)* if:

(i) for every nonzero non-unit $a \in R$, there exist irreducible $p_1, \ldots, p_r \in R$ (with $r \geq 1$) such that $a = p_1 \cdots p_r$;

(ii) if $r, s \in \mathbb{Z}_{\geq 1}$ and $p_1, \ldots, p_r, q_1, \ldots, q_s \in R$ are irreducible elements such that

$$p_1 \cdots p_r = q_1 \cdots q_s$$

then $r = s$ and there exist a permutation σ of $\{1, \ldots, r\}$ such that $p_1, q_{\sigma(i)}$ are associates for all $i = 1, \ldots, r$.

Theorem 10.8. If R is a PID, then R is a UFD.

Lemma 10.9. Let R be a UFD and $a \in R$ be a nonzero element. Then a is prime if and only if a is irreducible.

Theorem 10.10. Let R be a Noetherian integral domain. The following are equivalent:
(i) R is a UFD;
(ii) every irreducible element of R is prime.

Theorem 10.11. If R is a UFD, then $R[x]$ is a UFD.

Definition 10.12. Let R be an integral domain. Let I_R be the set of (nonzero) principal ideals of R. Let P_R be the set of (nonzero) prime principal ideals of R. Let S_R be the set of functions $e : P_R \to \mathbb{Z}_{\geq 0}$ such that $e^{-1}(\mathbb{Z}_{\geq 1})$ is finite. Let $\varphi_R : S_R \to I_R$ be the function

$$e \to \prod_{P \in e^{-1}(\mathbb{Z}_{\geq 1})} P^{e(P)}.$$

Theorem 10.13. If R is a UFD, the map φ_R is a bijection.

Definition 10.14. Let R be an integral domain, and $a_1, \ldots, a_n \in R$ be elements. Let $\mathrm{CD}(a_1, \ldots, a_n)$ be the set of common divisors of $a_1, \ldots, a_n$. An element $g \in \mathrm{CD}(a_1, \ldots, a_n)$ is a *greatest common divisor (gcd)* of $a_1, \ldots, a_n$ if $d \mid g$ for all $d \in \mathrm{CD}(a_1, \ldots, a_n)$. The gcd may not exist in an arbitrary integral domain.

Lemma 10.15. Let R be an integral domain, and $a_1, \ldots, a_n \in R$ be elements, and suppose $g \in R$ is a gcd of $a_1, \ldots, a_n$. For any $g' \in R$, we have g' is a gcd of $a_1, \ldots, a_n$ if and only if g, g' are associates.

Remark. Each time we enlarge the class of rings under consideration, we give up on some property of the gcd:

Property	$\mathbb{Z}$	$F[x]$	ED	PID	UFD	integral domains
literally "greatest"	✓	×	×	×	×	×
unique	✓	✓	×	×	×	×
computable via Euclidean algorithm	✓	✓	✓	×	×	×
linear combination of $a_1, \ldots, a_n$	✓	✓	✓	✓	×	×
exists	✓	✓	✓	✓	✓	×

10.4 Quadratic Integer Rings

Lemma 10.16. Let $d \in \mathbb{Z}$ be an integer which is note a perfect square We define the ring

$$\mathbb{Z}[\sqrt{d}] = \{s + t\sqrt{d} : s, t\imath\mathbb{Z}\}.$$

There is a norm function

$$N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$$

defined

$$N(s+t\sqrt{d}) = (s+t\sqrt{d})(s-t\sqrt{d}) = s^2 - dt^2$$

for all $s, t \in \mathbb{Z}$. Given the norm function N,

(i) for all $a, b \in \mathbb{Z}[\sqrt{d}]$, $N(a \cdot b) = N(a) \cdot N(b)$;

(ii) $N(a) = 0$ if and only if $a = 0$;

(iii) $a \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $N(a) = \pm 1$.

Lemma 10.17. Let $\mathbb{Z}[\sqrt{d}]$ be the ring defined in Lemma 10.16. If $d > 0$ then there are infinitely many units in $\mathbb{Z}[\sqrt{d}]$, and if $d < 0$ then there are only finitely many units in $\mathbb{Z}[\sqrt{d}]$. In fact, if $d = -1$ then the units of $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{d}]$ are $\pm 1, \pm i$; if $d \leq -2$ then the units of $\mathbb{Z}[\sqrt{d}] = \pm 1$.

Lemma 10.18. Let $\mathbb{Z}[\sqrt{d}]$ be the ring defined in Lemma 10.16. If $a \in \mathbb{Z}[\sqrt{d}]$ is an element such that $N(a)$ is irreducible in $\mathbb{Z}$, then a is irreducible in $\mathbb{Z}[\sqrt{d}]$.

Lemma 10.19. In $\mathbb{Z}[\sqrt{d}]$, every nonunit is equal to a product of irreducible elements.

Lemma 10.20. If $p \in \mathbb{Z}[i]$ is an irreducible element, then p is an associate of exactly one of the following:

(i) a positive prime $r \in \mathbb{Z}$ such that $r \equiv 3 \pmod 4$;

(ii) $r + si$ where $r^2 + s^2$ is a prime of $\mathbb{Z}$.

10.5 Dedekind Domains

Definition 10.21. Let R be a ring and $S \subseteq R$ be a subring.

(i) An element $R \in R$ is said to be *integral* (or *algebraic*) if there exists a monic polynomial $f \in S[x]$ such that $f(r) = 0$.

(ii) The *integral closure* of S in R is the subset $\overline{S} \subseteq R$ consisting of elements of R that are integral over S.

(iii) We say that S is *integrally closed* in R if $S = \overline{S}$.

Theorem 10.22. Let R be a ring and $S \subseteq R$ be a subring. Let $\overline{S}$ be the integral closure of S in R.

(i) $\overline{S}$ is a subring of R;

(ii) $\overline{S}$ is integrally closed in R.

Definition 10.23. A ring R is called a *Dedekind domain* if:

(i) R is an integral domain;

(ii) R is Noetherian, i.e. every ideal of R is finitely generated;

(iii) R is integrally closed in its field of fractions;

(iv) $\dim(R) = 1$.

Theorem 10.24. Let K be a subfield of $\mathbb{C}$ such that K is finite-dimensional $\mathbb{Q}$-vector space, and let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K. Then $\mathcal{O}_K$ is a Dedekind domain.

Theorem 10.25. Let R be a Dedekind domain. Then R is a PID if and only if R is a UFD.

Definition 10.26. Let R be a ring, and let I_R be the set of nonzero ideal of R, and let P_R be the set of nonzero prime ideals of R, and let S_R be the set of functions $e : P_R \to \mathbb{Z}_{\geq 0}$ such that $e^{-1}(\mathbb{Z}_{\geq 1})$ is finite. Let

$\varphi_R : S_R \to I_R$ be the function defined by

$$\varphi_R(e) = \prod_{P \in e^{-1}(\mathbb{Z}_{\geq 1})} P^{e(P)}.$$

Theorem 10.27. If R is a Dedekind domain, then φ_R is a bijection.

10.6 Field of Fractions of Integer Domains

Definition 10.28. Let R be an integral domain. Let $S = R \times (R \setminus \{0_R\})$ and we declare that $(a, b) \sim (a', b')$ if $ab' = a'b$. In this case, $(a, b), (a', b') \in S$ are called *equivalent*. Check that this defines an equivalence relation on S. The set of equivalence classes of S is called $\mathrm{Frac}(R)$, called the *fraction field* of R. Let

$$[a, b] = \{(c, d) \in S : (a, b) \sim (c, d)\}$$

denote the equivalence class containing (a, b). The addition and multiplication on $\mathrm{Frac}(R)$ is defined by

$$[a, b] + [c, d] = [ad + bc, bd]$$
$$[a, b] \cdot [c, d] = [ac, bd]$$

for all $[a, b], [c, d] \in \mathrm{Frac}(R)$.

There is a function $\xi : R \to \mathrm{Frac}(R)$ defined by $r \to [r, 1_R]$ for all $r \in R$ that is an injective unital ring homomorphism. If R is a field, then it is an isomorphism. Thus, we may identify R with the set of elements of the form $[r, 1_R]$. Under this identififcation, we see that the element $[a, b] \in \mathrm{Frac}(R)$ does indeed behave like the fraction "a/b", in the sense that it is "an element which, multiplied by b, gives a", i.e., $[b, 1_R] \cdot [a, b] = [a, 1_R]$.

Lemma 10.29. Given an integral domain R, a field F, and an injective unital ring homomorphism $\varphi : R \to F$ there exists a field embedding $\varphi' : \mathrm{Frac}(R) \to F$ such that $\varphi = \varphi' \circ \xi$.

Remark. In general, suppose R is a commutative ring with identity. For any prime ideal P or R, we can construct the *residue field* of P as follows: construct the quotient R/P, which is an integral domain, then construct the fraction field $\mathrm{Frac}(R/P)$

11 Field Extensions

11.1 Field Extensions

Definition 11.1. If F is a subfield of a field K, we say that K is a *field extension* of F, denoted "K/F" or "$F \subset K$". A *field embedding* is a unital ring homomorphism $\varphi : F \to K$, where F and K are fields. Here φ is necessarily injective by Lemma 11.2, hence φ induces an isomorphism $F \cong \varphi(F)$, we often (implicitly) identify the field embedding $F \to K$ with the induced field extension $\varphi(F) \subset K$.

Lemma 11.2. Let F be a field, let R be any nonzero commutative ring with identity, and let $\varphi : F \to R$ be a unital ring homomorphism. Then φ is injective.

11.2 Simple Extensions

Definition 11.3. For any commutative ring R with identity, there is a unique (unital) ring homomorphism $\epsilon_R : \mathbb{Z} \to \mathbb{R}$, namely $n \to n \cdot 1_R$ (we usually abbreviate $n \cdot 1_R$ as "n"). By the First Isomorphism Theorem, there is an injective ring homomorphism $\mathbb{Z}/\ker \epsilon_R \to R$. If F is a field, then $\mathbb{Z}/\ker \epsilon_F$ is isomorphic to a subring of a field, so it is an integral domain, so $\ker \epsilon_F$ is a prime ideal of $\mathbb{Z}$. Thus $\ker \epsilon_F$ is of the form (ℓ) for some nonnegative integer $\ell \in \mathbb{Z}_{\geq 0}$ which is either 0 or a postive prime integer p; this unique nonnegative integer ℓ satisfying $\ker \epsilon_F = (\ell)$ is called the *characteristic* of F, denoted $\operatorname{char} F$.

Lemma 11.4. Let F be a field.

(i) If $\operatorname{char} F = 0$, then F is an extension of $\mathbb{Q}$.

(ii) If $\operatorname{char} F = p$, then F is an extension of $\mathbb{F}_p$.

Lemma 11.5. Let F, K be fields. If there exists a field embedding $\varphi : F \to K$, then $\operatorname{char} F = \operatorname{char} K$.

Remark. By the previous lemma, if F_1, F_2 are fields of different characteristic, then there is no field embedding $F_1 \to F_2$ or $F_2 \to F_1$.

Definition 11.6. The *degree* of the extension K/F is the dimension of K as an F-vector space, and it is denoted $[K : F] = \dim_F K$. If $[K : F]$ is finite, we say that K/F is a *finite extension.*

Lemma 11.7. Let K/F be a field extension. Then $[K : F] = 1$ if and only if $F = K$.

Lemma 11.8. Let $F \subseteq K \subseteq K$ be field extensions.

(i) If $\mathcal{V} = \{v_1, \ldots, v_n\}$ is an F-basis for L, then $\mathcal{U} = \{v_i w_j : 1 \leq 1 \leq n, 1 \leq j \leq m\}$ is an F-basis for L.

(ii) The extension $F \subset L$ is finite if and only if $F \subset K$ and $K \subset L$ are finite, in which case we have an equality

$$[L : F] = [L : K][K : F]$$

of degrees.

Definition 11.9. Let K/F be an extension, and let $S \subset K$ be a subset. The intersection of all subfields of K that contain F and S is denoted $F(S)$ and called the "field obtained by adjoining S of F".

Remark.

(i) We can write any finitely generated extension $F(u_1, \ldots, u_n)/F$ as a composition of simple extensions:

$$F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq \cdots \subset F(u_1, \ldots, u_{n-1}) \subseteq F(u_1, \ldots, u_n).$$

(ii) The inclusion $F \subseteq F(S)$ is an equality if and only if $S \subset F$.

Lemma 11.10. Let K/F be an extension, let $S, T \subset K$ be subsets. Then

$$F(S, T) = (F(S))(T)$$

as subfields of K. In particular, for any $u_1, \ldots, u_n \in K$, we have

$$F(u_1, \ldots, u_n) = ((F(u_1, \ldots, u_{n-1}))(u_n))$$

in K.

Lemma 11.11. Let R, S be commutative rings with identity, and let $\sigma : R \to S$ be a unital ring homomorphism. For any $u \in S$, there exists a unique ring homomorphism $\varphi_u : R[x] \to S$ satisfying $\varphi_u(x) = x$.

Definition 11.12. Let K/F be a field extension, and let $u \in K$ be an element. Let

$$\varphi_u : F[x] \to K$$

be the F-homomorphism sending $x \to u$.

(i) If φ_u is injective, we say that u is *transcendental* over F.

(ii) If φ_u is not injective, we say that u is *algebraic* over F.

Lemma 11.13. If u is transcendental over F, then there is a F-isomorphism $F(x) \cong F(u)$.

Definition 11.14. In Definition 11.12, suppose that u is algebraic over F. Since $F[x]$ is a PID, there exists a unique monic polynomial

$$m_{u,F} \in F[x]$$

such that

$$\ker \varphi_u = (m_{u,F})$$

as ideals of $F[x]$; this $m_{u,F}$ is called the *minimal polynomial* of u over F. The degree of $m_{u,F}$ is called the *degree* of u over F.

Lemma 11.15. Let K/F be a field extension, and let $u \in K$ be algebraic over F with minimal polynomial $m_{u,F} \in F[x]$. Set $n = \deg m_{u,F}$. Then

(i) There is an F-isomorphism $F[x]/(m_{u,F}) \cong F(u)$.

(ii) The set $\{1, u, \dots, u^{n-1}\}$ is an F-basis of $F(u)$.

(iii) We have $[F(u) : F] = n$.

Lemma 11.16. Let K/F be a field extension. If $f \in F[x]$ is a monic irreducible polynomial and $u \in K$ is a root of f in K, then $m_{u,F} = f$.

Remark. Given an extension K/F, we often want to compute the degree $[K : F]$. We can reduce to computing the degrees of simple extensions $F(u)/F$. We have $[F(u) : F] = \deg m_{u,F}$ so the task is equivalent to determining the minimal polynomial $m_{u,F}$. We do this in two steps:

(i) Find some monic polynomial $f \in F[x]$ such that $f(u) = 0$.

(ii) Prove that f is irreducible.

Lemma 11.17. Let $F_1 \subset F_2 \subset K$ be field extensions, and let $u \in K$ be algebraic over F_1. Then u is algebraic over F_2, and $m_{u,F_2} \mid m_{u,F_1}$ in $F_2[x]$. In particular, $\deg m_{u,F_2} \le \deg m_{u,F_1}$.

Lemma 11.18. Let K/F be an extension, and $u_1, \dots, u_n \in K$ be algebraic over F. Then an F-basis for $F(u_1, \dots, u_n)$ is

$$\{u_1^{e_1} \cdots u_n^{e_n} : 0 \le e_i \le d_i \text{ for } 1 \le i \le n\}$$

where we define $d_i = \deg m_{u_1,F(u_1,\dots,u_{i-1})}$ for all $1 \le i \le n$. Thus

$$[F(u_1, \dots, u_n) : F] = d_1 \cdots d_n$$

and $F(u_1, \dots, u_n)/F$ is a finite extension.

Remark. If we reorder the $u_1, \dots, u_n$, the F-basis that we get will in general be different; this is because the bound $d_i = \deg m_{u_1,\dots,u_{i-1}}$ depends on the fact that $u_1, \dots, u_{i-1}$ are adjoined before u_i.

Lemma 11.19. Let F be a field with char $F \neq 2$, and let $a, b \in F$ be elements such that a, b, ab are not square in F. For any extension, K/F containing $\sqrt{a}, \sqrt{b}, \sqrt{ab}$, the set $\{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$ is linearly independent over F, i.e., $[F(\sqrt{a}, \sqrt{b}) : F] = 4$.

11.3 Algebraic Extensions

Definition 11.20. Let K/F be a field extension. We say that K/F is an *algebraic extension* if every element of K is algebraic over F.

Lemma 11.21. If K/F is a finite extension, then it is an algebraic extension.

Lemma 11.22. Let K/F be a field extension, and let $F' \subset K$ be the set of elements of K that are algebraic over F. Then F' is a field extension of F.

Lemma 11.23. Let $F \subset K \subset L$ be field extensions. If $F \subset K$ and $K \subset L$ are algebraic, then $F \subset L$ is algebraic.

Remark. We say that an extension K/F is an *algebraic closure* of F if:

(i) K/F is an algebraically extension, and

(ii) K is algebraically closed (i.e. every nonconstant $f \in K[x]$ has a root in K).

For any field F, it is known that

(i) (existence) There exists an algebraic closure K/F of F.

(ii) (uniqueness) Given two algebraic closures K_1/F and K_2/F of F, there exist an F-isomorphism $K_1 \cong K_2$.

11.4 Splitting Fields

Definition 11.24. Let F be a field, $f \in F[x]$ be a monic polynomial, and K/F a field extension. We say that f splits over K if there exists elements $u_1, \ldots, u_n \in K$, not necessarily distinct, such that $f = (x - u_1) \cdots (x - u_n)$ in $K[x]$.

Lemma 11.25. Let F be a field, and let $(u_1, \ldots, u_n)$, $(u'_1, \ldots, u'_n) \in F^n$ be n-tuples of elements such that

$$(x - u_1) \cdots (x - u_n) = (x - u'_1) \cdots (x - u'_n)$$

in $F[x]$. Then there exists a permutation $\sigma \in S_n$ such that $(u_1, \ldots, u_n) = (s'_{\sigma(1)}, \ldots, u'_{\sigma(n)})$.

Lemma 11.26. Let F be a field, and let $f \in F[x]$ be a monic polynomial. Then there exists a field extension $F \subseteq E$ such that f splits over E.

Definition 11.27. Let F be a field, and let $f \in F[x]$ be a polynomial. A *splitting field* of f over F is an extension K/F such that

(i) f splits over K, and

(ii) if $F \subseteq L \subseteq K$ and f splits over L, then $L = K$.

Lemma 11.28. Let F be a field, and let $f \in F[x]$ be a monic polynomial, and suppose $F \subset E$ is any field etension such that f splits over E as $f = (x - u_1) \cdots (x - u_n)$ for some $u_1, \ldots, u_n \in E$.

(i) The extension $F(u_1, \ldots, u_n)/F$ is a splitting field for f over F.

(ii) We have $[F(u_1, \ldots, u_n) : F] \leq n!$.

Theorem 11.29. Let F be a field, and let $f \in F[x]$ be a polynomial. Then there exists an extension K/F which a splitting field for f over F.

Lemma 11.30. Let F be a field, $f \in F[x]$ be a polynomial, and let K/F be a splitting field of f over F. For any field F' such that $F \subseteq F' \subseteq K$, the extension K/F' is a splitting field of f over F'.

Lemma 11.31 (Isomorphism Extension Theorem). Let $\phi : F_1 \to F_2$ be an isomorphism of fields. For $i = 1, 2$, let K_1/F_i be a field extension, and let $u_i \in K_1$ be an element which is algebraic over F_i, with minimal polynomial $m_{u_i,F_i} \in F_i[x]$. If $\phi(m_{u_1,F_1}) = m_{u_2,F_2}$, there exists a unique isomorphism $\widetilde{\phi} : F_1(u_1) \to F_2(u_2)$ such that $\widetilde{\phi}(u_1) = u_2$ and $\widetilde{\phi}$ extends ϕ.

Theorem 11.32. (Splitting fields are unique) Let $\phi : F_1 \to F_2$ be an isomorphism of fields. For $i = 1, 2$, let $f_i \in F_i[x]$ be a polynomial, and let K_i/F_i be a splitting field of f_i over F_i. If $f_2 = \phi(f_1)$, then there exists an isomorphism $\phi' : K_1 \to K_2$ which extends ϕ.

Definition 11.33. An algebraic extension K/F is a *normal extension* if, for every $u \in K$, the minimal polynomial $m_{u,F} \in F[x]$ splits over K.

Theorem 11.34. Let K/F be a finite extension. The following are equivalent:

(i) The extension K/F is a splitting field for some polynomial $f \in F[x]$;

(ii) The extension K/F is a normal extension.

11.5 Separability

Definition 11.35. Let F be a field and let $f = \sum_{i=0} a_i x^i \in F[x]$ be a polynomial. The *derivative* of f is $f' = \sum_{i=1} i a_i x^{i-1} \in F[x]$.

Lemma 11.36. Let F be a field.

(i) Given $c \in F$ and $f \in F[x]$, we have $(cf)' = cf'$.

(ii) Given $f, g \in F[x]$, we have $(f + g)' = f' + g'$.

(iii) Given $f, g \in F[x]$, we have $(fg)' + f'g + fg'$.

Lemma 11.37. For F be a field. For a polynomial $f \in F[x]$ of degree n, the following are equivalent:

(i) $\gcd(f, f') = 1$

(ii) For all extensions K/F such that f splits over K, f has n distinct roots in K.

(iii) There exists an extension K/F such that f splits over K and f has n distinct roots in K.

Definition 11.38. Let F be a field. A polynomial $f \in F[x]$ is a *seprable polynomial* if the conditions of the previous lemma are satisfied; otherwise, f is *inseparable*. Let K/F be a field extension, and let $u \in K$ be algebraic over F. We say that u is a *separable element* over F if its minimal polynomial $m_{u,F} \in F[x]$ is a separable polynomial. An algebraic extension K/F is *separable extension* if every element $u \in K$ is separable over F.

Lemma 11.39. Let F be a field, and let $f \in F[x]$ be a monic irreducible polynomial. Then $f' \neq 0$ if and only if f is separable.

Lemma 11.40. Let F be a field of $\operatorname{char} F = 0$.

(i) Every irreducible polynomial $f \in F[x]$ is separable.

(ii) Every algebraic extension K/F is a separable extension.

Theorem 11.41 (Primitive Element Theorem). Let K/F be a finite separable extension. Then there exists some $u \in K$ such that $K = F(u)$.

11.6 Finite Fields

Lemma 11.42. Let F be a finite field. Then $\operatorname{char} F = p$ for some prime p (hence $\mathbb{F}_p \subseteq F$).

Lemma 11.43. Let F be a finite field. Then $|F| = p^n$ where $p = \operatorname{char} F$ and $n = [F : \mathbb{F}_p]$.

Lemma 11.44. Let F be a field of $\operatorname{char} F = p$. For any positive integer n, the subset

$$F = \{u \in F : u^{p^n} = u\}$$

is a subfield of F.

Lemma 11.45. Let p is a prime.

(i) The polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$ is separable.

(ii) If $m \mid n$, then $x^{p^m} - x \mid x^{p^n} - x$.

Theorem 11.46. Let F be a finite field and set $p = \operatorname{char} F$. The following are equivalent:

(i) We have $|F| = p^n$.

(ii) The extension $F/\mathbb{F}_p$ is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Theorem 11.47. Let P be a prime, and let n be a positive integer.

(i) There exists a field F of order p^n.

(ii) If F_1, F_2 are both fields of order p^n, then $F_1 \cong F_2$.

(iii) If F_1, F_2 are subfield of K of order p^n, then $F_1 = F_2$.

Definition 11.48. The field of order p^n is unique and denoted $\mathbb{F}_{p^n}$.

Lemma 11.49. We have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$.

Lemma 11.50. Let K be a field, and let $G \subseteq K^\times$ be a finite subgroup. Then G is cyclic.

Theorem 11.51 (Primitive Element Theorem for Finite Fields). Let K/F be an extension of finite fields. Then there exists some $u \in K$ such that $K = F(u)$.

Lemma 11.52. Let p be a prime. For any positive integer n, there exists a monic irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree $\deg f = n$.

Lemma 11.53. Let p be a prime. For any positive integer n, we have

$$x^{p^n} - x = \prod_{d \mid n, f \in M_d} f$$

in $\mathbb{F}_p[x]$, where "M_d" denotes the set of monic irreducible polynomials of degree d in $\mathbb{F}_p[x]$.

Lemma 11.54. Let K/F be an extension of finite fields. Then the extension K/F is normal and separable.

12 Galois Theory

12.1 Automorphism Groups

Definition 12.1. Let K be a field. The set of field automorphisms $\varphi : K \to K$ is denoted $\mathrm{Aut}(K)$; this is a group under composition called the *automorphism group*. Let K/F be a field extension. An automorphism $\varphi \in \mathrm{Aut}(K)$ is an F-automorphism if $\varphi(a) = a$ for all $a \in F$ (we also say that φ *fixes* F). The subset

$$\mathrm{Aut}(K/F) = \{\varphi \in \mathrm{Aut}(K) : \varphi(a) = a \text{ for all } a \in F\}$$

of F-automorphism of K is a subgroup of $\mathrm{Aut}(K)$.

Lemma 12.2. Let F be a field, and let $f \in F[x]$ be a polynomial.

(i) Let K/F be a field extension, and let $\varphi \in \mathrm{Aut}(K/F)$; if $u \in K$ is a root of f, then $\varphi(u) \in K$ is also a root of f.

(ii) Assume that f is monic irreducible over F and that K/F is the splitting field of f over F. If $u, v \in K$ are two roots of f, then there exists some $\varphi \in \mathrm{Aut}(K/F)$ such that $\varphi(u) = v$.

Lemma 12.3. Let K/F be a field extension, and let $S \subset K$ be a generating set for K/F (so that $K = F(S)$). If $\varphi_1, \varphi_2 \in \mathrm{Aut}(K/F)$ are two F-automorphisms such that $\varphi_1(s) = \varphi_2(s)$ for all $s \in S$, then $\varphi_1 = \varphi_2$.

Lemma 12.4. If K/F is a finite extension, then $\mathrm{Aut}(K/F)$ is a finite group.

Lemma 12.5. Let F be a field, $f \in F[x]$ be a polynomial, and K/F be a splitting field of f over F. If there are n distinct roots of f in K, there is an injective group homomorphism

$$\mathrm{Aut}(K/F) \to S_n$$

where S_n is the symmetric group of degree n. In particular, $|\mathrm{Aut}(K/F)| \leq n!$.

Lemma 12.6. Let F be a field, $f \in F[x]$ be a polynomial, and K/F be a splitting field of f over F. Then

(i) $|\mathrm{Aut}(K/F)| \leq [K : F]$;

(ii) if f is separable, then $|\mathrm{Aut}(K/F)| = [K : F]$.

12.2 Galois Theory

Definition 12.7. Let K be a field and $G \subseteq \mathrm{Aut}(K)$ be a subgroup. The set

$$K^G = \{a \in K : \varphi(a) = a \text{ for all } \varphi \in G\}$$

is a subfield of K, called the *fixed field* of G.

Remark. (Galois correspondence) For a field K, there are functions between the subgroups of $\mathrm{Aut}(K)$ and the subfields of K defined by

$$F(G) = K^G \qquad G(F) = \mathrm{Aut}(K/F)$$

for any subgroup $G \subseteq \mathrm{Aut}(K)$ and subfield $F \subseteq K$.

Lemma 12.8. Let K be a field.

(i) If $G_1 \subseteq G_2$ are two subgroups of $\mathrm{Aut}(K)$, then $K^{G_1} \supseteq K^{G_2}$.

(ii) If $F_1 \subseteq F_2$ are two subfields of K, then $\mathrm{Aut}(K/F_!) \supseteq \mathrm{Aut}(K/F_2)$.

Remark. Let K be a field. For a subfield F of K, we have an inclusion $F \subseteq K^{\mathrm{Aut}(K/F)}$ of subfields of K. For any subgroup G of $\mathrm{Aut}(K)$, we have an inclusion $G \subseteq \mathrm{Aut}(K/K^G)$ of subgroups of $\mathrm{Aut}(K)$.

Lemma 12.9. Let K be a field, and let $\varphi_1, \ldots, \varphi_n \in \mathrm{Aut}(K)$ be distinct automorphisms of K. Then $\{\varphi_1, \ldots, \varphi_n\}$ is linearly independent over K.

Theorem 12.10. Let K be a field, and let G be a finite subgroup of $\mathrm{Aut}(K)$.

(i) The extension K/K^G is a finite extension and its degree is $[K : K^G] = |G|$.

(ii) The extension K/K^G is separable and normal.

Lemma 12.11. For any finite extension K/F, we have

$$|\mathrm{Aut}(K/F)| \leq [K : F].$$

Lemma 12.12. If $G \subseteq \mathrm{Aut}(K)$ is a finite subgroup, then the inclusion $G \subseteq \mathrm{Aut}(K/K^G)$ is an equality.

Theorem 12.13 (Galois extension). Let K/F be a finite extension. The following are equivalent:

(i) The extension K/F is separable and normal.

(ii) The field K is the splitting field of a separable polynomial $f \in F[x]$.

(iii) The inequality $|\mathrm{Aut}(K/F)| \leq [K : F]$ is an equality.

(iv) The inclusion $F \subseteq K^{\mathrm{Aut}(K/F)}$ is an equality.

We say that K/F is a *Galois extension* if it satisfies the above conditions.

Theorem 12.14 (Fundamental Theorem of Galois Theory). Let K/F be a Galois extension.

(i) The correspondence between the subgroups of $\mathrm{Aut}(K/F)$ and the subfield of K containing F is bijective.

(ii) Under the correspondence in (i), a subgroup $G \subseteq \mathrm{Aut}(K/F)$ is a normal subgroup if and only if K^G/F is a normal extension.

(iii) If $F \subseteq E \subseteq K$ is an intermediate subfield such that E/F is normal, then there is an isomorphism

$$\mathrm{Aut}(K/F)/\mathrm{Aut}(K/E) \cong \mathrm{Aut}(E/F)$$

of groups.

Lemma 12.15. Let K be a field, and let $\varphi_1, \ldots, \varphi_n \in \mathrm{Aut}(K)$ be automorphisms and let $G = \langle \varphi_1, \ldots, \varphi_n \rangle \subseteq \mathrm{Aut}(K)$ be the subgroup generated by the φ_i. Then we have

$$K^G = \{a \in K : \varphi_i(a) = a \text{ for all } i = 1, \ldots, n\}$$

as subfields of K.

12.3 Solvability

Definition 12.16. Let K/F be a finite extension. We say that K/F is a *radical extension* if there is a sequence of fields

$$F_0 \subseteq \cdots \subseteq F_t$$

such that $F_0 = F$ and $F_t = K$ and for all $i = 1, \ldots, t$ there exists some $u_i \in F_i$ and $n_i \in \mathbb{Z}_{\geq 1}$ such that $u_i^{n_1} \in F_{i-1}$ and $F_i = F_{i-1}(u)$.

Lemma 12.17. If $F \subseteq F' \subseteq F''$ are field extensions such that F''/F' and F'/F are radical extensions, then F''/F is a radical extension.

Lemma 12.18. If K/F is a field extension such that $K = F(u_1, \dots, u_t)$ for some $u_1, \dots, u_t \in K$ and for all $1 \le i \le t$ there exists $n_i \in \mathbb{Z}$ such that $u_i^{n_i} \in F$, then K/F is radical.

Definition 12.19. Let $f \in F[x]$. We say that f is *solvable by radicals* if there exists a radical extension K/F such that f splits over K.

Definition 12.20. Let F be a field, and let n be a positive integer. An element $\zeta \in F$ is called an *nth root of unity* if $\zeta^n = 1_F$. Let

$$\mu_n(F) = \{\zeta \in F : \zeta^n = 1_F\}$$

be the set of all nth roots of unity in F; then $\mu_n(F)$ is a subgroup of $F^\times$ of order at most n (hence is cylic). We say that an nth root of unity $\zeta \in \mu_n(F)$ is *primitive* if $\operatorname{ord}(\zeta) = n$ as an element of the multiplicative group $F^\times$; equivalently, $|\mu_n(F)| = n$ and ζ is a generator of $\mu_n(F)$.

Lemma 12.21. Let F be a field, and let $n \in \mathbb{Z}_{\ge 1}$ be a positive integer.

(i) If $|\mu_n(F)| = n$, then $n \neq 0$ in F, i.e., either $\operatorname{char} F = 0$ or $\operatorname{char} F \nmid n$.

(ii) If $n \neq 0$ in F, then there exists an extension K/F such that $|\mu_n(K)| = n$.

Lemma 12.22. Let F be a field, and let K/F be an extension containing a primitive nth root of unity $\zeta \in K$. Then $F(\zeta)/F$ is a Galois radical extension, and $\operatorname{Aut}(F(\zeta)/F)$ is an abelian group.

Lemma 12.23. Let F be a field containing a primitive nth root of unity $\zeta \in F$, K/F be an extension, ad $u \in K$ be an element such that $u^n \in F$ for some $n \in \mathbb{Z}$. Then $F(u)/F$ is a Galois radical extension, and $\operatorname{Aut}(F(u)/F)$ is an abelian group.

Lemma 12.24. Let F be a field of $\operatorname{char} F = 0$, and let K/F be a radical extension. Then there exists an extension L/K such that L/F is a Galois radical extension.

Definition 12.25. A finite group G is said to be a *solvable group* if there is a sequence

$$G_0 \subseteq \cdots \subseteq G_n$$

of subgroups of G such that $G_0 = \{e\}$ and $G_n = G$ and for all $i = 1, \dots, n$, the group G_{i-1} is a normal subgroup of G_i and the quotient G_i/G_{i-1} is abelian.

Lemma 12.26. Let G be a solvable group.

(i) For any subgroup $H \subseteq G$, we have that H is a solvable group.

(ii) For any group homomorphism $f : G \to H$, we have that $f(G)$ is a solvable group.

Lemma 12.27. If G is a finite, simple, non-abelian group, then G is not solvable.

Lemma 12.28. For any $n \ge 5$, the symmetric group S_n is not solvable.

Theorem 12.29. Let F be a field of $\operatorname{char} F = 0$, and let K/F be a Galois radical extension. Then $\operatorname{Aut}(K/F)$ is a solvable group.

Definition 12.30. Let $f \in F[x]$ be a polynomial and K/F be a splitting field of f over F. The *Galois group* of f is the automorphism group $\operatorname{Aut}(K/F)$.

Theorem 12.31 (Galois' criterion). Let F be a field of $\operatorname{char} F = 0$, and let $f \in F[x]$ be a polynomial. The following are equivalent:

(i) f is solvable by radicals;

(ii) the Galois group of f is a solvable group.

Theorem 12.32. Let $n \geq 5$ and $f \in \mathbb{Q}[x]$ be a polynomial of $\deg f = n$. If the Galois group of f is S_n, then f is not solvable by radicals.

Lemma 12.33. Let G be a subgroup of S_n that contains a 2-cycle $(a_1 a_2)$ and an n-cycle $(a_1 a_2 \cdots a_n)$. Then $G = S_n$.

15 Geometric Constructions

Let $P = (x_P, y_P), Q = (x_Q, y_Q) \in \mathbb{R}^2$ be distinct points. Let

$$L(P, Q) = \{(x, y) \in \mathbb{R}^2 : (x - x_P)(y_Q - y_P) = (y - y_P)(x_Q - x_P)\}$$

denote the line passing through P and Q. Let

$$C(P, Q) = \{(x, y) \in \mathbb{R}^2 : (x - x_P)^2 + (y - y_P)^2 = (x_Q - x_P)^2 + (y_Q - y_P)^2\}$$

denote the circle whose center is P and passes through Q. We can use a straight edge to constrct $L(P, Q)$, and a compass to construct $C(P, Q)$.

Definition 15.1. We say that a point $P \in \mathbb{R}^2$ is a *constructible point* if there exists a finite sequence of points $P_0, P_1, \ldots, P_n \in \mathbb{R}^2$ such that $P_0 = (0, 0)$, $P = (1, 0)$, and $P_n = P$, such that for all $i \geq 2$, there exists indices $0 \leq i_1, i_2, i_3, i_4 \leq i - 1$ (not necessarily distinct) such that at least one of the following is true

(i) we have $P_i \in L(P_{i_1}, P_{i_2}) \cap L(P_{i_3}, P_{i_4})$ and $L(P_{i_1}, P_{i_2}) \neq L(P_{i_3}, P_{i_4})$, or

(ii) we have $P_i \in C(P_{i_1}, P_{i_2}) \cap C(P_{i_3}, P_{i_4})$ and $P_{i_1} \neq P_{i_3}$, or

(iii) we have $P_i \in L(P_{i_1}, P_{i_2}) \cap C(P_{i_3}, P_{i_4})$.

We say that $r \in \mathbb{R}$ is a constructible if $(r, 0) \in \mathbb{R}^2$ is a constructible point. The set of constructible numbers is denoted $\mathscr{C}$.

Lemma 15.2. Let $\mathscr{C} \in \mathbb{R}$ be the set of constructible numbers.

(i) A point $(x, y) \in \mathbb{R}^2$ is constructible if and only if $x, y \in \mathscr{C}$.

(ii) The set $\mathscr{C}$ is a subfield of $\mathbb{R}$ (hence contains $\mathscr{C}$).

(iii) If $r \in \mathbb{R}_{\geq 0}$ and $r \in \mathscr{C}$, then $\sqrt{r} \in \mathscr{C}$.

Lemma 15.3. Let $P_i \in (x_i, y_i) \in \mathbb{R}^2$ be points for $1 \leq i \leq 4$ such that $P_1 \neq P_2$ and $P_3 \neq P_4$; let F be a subfield of $\mathbb{R}$ containing $\{x_i, y_i\}_{1 \leq i \leq 4}$, and let $P = (x, y) \in \mathbb{R}^2$ be a point.

(i) If $P \in L(P_1, P_2) \cap L(P_3, P_4)$ and $L(P_1, P_2) \neq L(P_3, P_4)$, then $x, y \in F$.

(ii) If $P \in L(P_1, P_2) \cap C(P_3, P_4)$, then there exists some $u \in F$ such that $x, y \in F(\sqrt{u})$.

(iii) If $P \in C(P_1, P_2) \cap C(P_3, P_4)$ and $P_1 \neq P_3$, then there exists some $u \in F$ such that $x, y \in F(\sqrt{u})$.

In particular, the degree $[F(x, y) : F]$ is either 1 or 2.

Theorem 15.4. For a real number $r \in \mathbb{R}$, the following are equivalent:

(i) The number r is a constructible number.

(ii) There exists a sequence of extensions $F_0 \subseteq \cdots \subseteq F_\ell$ where $F_0 = \mathbb{Q}$ and $r \in F_\ell$ and $[F_i : F_{i-1}] = 2$ for all $1 \leq i \leq \ell$.

Lemma 15.5. If char $F \neq 2$ and K/F is an extension of degree $[K : F] = 2$, then $K = F(u)$ for some $u \in K$ such that $u^2 \in F$.

Lemma 15.6. If $P_1, P_2 \in \mathbb{R}^2$ are constructible points, then the distance $||P_1P_2||$ is a constructible number.