Chapter 1

Groups

1.1 Definitions and Examples

Definition 1.1.1. A ***group*** is a set G together with a binary operation $* : G \times G \to G$ which satisfies the following axioms:

(i) $(x * y) * z = x * (y * z)$ for all x, y, z in G,

(ii) $\exists\, e \in G$ such that $e * x = x = x * e$ for all x in G,

(iii) for each x in G, $\exists\, y \in G$ such that $y * x = e = x * y$.

Definition 1.1.2. Let G be a group. If G is finite, then the ***order*** of G, denoted $|G|$, is the number of elements of G. If G is infinite, G is said to have an ***infinite order***.

Definition 1.1.3. Let G be a group and $x \in G$. Then x is said to be of ***infinite order*** if there is no positive power of x equals the identity. If $x^n = e$ for some $n \in \mathbb{N}$, the smallest such n is called the ***order of x***, denoted $o(x)$.

Theorem 1.1.4. *Let G be a semigroup. Then TFAE:*

(i) *G is a group.*

(ii) *$\exists\, e \in G$ such that $ae = a$ for all $a \in G$; and for each $a \in G$ there is an $a' \in G$ such that $aa' = e$. (e and a' multiply on the right.)*

(iii) $\exists e \in G$ *such that* $ea = a$ *for all* $a \in G$*; and for each* $a \in G$ *there is an* $a' \in G$ *such that* $a'a = e$*. (*e *and* a' *multiply on the left.)*

Definition 1.1.5. A group G is ***abelian*** if $xy = yx$ for all $x, y \in G$. In this case, one can choose to write additively, that is:

(i) the binary operation is "+" ($x + y := x * y$), and

(ii) 0 is the unit element, and $-x$ denotes the inverse of x.

Definition 1.1.6. A nonempty subset H of a group G is called a ***subgroup*** of G if H is a group under the group operation inherited from G. If H is a subgroup of G, we write $H \leq G$.

Theorem 1.1.7. *Let* G *be a group and let* $\emptyset \neq H \subseteq G$*. Then TFAE:*

(i) H *is a subgroup of* G*.*

(ii) $a, b \in H \Rightarrow ab \in H$*, and* $a \in H \Rightarrow a^{-1} \in H$*.*

(iii) $a, b \in H \Rightarrow ab^{-1} \in H$*.*

1.2 Homomorphisms

Definition 1.2.1. Let $(G, \circ)$ and $(G', *)$ be groups. A mapping $\psi : G \to G'$ is called a ***homomorphism*** (of groups) if

$$\psi(a \circ b) = \psi(a) * \psi(b) \quad \text{for all } a, b \in G.$$

A homomorphism is called an ***isomorphism*** if it is bijective (1–1 and onto). G and G' are said to be ***isomorphic***, denoted $G \cong G'$, if there exists an isomorphism from G onto G'.

Definition 1.2.2. Let ψ be a homomorphism from G to G'. The ***kernel*** of ψ, $\ker \psi$, is defined to be

$$\ker \psi = \{g \in G \mid \psi(g) = e'\}$$

where e' is the identity of G'.

Theorem 1.2.3. *Let $\psi : G \to G'$ be a homomorphism. Then*

(i) $\psi(e) = e'$ *where e and e' are identities in G and G', respectively;*

(ii) $\psi(x^{-1}) = (\psi(x))^{-1}$ *for all $x \in G$;*

(iii) $\psi(x_1 x_2 \dots x_n) = \psi(x_1)\psi(x_2)\dots\psi(x_n)$ *for all $x_1, x_2, \dots, x_n \in G$;*

(iv) $\psi(x^n) = (\psi(x))^n$ *for all $n \in \mathbb{Z}$;*

(v) $\ker \psi$ *is a subgroup of G';*

(vi) $\ker \psi = \{e\}$ *if and only if ψ is 1-1;*

(vii) $\operatorname{Im} \psi$ *is a subgroup of G'.*

1.3 Cyclic Groups and Generators

Theorem 1.3.1. *Let G be a group and $a \in G$. Then $\{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and it is the smallest subgroup of G containing a.*

Definition 1.3.2. The subgroup $\{a^n \mid n \in \mathbb{Z}\}$ of a group G is called the ***cyclic subgroup*** of G ***generated by a*** and will be denoted by $\langle a \rangle$.

Definition 1.3.3. A group G is called a ***cyclic group*** if $G = \langle a \rangle$ for some $a \in G$. a is then called a ***generator*** of G and we say that a ***generates*** G.

Theorem 1.3.4. *Every cyclic group is abelian.*

Theorem 1.3.5. *A subgroup of cyclic group is cyclic.*

Theorem 1.3.6. *Let G be a cyclic group of order n generated by a. Let $b = a^s$ for some $s < n$. Then b generates a cyclic subgroup of G containing $\dfrac{n}{d}$ elements, where $d = \gcd(n, s)$.*

Corollary 1.3.7. *If a is a generator of a finite cyclic group G of order n, then the set of all generators of G is $\{a^r \mid \gcd(n, r) = 1\}$.*

Theorem 1.3.8. (i) $(\mathbb{Z}, +)$ is the only infinite cyclic group (up to isomorphism).

(ii) $(\mathbb{Z}_n, +)$ is the only cyclic group of order n (up to isomorphism).

Corollary 1.3.9. *The subgroups of* $(\mathbb{Z}, +)$ *are the groups* $n\mathbb{Z}$ *for* $n \in \mathbb{Z}$.

Definition 1.3.10. Let X be a nonempty subset of a group G. The smallest subgroup of G containing X, denoted $\langle X \rangle$, is called the ***subgroup of G generated by X***. We say that X ***generates*** $\langle X \rangle$.

If X is finite, say $X = \{x_1, x_2, \ldots, x_n\}$, we shall simply write $\langle x_1, x_2, \ldots, x_n \rangle$ for $\langle X \rangle$. If $\langle X \rangle = G$, we say that X is a set of ***generators*** of G. If X is finite and $\langle X \rangle = G$, then G is said to be ***finitely generated***.

Theorem 1.3.11. *Let* G *be a group and* $X \subseteq G$. *Then*

(i) $\langle \emptyset \rangle = \{e\}$,

(ii) $\langle X \rangle = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid x_i$ *are* n *distinct elements of* X, $\alpha_i \in \mathbb{Z}$ *and* $n \in \mathbb{N}\}$.

Moreover, if G *is finite, then* $\langle X \rangle$ *is the set of all products of elements of* X *(i.e. each* α_i *is a positive integer).*

Theorem 1.3.12. *A group* G *is isomorphic to* D_n *if and only if it is generated by two elements* a, b *such that* $a^n = 1 = b^2$ *and* $bab = a^{-1}$.

1.4 Group Actions

Definition 1.4.1. Let G be a group and X be a set. We say that the group G ***acts on*** the set X or X is a G***–set*** if there is a mapping $G \times X \to X$, $(g, x) \mapsto g \cdot x$ (or gx), which satisfies

(i) $1 \cdot x = x$ for all $x \in X$, where 1 is the identity element of G; and

(ii) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and all $x \in X$.

Definition 1.4.2. Let G act on X. If $g = 1$ is the only element of G which fulfills the identity $g \cdot x = x$ for all $x \in X$, then we say that G ***acts faithfully*** on X.

For each $x \in X$, $G \cdot x = \{g \cdot x \mid g \in G\}$ is called the ***orbit*** of x and is also denoted by $\text{orb}(x)$. If $G \cdot x = X$ for some $x \in X$, then G is said to ***act transitively*** on X. For each $Y \subseteq X$, the set $\{g \in G \mid g \cdot Y = Y\}$ is called the ***stabilizer*** of Y, denoted $\text{Stab}(Y)$, or $\text{Stab}(x)$ in case $Y = \{x\}$.

Theorem 1.4.3. *Let G act on X. Then for each $g \in G$ the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = g \cdot x$ is a permutation of X. Furthermore, the map $\phi : G \to S(X)$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $(\phi(g))(x) = g \cdot x$. The homomorphism ϕ is called the **permutation representation** associated to the given action. The kernel of this homomorphism is the set $\{g \in G \mid g \cdot x = x \ \ \forall x \in X\}$.*

Theorem 1.4.4 (Cayley's Theorem). *Every group is isomorphic to a subgroup of a permutation group. If a group is of order n, then it is isomorphic to a subgroup of S_n.*

Theorem 1.4.5. *Let G be a group. Suppose that G acts on a set X. Define a relation $\sim$ on X by*

$$x \sim y \ \text{ if and only if } \ y = g \cdot x \text{ for some } g \in G.$$

Then

(i) *$\sim$ is an equivalence relation on X, and*

(ii) *the **orbit** of $x \in X$, $G \cdot x$, is its equivalence class w.r.t. the relation $\sim$.*

Thus X is the disjoint union of all distinct orbits under the action of G.

Definition 1.4.6. If $H \leq G$ and $x \in G$, $Hx = \{hx \mid h \in H\}$ is called a ***right coset*** of H in G, and $xH = \{xh \mid h \in H\}$ is called a ***left coset*** of H in G.

Definition 1.4.7. Let H be a subgroup of a group G. Then the number of disjoint right (or left) cosets of H in G is called the ***index*** of H in G, denoted $[G : H]$. (i.e. $[G : H] = |\Lambda|$ where Λ is the index set of $\{x_\alpha \mid \alpha \in \Lambda\}$, the right transversal of H in G.)

Theorem 1.4.8 (Lagrange's Theorem). *Let G be a finite group and $H \leq G$. Then $|H|$ divides $|G|$. In particular $o(g)\big||G|$ for all $g \in G$.*

Corollary 1.4.9. *Let G be a finite group and $H \leq G$. Then*

$$|G| = [G : H]\,|H|.$$

Theorem 1.4.10. *Let G be a group which acts on a set X and $x \in X$. Then* $\mathrm{Stab}(x)$*, the stabilizer of $\{x\}$, is a subgroup of G, and*

$$[G : \mathrm{Stab}(x)] = |G \cdot x|.$$

Theorem 1.4.11 (The Orbit-Stabilizer Theorem). *Let G be a finite group which acts on a set X. Then for each $x \in X$,*

$$|G| = |G \cdot x| \cdot |\mathrm{Stab}(x)|.$$

Definition 1.4.12. Let G be a group and A be a nonempty subset of G. The ***centralizer*** of A in G, $C_G(A)$, and the ***normalizer*** of A in G, $N_G(A)$, are defined as follows:

$$\begin{aligned} C_G(A) &= \{g \in G \mid gag^{-1} = a \ \text{ for all } \ a \in A\}, \\ N_G(A) &= \{g \in G \mid gAg^{-1} = A\}, \end{aligned}$$

In particular, $Z(G) = C_G(G)$ is called the ***center*** of G

Theorem 1.4.13. *Let G be a group and $\emptyset \neq A \subseteq G$. Then $C_G(A)$ and $N_G(A)$ are subgroups of G. Moreover $C_G(A)$ is a subgroup of $N_G(A)$.*

Theorem 1.4.14. *Let G be a finite group and $x \in G$. Then the number of conjugates of x is $[G : C_G(x)]$. In particular, the number of conjugates of x divides the group order.*

Theorem 1.4.15 (The Class Equation). *Let G be a finite group. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)]$$

where $x_1, x_2, \ldots, x_t$ are representatives from all orbits of size greater than one.

Theorem 1.4.16. *Let G be a finite group and $Y \subseteq G$. Then the number of conjugates of Y is $[G : N_G(Y)]$. In particular, the number of conjugates of Y divides the group order.*

Theorem 1.4.17 (Cauchy' s Theorem). *If G is a finite group and p is a prime divisor of $|G|$, then the number of solutions of $g^p = 1$ in G is a multiple of p. Hence G contains an element of order p.*

Theorem 1.4.18 (Burnside' s Theorem). *Let G be a finite group acting on a finite set X. For each $g \in G$, let*

$$\tau(g) = \text{ the number of points in } X \text{ fixed by } g.$$

Then the number of orbits in X is

$$N = \frac{1}{|G|} \sum_{g \in G} \tau(g).$$

1.5 Quotient Groups and Isomorphism Theorems

Definition 1.5.1. Let N be a subgroup of a group G. Then N is said to be a ***normal subgroup*** of G, and write $N \lhd G$, if $gNg^{-1} \subseteq N$ for all $g \in G$.

Theorem 1.5.2. *Let N be a subgroup of a group G. Then TFAE:*

(i) *N is a normal subgroup of G.*

(ii) $gNg^{-1} = N$ *for all $g \in G$.*

(iii) $gN = Ng$ *for all $g \in G$.*

(iv) $(Na)(Nb) = Nab$ *for all $a, b \in G$.*

(v) $(aN)(bN) = abN$ *for all $a, b \in G$.*

Theorem 1.5.3. *Let N be a normal subgroup of a group G. Then $G/N = \{Na \mid a \in G\}$ is a group under the multiplication defined by*

$$Na \cdot Nb = Nab, \qquad (a, b \in G).$$

*The group G/N is called the **quotient group** or the **factor group** of G by N.*

The map $\theta : G \to G/N$ defined by $\theta(a) = Na$ is a group homomorphism whose kernel is N.

Definition 1.5.4. Let $G \xrightarrow{\theta} H \xrightarrow{\phi} K$ be a sequence of group homomorphisms. We say that it is ***exact*** at H if $\operatorname{Im}\theta = \ker\phi$. A ***short exact sequence*** of groups is a sequence of group homomorphisms

$$1 \longrightarrow G \xrightarrow{\theta} H \xrightarrow{\phi} K \longrightarrow 1\,,$$

which is exact at G, H and K.

Theorem 1.5.5 (The First Isomorphism Theorem). *If $\phi : G \to H$ is a group homomorphism, then $\ker\phi$ is a normal subgroup of G and $G/\ker\phi \cong \operatorname{Im}\phi$.*

Theorem 1.5.6. *If H and K are finite subgroups of a group, $|HK| = \dfrac{|H||K|}{|H \cap K|}$.*

Theorem 1.5.7. *If H and K are subgroups of a group G, then HK is a subgroup if and only if $HK = KH$.*

Corollary 1.5.8. *If H and K are subgroups of a group G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if K is normal in G, then HK is a subgroup of G for any subgroup H of G.*

Theorem 1.5.9 (The Second Isomorphism Theorem). *Let H and N be subgroups of a group G with N normal. Then $H \cap N$ is normal in H and $H\big/(H \cap N) \cong HN/N$.*

Theorem 1.5.10 (The Third Isomorphism Theorem). *Let N be a normal subgroup of a group G. Then the map $H \mapsto H/N$ gives a 1-1 correspondence between the set of subgroups of G containing N and the set of subgroups of G/N. Moreover this correspondence carries normal subgroups to normal subgroups. If $H \triangleleft G$, and $N \subseteq H \subseteq G$, then*

$$G/H \cong (G/N)\big/(H/N).$$

1.6 Direct Products and Abelian Groups

Definition 1.6.1. Let $\{A_\alpha \mid \alpha \in \Lambda\}$ be a family of groups. The set $\prod_{\alpha\in\Lambda} A_\alpha$ is a group under the coordinatewise operation. It is called the (***strong***) ***direct product*** of the groups A_α. The subgroup $\{(a_\alpha) \in \prod_{\alpha\in\Lambda} A_\alpha \mid \text{all but finitely many } a_\alpha = 1_\alpha\}$ is called the ***weak direct product*** (***or direct sum***) of the groups A_α, and is denoted $\bigoplus\{A_\alpha \mid \alpha \in \Lambda\}$ or $\sum_{\alpha\in\Lambda} A_\alpha$.

Theorem 1.6.2. *If A and B are subgroups of G such that*

(i) $A \cap B = \{e\}$,

(ii) $AB = G$, *and*

(iii) $ab = ba \quad \forall\, a \in A\ \forall\, b \in B$,

then $G \cong A \times B$. We say that G is the ***(internal) direct product*** *of A and B. Note that the condition (iii) can be replaced by that A and B are normal subgroups of G.*

Theorem 1.6.3 (Chinese Remainder Theorem). *Let $m_1, \ldots, m_k$, $n_1, \ldots, n_k$ be integers. If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime, then there exists an integer n such that*

$$n \equiv n_i \mod m_i \quad \text{for all } i = 1, \ldots, k.$$

Theorem 1.6.4. *Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime integers and $m = m_1 m_2 \cdots m_k$. If g is an element in G satisfying $g^m = 1$, then there exist unique $g_1, g_2, \ldots, g_k \in G$ such that*

(i) $g_i^{m_i} = 1 \quad$ *for all $i = 1, 2, \ldots, k$,*

(ii) $g_1, g_2, \ldots, g_k$ *are pairwise commutative, and*

(iii) $g = g_1 g_2 \ldots g_k$.

Definition 1.6.5. Let g be an element of a group G. If g has order $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where p_i's are distinct primes, then p_i is called the $\boldsymbol{p_i-primary\ part}$ of g.

Theorem 1.6.6. *Let A be a finite abelian group of order $m = m_1 m_2 \dots m_k$ where the m_i's are pairwise relatively prime. Let $A_i = \{g \in A \mid g^{m_i} = 1\}$. Then $A \cong A_1 \times A_2 \times \cdots \times A_k$. Moreover $|A_i| = m_i$.*

Theorem 1.6.7. *Let A be an abelian group of order p^α, where p is a prime. If A has exponent p (i.e. $a^p = 1$ for all $a \in A$), then*

$$A \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{\alpha \text{ times}} = (\mathbb{Z}_p)^\alpha.$$

Definition 1.6.8. A group G is called a ***p-group***, where p is a prime, if every element of G has the order as a (finite) power of p.

Definition 1.6.9. A positive integer n is said to be an ***exponent*** of a group G, if $g^n = 1$ for each $g \in G$. In this case G is said to have ***finite exponent***, and the least such positive integer n is called ***the exponent*** of G.

Theorem 1.6.10 (Burnside Basis Theorem for Abelian p-Group). *Let A be an abelian group of exponent p^α where p is a prime. If H is a subgroup of A and $HA^p = A$, then $H = A$. (Equivalence: If the cosets $A^p a_1, \dots, A^p a_k$ of A/A^p generate A/A^p, then $a_1, a_2, \dots, a_k$ generate A.)*

Theorem 1.6.11. *If A is a finite abelian group of exponent p, where p is a prime, then for any $H \leq A$, there exists a subgroup K of A such that $A \cong H \times K$. (Equivalence: If V is a finite dimensional vector space over $\mathbb{Z}_p$ and U is a subspace of V, then there is a subspace W of V such that $V = U \oplus W$.)*

Theorem 1.6.12. *Every finite abelian $p-$group is a direct product of cyclic groups.*

Theorem 1.6.13. *Let $A = (\mathbb{Z}_p)^{u_1} \times (\mathbb{Z}_{p^2})^{u_2} \times \ldots \times (\mathbb{Z}_{p^m})^{u_m}$, and*

$$B = (\mathbb{Z}_p)^{v_1} \times (\mathbb{Z}_{p^2})^{v_2} \times \ldots \times (\mathbb{Z}_{p^m})^{v_m} \text{ where } u_i \geq 0, v_j \geq 0.$$

If $A \cong B$, then $u_i = v_i$ for all $i = 1, 2, \dots, m$.

Definition 1.6.14. A ***partition of a positive integer*** n is a sequence $\{a_1, a_2, \ldots, a_k\}$ of positive integers where $a_{i+1} \geq a_i$ and $a_1 + a_2 + \ldots + a_k = n$. The number of partition of n is denoted $\Pi(n)$.

Theorem 1.6.15. *Let p be a prime and n a positive integer. Then*

$$\{\alpha_1, \alpha_2, \ldots, \alpha_k\} \ \mapsto \ \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p^{\alpha_k}}$$

defines a 1-1 correspondence between partitions of n and isomorphism classes of abelian groups of order p^n. In particular, the number of isomorphism classes of abelian groups of order p^n is $\Pi(n)$.

Theorem 1.6.16. *A finite abelian group is (isomorphic to) a direct product of cyclic group.*

Theorem 1.6.17. *Let A be a finite abelian group. Then there exist integers $n_1, \ldots, n_t > 1$ such that $n_1 \mid n_2,\ n_2 \mid n_3, \ldots,\ n_{t-1} \mid n_t$ and*

$$A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_t}.$$

Moreover, the integers are uniquely defined by A; more preciely if $m_1, \ldots, m_s$ are integers > 1 such that $m_1 \mid m_2,\ m_2 \mid m_3, \ldots,\ m_{s-1} \mid m_s$, and $A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_s}$, then $t = s$, and $n_1 = m_1, \ldots, n_t = m_t$.

1.7 The Sylow Theorem and Applications

Definition 1.7.1. Let G be a finite group of order $p_1^{a_1} \cdots p_k^{a_k}$ where p_i's are distinct primes. A subgroup of G of order $p_i^{a_i}$ is called a ***Sylow p_i-subgroup*** of G.

Theorem 1.7.2 (The second proof of Cauchy's Theorem). *If G is finite and $p \,\big|\, |G|$ is a positive prime number, then G has an element of order p.*

Theorem 1.7.3. *Let P be a sylow p-subgroup of G, Q a p-subgroup of G. If $Q \subseteq N_G(P)$, then $Q \leq P$.*

Theorem 1.7.4 (The Sylow Theorem). *Let G be a group of order $p^\alpha m$ where p is a prime, $\alpha > 0$, and $p \nmid m$. Then*

(i) *G contains a Sylow p-subgroup.*

(ii) *The number of Sylow p-subgroups is $\equiv 1 \mod p$.*

(iii) *If H is a p-subgroup of G and P is a Sylow $p-$subgroup of G, then some conjugate of P contains H. In particular,*

(iv) *All Sylow p-subgroups of G are conjugated.*

Corollary 1.7.5. *The number of Sylow p-subgroup of G divides $|G|$. (In particular it divides m if $|G| = p^\alpha m,\ p \nmid m$).*

Corollary 1.7.6. *Let G be a finite group and S a Sylow p-subgroup of G. Then S is the only Sylow p-subgroup of G if and only if $S \lhd G$.*

Theorem 1.7.7. *Let $n = p^\alpha m$ where p is a prime and $p \nmid m$. Then $\binom{n}{p^\alpha} \equiv m \mod p$.*

Theorem 1.7.8 (Combinatorial Proof of The Sylow's Theorem). *Let $|G| = p^a m$, where p is a prime and $p \nmid m$. Then G has a subgroup of order p^a.*

Theorem 1.7.9. *Let G be a finite group and P a Sylow p-subgroup of G. Then*

(i) *$N(P)$ is equal to its own normalizer, i.e. $N(N(P)) = N(P)$.*

(ii) *If $N(P) \leq T \leq G$, then T is equal to its own normalizer, i.e. $N(T) = T$.*

Theorem 1.7.10. *Let G be a group and $|G| = p^\alpha m$ where p is a prime and $p \nmid m$. Then G has a subgroup of order p^β for each β where $1 \leq \beta \leq \alpha$. Moreover, every subgroup H of G of order p^β is normal in a subgroup of order $p^{\beta+1}$ for $1 \leq \beta \leq \alpha$.*

Definition 1.7.11. An automorphism of a group G is an isomorphism $\phi : G \to G$. The set of all automorphism of a group G is denoted $\mathrm{Aut}(G)$.

Theorem 1.7.12. (i) *With group operation the composition of functions, $\mathrm{Aut}(G)$ is a group.*

(ii) *Each $g \in G$ determines an automorphism on G, $\phi_g : G \to G$ defined by $\phi(g)(h) = ghg^{-1}$. ϕ_g is called an* ***inner automorphism****. The subgroup of* $\mathrm{Aut}(G)$ *consisting of all such ϕ_g, $\{\phi_g \mid g \in G\}$ is called the* ***inner automorphism group*** *of G and is denoted* $\mathrm{Inn}\,(G)$.

(iii) *The map $g \mapsto \phi_g$ is a group homomorphism $G \xrightarrow{\phi}$* $\mathrm{Aut}(G)$.

(iv) *The kernel of ϕ is $Z(G)$, i.e. the center of G. The image of ϕ is* $\mathrm{Inn}\,(G)$.

Definition 1.7.13. A subgroup H of a group G is a ***characteristic subgroup*** if $\phi(H) = H$ for each $\phi \in \mathrm{Aut}(G)$.

Definition 1.7.14. A group is ***simple*** if it has no nontrivial normal subgroups.

Chapter 2

Rings

2.1 Basic Definitions and Examples

Definition 2.1.1. A ***ring*** R is a set with two binary operations, called addition "$+$" and multiplication "$\cdot$", satisfying the following axioms:

(i) $(R, +)$ is an abelian group, (0 denotes the neutral element),

(ii) $(R, \cdot)$ is a semigroup, and

(iii) $\forall\, a, b, c \in R, \quad a(b+c) = ab + ac$ and $(b+c)a = ba + ca$.

Definition 2.1.2. A ring R is said to be a ***ring with identity*** if there is $1 \in R$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$. A ring R is ***commutative*** if $xy = yx$ for all x, y in R.

Definition 2.1.3. Let R be a ring and $x \in R \setminus \{0\}$. x is called a ***left*** (***right***) ***zero divisor*** if there is an element $y \neq 0$ in R such that $xy = 0$ ($yx = 0$). x is called a ***zero divisor*** if x is either a left or a right zero divisor.

Definition 2.1.4. A ring R with identity is ***entire*** if R has no zero divisor. A commutative entire ring is called an ***integral domain***.

Definition 2.1.5. Let R be a ring with identity. An element x in R is said to be ***invertible*** if there exists $y \in R$ such that $xy = yx = 1$. In this case y is called the ***inverse*** of x.

Definition 2.1.6. A ring D with identity is a ***division ring*** (or ***skew field***) if every nonzero element in D is invertible.

Definition 2.1.7. A commutative division ring is called a ***field***.

Theorem 2.1.8. *Every field is an integral domain.*

Theorem 2.1.9. *Every finite integral domain is a field.*

Definition 2.1.10. A subset $S \subseteq R$ is a ***subring*** of a ring R if S is a ring with respect to $+$ and $\cdot$ in R.

Theorem 2.1.11. *Let S be a nonempty subset of a ring R. Then S is a subring of R if and only if $a - b$ and $ab \in S$ for all $a, b \in S$.*

2.2 Ring Homomorphisms and Quotient Rings.

Definition 2.2.1. Let R and S be rings. $\phi : R \to S$ is called a (***ring***) ***homomorphism*** if

$$\phi(x + y) = \phi(x) + \phi(y) \quad \text{and} \quad \phi(xy) = \phi(x)\phi(y) \quad \forall\, x, y \in R.$$

The ***kernel of*** ϕ, denoted $\ker \phi$ is the set $\{x \in R \mid \phi(x) = 0\}$. An ***isomorphism*** is a bijective homomorphism.

Definition 2.2.2. Let A be a subring of a ring R. Then A is called a ***left*** (***right***) ***ideal*** of R if $RA \subseteq A$ ($AR \subseteq A$). A is an ***ideal*** of R if A is both a left and right ideal of R.

Theorem 2.2.3. *Let R be a ring and I an ideal of R. Then R/I is a ring under the operations*

$$\begin{aligned}(r + I) + (s + I) &= (r + s) + I \\ (r + I)(s + I) &= rs + I.\end{aligned}$$

It is called the ***quotient*** (or ***factor***) *ring of R by I.*

The map $\psi : R \to R/I$ defined by $\psi(r) = r + I$ is a ring homomorphism which is surjective and has the kernel I. ψ is called the ***canonical*** (or ***natural***) *projection of R onto R/I.*

Theorem 2.2.4. *Let $\varphi : R \to S$ be a ring homomorphism. Then*

(i) $\operatorname{Im}\varphi$ *is a subring of* S,

(ii) $\ker\varphi$ *is an ideal of* R, *and*

(iii) $R/\ker\varphi \cong \operatorname{Im}\ \varphi$.

Theorem 2.2.5 (The Second Isomorphism Theorem). *Let S be a subring of R and let I be an ideal of R. Then*

(i) $S + I$ *is a subring of* R,

(ii) $S \cap I$ *is an ideal of* S, *and*

(iii) $(S + I)/I \cong S/(S \cap I)$.

Theorem 2.2.6 (The Third Isomorphism Theorem). *Let I be an ideal of R and A be an ideal of R containing I. Then A/I is an ideal of R/I and $(R/I)/(A/I) \cong R/A$.*

Theorem 2.2.7. *Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R containing I and the set of subrings of R/I. Furthermore, a subring A containing I is an ideal of R if and only if A/I is an ideal of R/I.*

Theorem 2.2.8. *A ring R with 1 is a division ring if and only if 0 and R are the only left (right) ideals of R.*

Corollary 2.2.9. *Let R be a commutative ring with 1. Then R is a field if and only if its only ideals are 0 and R.*

Corollary 2.2.10. *If R is a field then any nonzero ring homomorphism from R into another ring is an injection.*

2.3 Properties of Ideals.

From now on R is a ring ***with identity*** $1 \neq 0$.

Definition 2.3.1. Let A be a nonempty subset of a ring R. The ***ideal generated*** by A, denoted (A) is the smallest ideal of R containing A. An ideal generated by a single element set, $\{a\}$, is called a ***principal ideal***, it will be denoted (a).

If $A = \{a_1, a_2, \ldots, a_n\}$, the ideal generate by A is called a ***finitely generated ideal*** and denoted $(a_1, a_2, \ldots, a_n)$.

$$RA = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_i \in R, a_i \in A, n \in \mathbb{N}\}$$

is the left ideal generated by A.

$$AR = \{a_1r_1 + a_2r_2 + \ldots + a_nr_n \mid r_i \in R, a_i \in A, n \in \mathbb{N}\}$$

is the right ideal generated by A.

$$RAR = \{r_1a_1s_1 + r_2a_2s_2 + \ldots + r_na_ns_n \mid r_i, s_i \in R, a_i \in A, n \in \mathbb{N}\}$$

is the ideal generated by A.

Definition 2.3.2. An ideal M of a ring R is called a ***maximal ideal*** if $M \neq R$ and the only ideals containing M are M and R.

Theorem 2.3.3. *Every proper ideal in a ring with identity* $1 \neq 0$ *is contained in a maximal ideal.*

Theorem 2.3.4. *Let R be a commutative ring and M an ideal of R. Then M is an maximal ideal if and only if R/M is a field.*

Definition 2.3.5. Let R be a ring and P an ideal of R with $P \neq R$. P is called a ***prime ideal*** if whenever A and B are ideals of R and $AB \subseteq P$, then $A \subseteq P$ or $B \subseteq P$. If, in addition, R is commutative, then this notion becomes the notion of prime in $\mathbb{Z}$.

Lemma 2.3.6. *An ideal P of a ring R is prime if and only if for any a and b in R, $aRb \subseteq P$ implies $a \in P$ or $b \in P$.*

Theorem 2.3.7. *Let R be a commutative ring and P an ideal of R with $P \neq R$. Then P is prime if and only if $ab \in P$ implies $a \in P$ or $b \in P$ for any $a, b \in R$.*

Theorem 2.3.8. *Let P be an ideal of a commutative ring R. Then P is a prime ideal if and only if R/P is an integral domain.*

Corollary 2.3.9. *Every maximal ideal of a commutative ring is a prime ideal.*

Definition 2.3.10. Let R be a commutative ring with 1 and $x,\ y \in R$. We say that x ***divides*** y, denoted $x \mid y$ if there exists $q \in R$ such that $y = xq$ (i.e. $Ry \subseteq Rx$ or $(y) \subseteq (x)$).

Definition 2.3.11. Let R be an integral domain and $a, b \in R$. We say that a and b are ***associated*** if $a \mid b$ and $b \mid a$.

Theorem 2.3.12. *Let R be an integral domain, $a, b \in R$. Then TFAE:*

(i) *a and b are associated,*

(ii) *$Ra = Rb$, and*

(iii) *$a = ub$ for some $u \in U(R)$.*

Definition 2.3.13. Let R be an integral domain and $a, b \in R$. A ***greatest common divisor*** of a and b is an element d which satisfies:

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

(ii) if $d_1 \mid a$ and $d_1 \mid b$, then $d_1 \mid d$.

A ***least common multiple*** of a and b is an element m which satisfies:

(i) $a \mid m$ and $b \mid m$, and

(ii) if $a \mid m_1$ and $b \mid m_1$, then $m \mid m_1$.

Theorem 2.3.14. *Let R be an integral domain and $a, b \in R$.*

(i) *If d and d_1 are* gcd*'s of a and b, then d and d_1 are associated.*

(ii) *If m and m_1 are* lcm*'s of a and b, then m and m_1 are associated.*

Theorem 2.3.15. *Let R be an integral domain. If $Ra + Rb = Rc$, then $c = \gcd(a, b)$.*

Definition 2.3.16. Let R be an integral domain. A nonzero element p is called a ***prime*** in R if Rp is a prime ideal.

Definition 2.3.17. Let R be an integral domain. An element a in R is called an ***irreducible element*** (atom) if

(i) $a \neq 0$ and $a \notin U(R)$, and

(ii) a cannot be expressed as a product $a = bc$ where $b \notin U(R), c \notin U(R)$.

Theorem 2.3.18. *Every prime element in an integral domain is irreducible.*

2.4 Euclidean Domains

Definition 2.4.1. A function $\mathcal{N} : R \to \mathbb{N} \cup \{0\} = \mathbb{N}_0$ is called a ***norm*** on an integral domain R if $\mathcal{N}(0) = 0$.
A norm $\mathcal{N}$ is said to be ***multiplicative*** if it satisfies the following conditions:

(i) $\mathcal{N}(a) = 0$ if and only if $a = 0$.

(ii) $\mathcal{N}(ab) = \mathcal{N}(a)\mathcal{N}(b)$ for all $a, b \in R$.

Proposition 2.4.2. *Let R be an integral domain with a multiplicative norm $\mathcal{N}$ on R. Then*

(i) $\mathcal{N}(u) = 1$ *for every unit u in R.*

(ii) *If in addition $\mathcal{N}$ has a property that every x such that $\mathcal{N}(x) = 1$ is a unit in R, then an element π in R, with $\mathcal{N}(\pi) = p$ for some prime p in $\mathbb{Z}$, is an irreducible element of R.*

Definition 2.4.3. Let R be an integral domain. R is said to be a ***Euclidean Domain*** if there is a function $\mathcal{N}$ from $R \setminus \{0\}$ to $\mathbb{N}$ satisfying

(i) $\mathcal{N}(ab) \geq \mathcal{N}(a)$ for all nonzero elements a and b in R.

(ii) If $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = bq + r$ with $r = 0$ or $r \neq 0$ and $\mathcal{N}(r) < \mathcal{N}(b)$.

Proposition 2.4.4. *Let R be a Euclidean Domain with norm $\mathcal{N}$. Then*

(i) *$\mathcal{N}(1)$ is minimal among $\mathcal{N}(a)$ for all nonzero $a \in R$.*

(ii) *$U(R) = \{u \in R \mid \mathcal{N}(u) = 1\}$.*

Theorem 2.4.5. *$\mathbb{Z}[i]$ is a Euclidean Domain.(with respect to the norm $\mathcal{N}(a + bi) = a^2 + b^2$.)*

Theorem 2.4.6. *Every ideal of a Euclidean domain is a principal ideal.*

Theorem 2.4.7 (Euclidean Algorithm). *Let R be a Euclidean domain and let a and b be elements in R. Then*

$$Ra + Rb = Rc$$

for some $c \in R$. Furthermore, c can be explicitly constructed and $\gcd(a, b) = c$ so $\gcd(a, b)$ always exists.

2.5 Principal Ideal Domains

Definition 2.5.1. A ***Principal Ideal Domain*** **(PID)** is an integral domain in which every ideal is principal.

Theorem 2.5.2. *Every nonzero prime ideal in a PID is a maximal ideal.*

Theorem 2.5.3. *In a PID, (p) is a maximal ideal if and only if p is irreducible.*

Corollary 2.5.4. *Let R be a PID and $p \in R$. Then p is irreducible if and only if (p) is a prime ideal.*

Theorem 2.5.5. *In a PID, a nonzero element is a prime if and only if it is irreducible.*

Theorem 2.5.6 (ACC for ideals in a PID). *Let D be a PID. If $I_1 \subseteq I_2 \subseteq \ldots$ is a monotonic ascending chain of ideals, then there exists r such that $I_s = I_r$ for all $s \geq r$. (Ascending chain condition (ACC) holds for ideals in a PID.)*

Theorem 2.5.7. *Every Euclidean Domain is a PID.*

2.6 Unique factorization Domains

Definition 2.6.1. A ***Unique Factorization Domain*(UFD)** is an integral domain R in which every nonzero nonunit element $a \in R$ has the following factorization property:

(i) a is a (finite) product of irreducible elements of R, and

(ii) the decomposition of (i) is unique up to associates, namely if $a = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$ where p_i, q_i are irreducible, then $m = n$ and there is a reordering $q_{i_1}, \ldots, q_{i_m}$ of $q_1, \ldots, q_m$ such that p_j and q_{i_j} are associated.

Theorem 2.6.2. *Let R be an integral domain. Then R is a UFD if and only if*

(i) *Every nonzero nonunit element of R is a product of irreducible elements.*

(ii) *Every irreducible element is a prime.*

Definition 2.6.3. Let R be an integral domain. Define an equivalence relation on the set of irreducible elements of R by

$$a \sim b \iff a \text{ and } b \text{ are associated.}$$

Then a ***set of representative irreducible elements*** of R is a set which contains exactly one irreducible elements from each equivalence class.

Theorem 2.6.4. *Let R be an integral domain and P be a set of representative irreducible element of R. Then TFAE:*

(i) *R is a UFD.*

(ii) *Every nonzero nonunit element of R can be expressed uniquely (up to ordering) as $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where u is a unit $k \geq 0, \alpha_1, \cdots, \alpha_k > 0$ and $p_1, \ldots, p_k$ are distinct elements of P.*

Theorem 2.6.5. *Let R be a UFD and $a, b \in R$. Then*

(i) *a and b have a gcd.*

(ii) *a and b have an lcm.*

(iii) *If P is a set of representative irreducible elements for R, then among the gcd of a and b, there is exactly one which is a product of elements of P. The same is true for lcm.*

(iv) *If a and b are nonzero, $\gcd(a, b) = d$ and $\operatorname{lcm}(a, b) = m$ then ab and dm are associated.*

Theorem 2.6.6. *Every PID is a UFD. In particular, every Euclidean domain is a UFD.*

2.7 Fields of Fractions

Theorem 2.7.1. *Let R be an integral domain. Define a relation $\sim$ on $S = R \times (R \setminus \{0\})$ by*

$$(r_1, s_1) \sim (r_2, s_2) \Longleftrightarrow r_1 s_2 = r_2 s_1.$$

Then

(i) *$\sim$ is an equivalence relation on S.*

(ii) *$Q(R) = S/\sim$ is a field under the following addition and multiplication:*

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

(iii) *$Q(R)$ is the smallest field containing R in the sense that any field containing an isomorphic copy of R in which all nonzero elements of R are units must contain an isomorphic copy of $Q(R)$.*

Definition 2.7.2. The field in Theorem 2.7.1 is called ***the field of fractions*** or ***quotient field*** of R.

2.8 Polynomial Rings

Definition 2.8.1. The ***polynomial ring*** $R[x]$ in the indeterminate x with coefficient from R is the set of formal sums of the form

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

where $n \geq 0, a_0, \ldots, a_n \in R$ with $a_n \neq 0$. The integer n is called the ***degree*** of f. The degree of "0" is defined to be $-\infty$. The polynomial f is called monic if $a_n = 1$.

Define the addition and the multiplication on $R[x]$ as follows:

$$(\sum_{i=0}^{n} a_i x^i) + (\sum_{i=0}^{n} b_i x^i) = \sum_{i=0}^{n} (a_i + b_i)x^i$$
$$(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{n} b_i x^i) = \sum_{k=0}^{m+n} (\sum_{i=0}^{k} a_i b_{k-i})x^k,$$

where some leading terms a_i or b_j are allowed to be zero.

Then $R[x]$ is a ring with identity 1. If R is commutative then so is $R[x]$. Note that R can be considered as a subring of $R[x]$.

Theorem 2.8.2. *Let R be an integral domain (entire ring) and $f(x), g(x) \in R[x]$. Then*

(i) $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$ *(note that the hypothesis that R is an integral domain is unnecessary).*

(ii) $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

(iii) $U(R[x]) = U(R)$.

(iv) $R[x]$ *is an integral domain. (entire ring).*

Theorem 2.8.3. *Let R be a commutative ring with 1 and $i : R \to R[x]$ the inclusion map. Let S be a commutative ring with 1 and $\phi : R \to S$ a ring homomorphism. Then there exists a unique homomorphism $\hat{\phi} : R[x] \to S$ such that $\hat{\phi}(x) = a$ where $a \in S$ and $\phi = \hat{\phi} \circ i$. In particular, if $R = S$, then $\hat{\phi} : R[x] \to R$ is given by $\hat{\phi}(f(x)) = f(a)$ and $\ker \hat{\phi} = R[x](x - a)$, the ideal of $R[x]$ generated by $x - a$.*

Definition 2.8.4. The polynomial ring in the variables $x_1, x_2, \ldots, x_n$ with coefficients in R is denoted by $R[x_1, \ldots, x_n]$ and defined inductively by $R[x_1, x_2, \ldots, x_{n-1}][x_n]$.

Theorem 2.8.5 (Division Algorithm). *Let R be a ring with 1 (not necessary commutative). Let $f(x)$ be a **monic** polynomial of degree n in $R[x]$. Then for any $g(x) \in R[x]$, there exist unique polynomials $q(x)$ and $r(x)$ in $R[x]$ satisfying*

(i) $g(x) = f(x)q(x) + r(x)$.

(ii) $\deg r(x) < n$.

Theorem 2.8.6. *Let R be a commutative ring with 1, $a \in R$ and $f(x) \in R[x]$. Then*

(i) $\exists\, g(x) \in R[x],\ f(x) = (x - a)g(x) + f(a)$.

(ii) $(x - a) | f(x) \iff f(a) = 0$.

Definition 2.8.7. Let $f(x) \in R[x]$ and $a \in R$. Then a is called *a root of $f(x)$* if $f(a) = 0$.

Theorem 2.8.8. *Let R be an integral domain and $f(x) \in R[x] \backslash \{0\}$. If $a_1, a_2, \ldots, a_k$ are distinct roots of $f(x)$, then $(x - a_1)(x - a_2) \cdots (x - a_k) | f(x)$.*

Theorem 2.8.9. *If F is field, then $F[x]$ is a Euclidean Domain.*

Theorem 2.8.10. *Let F be a field.*

(i) *If $f(x) \in F[x]$ and $\deg f = n$, then $f(x)$ has at most n distinct roots.*

(ii) *If* $f(x), g(x) \in F[x]$ *and* $\deg f$, $\deg g \leq n$, *and* $f(\alpha_i) = g(\alpha_i)$ *for all* $i = 1, 2, \ldots, n+1$ *where* α_i*'s are distinct elements in* F, *then* $f(x) = g(x)$.

Definition 2.8.11. Let $f(x) \in R$ and a a root of $f(x)$. If $f(x)$ is divisible by $(x-a)^m$ but not by $(x-a)^{m+1}$ for some positive integer m, then a is said to be a root of ***multiplicity*** m.

Corollary 2.8.12. *If* F *is a field,* $f(x) \in F[x]$, *and* $\deg f(x) = n$, *then* $f(x)$ *has at most* n *roots.*

Theorem 2.8.13. *Let* F *be a field with* q *elements. Then*

(i) $F^* = F \backslash \{0\}$ *is a cyclic group (under multiplication) of order* $q-1$.

(ii) *If* $F^* = \{a_1, \ldots, a_{q-1}\}$, *then* $(x-a_1)(x-a_2)\cdots(x-a_{q-1}) = x^{q-1} - 1$.

(iii) *If* $F = \{0, a_1, \ldots, a_{q-1}\}$, *then* $x(x-a_1)(x-a_2)\cdots(x-a_{q-1}) = x^q - x$.

Theorem 2.8.14. *Let* F *be a field. Then*

(i) *Linear polynomials (polynomial of degree 1) are irreducible in* $F[x]$.

(ii) *Linear polynomials are the only irreducible elements in* $F[x]$ *iff each polynomial of positive degree has a root in* F.

Definition 2.8.15. Let R be a UFD and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 + a_0$ is a nonzero polynomial over R. The ***content*** of $f(x)$ is the greatest common divisor of $a_0, a_1, \ldots, a_n$. We say that $f(x)$ is ***primitive*** if $a_0, a_1, \ldots, a_n$ have no common divisor except units.

Theorem 2.8.16. *Let* R *be a UFD and* $f(x), g(x) \in R[x]$. *If* $f(x)$ *and* $g(x)$ *are primitive, then so is* $f(x)g(x)$.

Theorem 2.8.17. *Let* R *be a UFD and* $f(x)$ *and* $g(x)$ *are nonzero polynomials of* $F[x]$. *Then*

(i) $f(x)$ *is primitive iff the content of* $f(x)$ *is 1.*

(ii) *If* a *is the content of* f, *then* $f(x) = af_1(x)$ *where* $f_1(x)$ *is primitive.*

(iii) *If $f(x) = af_1(x)$ where $f_1(x)$ is primitive, then a is a content of f.*

(iv) *If a is the content of $f(x)$ and b is the content of $g(x)$, then ab is the content of fg.*

Theorem 2.8.18. *Let R be a UFD and $F = \mathbb{Q}(R)$ be its field of fraction. If $f(x)$ is an irreducible polynomial in $R[x]$, then $f(x)$, considered as a polynomial in $F[x]$ is irreducible in $F[x]$. In particular, if $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

Theorem 2.8.19. *Let R be a UFD and F its field of quotient. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. If $\frac{r}{s} \in F$ is a root of $f(x)$, where r and s are relatively prime, then $(sx - r)|f(x)$ in $R[x]$ and so $s|a_n$ and $r|a_0$ if $r \neq 0$.*

Corollary Let R be a UFD and F its field of fractions. Let $f(x) \in R[x]$ be primitive. Then $f(x)$ is irreducible in $R[x]$ iff $f(x)$ is irreducible in $F[x]$.

Theorem 2.8.20 (Eisenstein's Criterion). *Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$ $(n \geq 1)$. Assume that $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ are all in P and a_0 is not in P^2. Then $f(x)$ is irreducible in $R[x]$.*

Corollary (Eisenstein's Criterion for $\mathbb{Z}[x]$) Let p be a prime in $\mathbb{Z}$ and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] (n \geq 1)$. If $p|a_i$ for all i but $p^2 \nmid a_0$, then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Theorem 2.8.21. *Let R be UFD and F its field of fractions. Let $f(x) \in R[x]$. Then $f(x)$ is irreducible in $R[x]$ iff either*

(i) *$f(x) \in R$ and $f(x)$ is irreducible in R, or*

(ii) *$f(x)$ is a primitive polynomial of degree $n \geq 1$ and $f(x)$ is irreducible in $F[x]$.*

Theorem 2.8.22. *Let R be a UFD and $f(x) \in R[x]$. If $f(x)$ is irreducible in $R[x]$, then $(f(x))$ is a prime ideal, i.e. $f(x)$ is a prime.*

Theorem 2.8.23. *If R is a UFD, then $R[x]$ is a UFD.*

Corollary If R is a UFD then a polynomial ring in an arbitrary number of variables with coefficient in R is also a UFD.

Chapter 3

Fields

3.1 The Characteristic Fields

Definition 3.1.1. The **characteristic** of a field F, denoted $\text{char}(F)$, is the smallest positive integer m with the property that $m \cdot 1 = 0$ provided such a m exists, otherwise, it is defined to be 0.

Proposition 3.1.2. *For any field F,* $\text{char}(F)$ *is either* 0 *or a prime p.*

3.2 Extension Fields and Degrees of Extensions

Definition 3.2.1. A field K is said to be an **extension field** of a field F and is denoted $K_{|F}$, if $K \supseteq F$. The dimension of K as a vector space over F is called the **degree of a field extension** $K_{|F}$, denoted $[K : F]$. The extension is said to be finite if $[K : F]$ is **finite** and it is said to be **infinite** otherwise.

Theorem 3.2.2. *If $K_{|E}$ and $E_{|F}$ are finite field extensions, then $K_{|F}$ is also a finite field extension and*

$$[K : F] = [K : E][E : F]$$

.

Theorem 3.2.3. *Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial. Then there is an extension field E of F in which $p(x)$ has a root and $[E : F] =$ $\deg p(x)$. Moreover*

$$E = \{b_{n-1}\theta^{n-1}+b_{n-2}\theta^{n-2}+\cdots+b_1\theta+b_0 \mid b_{n-1}, b_{n-2}, ..., b_1, b_0 \in F\} \text{ where } \theta = x+(p(x)).$$

Definition 3.2.4. Let $K_{|F}$ be a field extension of a field F and $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. The intersection of all subfields of K containing F and $\alpha_1, \alpha_2, \ldots, \ldots, \alpha_n$, is called the **field generated by** $\alpha_1, \alpha_2, \ldots, \ldots, \alpha_n$ **over F** and is denoted $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

It is the smallest subfield with the above property. In particular, for each $\alpha \in K$, $F(\alpha)$ is the smallest subfields of K containing F and α.

Lemma 3.2.5. *Let $K_{|F}$ be a field extension of a field F. Let $\alpha, \beta \in K$. Then*

$$F(\alpha, \beta) = (F(\alpha))(\beta).$$

Moreover, if $[F(\alpha) : F] = m$ and $[F(\alpha)(\beta) : F(\alpha)] = n$, then $[F(\alpha, \beta)] = mn$ and any element of $F(\alpha, \beta)$ has the form $\sum_{\substack{i=1,2,...,m \\ j=1,2,...,n}} a_{ij}\alpha^i\beta^j$.

Definition 3.2.6. Let E_1 and E_2 be subfields of E. Then the ***composite field*** of E_1 and E_2, denoted E_1E_2, is the smallest subfield of E containing both E_1 and E_2. In general, the composite of any collection of subfields of E is the smallest subfield of E containing all the subfields.

Theorem 3.2.7. *Let E_1 and E_2 be two finite field extensions of a filed F both contained in E. Then $[E_1E_2 : F] \leq [E_1 : F][E_2 : F]$.*

Corollary *Let E_1 and E_2 be two finite field extensions of a field F both contained in E. Assume $[E_1 : F] = m$ and $[E_2 : F] = n$ where $(m, n) = 1$. Then $[E_1E_2 : F] = [E_1 : F][E_2 : F] = mn$*

Theorem 3.2.8. *Let $p(x)$ be an irreducible polynomial of $F[x]$. Let K be an extension field of F containing a root α of $p(x)$. Then*

(i) $F(\alpha) \cong F[x]/(p(x))$.

(ii) *If* $\deg p(x) = n$, *then* $F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F\}$.

Theorem 3.2.9. *Let* $\varphi : F \to F'$ *be a field isomorphism. Then* φ *induces a ring isomorphism* $\varphi^* F[x] \to F'[x]$ *with the property that* $\varphi^*(a) = \varphi(a)$ *for all* $a \in F$, *and* φ^* *maps a irreducible polynomial to the a irreducible polynomial. Moreover, if* α *is a root of an irreducible polynomial* $p(x)$ *and* β *is a root of* $\varphi^*(p(x))$, *then there exists an isomorphism* $\sigma : F(\alpha) \to F^{'}(\beta)$ *mapping* α *to* β *and extending* φ.

3.3 Algebraic Extensions

Definition 3.3.1. Let $E_{|F}$ be a field extension. $\alpha \in E$ is said to be ***algebraic over*** F if α is a root of some polynomial $f(x) \in F[x]$. If α is not algebraic over F, then α is said to be ***transcendental over*** F. $E_{|F}$ is said to be ***algebraic*** if every element of E is algebraic over F, and E is called an ***algebraic extension*** of F.

Theorem 3.3.2. *Let* $E_{|F}$ *be an extension and assume that* $\alpha \in E$ *is algebraic over* F. *Then*

(i) $\exists!$ *monic irreducible polynomial, denoted* $m_F(\alpha)$, *which has* α *as a root.*

(ii) $f(x) \in F[x]$ *has* α *as a root iff* $m_F(\alpha)$ *divides* $f(x)$ *in* $F[x]$ *(i.e. if* $I = \{f(x) \in F[x] \mid f(\alpha) = 0\}$, *then* I *is the ideal generated by* $m_F(\alpha)$*).*

(iii) $F(\alpha) \cong F[x]/(m_F(\alpha))$ *and* $[F(\alpha) : F] = \deg m_F(\alpha)$.

(iv) $F[\alpha] = F(\alpha)$.

Definition 3.3.3. The unique monic irreducible polynomial $m_F(\alpha)$ in theorem 3.3.2 is called the ***minimal polynomial*** for α over F. The degree of $m_F(\alpha)$ is called the ***degree*** of α over F, denoted $\deg(\alpha, F)$

Theorem 3.3.4. *Let* $E_{|F}$ *be an extension and* $\alpha \in E$. *Then* α *is algebraic over* F *iff* $F[\alpha]$ *is the field* $F(\alpha)$, *where* $F[\alpha] = \{f(\alpha) \mid f(x) \in F[x]\}$.

Theorem 3.3.5. *Let* $E_{|F}$ *be an extension. If* $[E : F] < \infty$, *then* E *is algebraic over* F.

Theorem 3.3.6. *Let $K_{|F}$ be an extension. Then $[K : F]$ is finite if and only if $K = F(\alpha_1, \alpha_2, ..., \alpha_k)$ for some algebraic elements $\alpha_1, \alpha_2, ..., \alpha_k$ over F. Moreover if, for each i, $[F(\alpha_i) : F] = n_i$, then $[K : F] \leq n_1 n_2 \cdots n_k$.*

Corollary *Let $K_{|F}$ be an extension. Then the set of elements of K that are algebraic over F forms a subfield of K.*

Theorem 3.3.7. *If $K_{|E}$ and $E_{|F}$ are algebraic extensions, then so is $K_{|F}$.*

3.4 Finite Fields

Theorem 3.4.1. *Every finite field must have prime power order.*

Corollary 3.4.2. *Every element of a finite field with characteristic p is algebraic over $\mathbb{Z}_p$.*

Definition 3.4.3. The extension field K of F is called a ***splitting field*** for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (or splits completely) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Theorem 3.4.4. *For any field F, if $f(x) \in F[x]$, then there exists an extension K of F which is a splitting field for $f(x)$.*

Theorem 3.4.5. *Let $\varphi : F \to F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ and let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and Let E' be a splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to an isomorphism $\sigma : E \to E'$.*

Theorem 3.4.6. *(Uniqueness of Splitting Fields) Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.*

Theorem 3.4.7. *For each prime p and each positive integer n, there is (up to isomorphism) a unique finite field of order p^n.*

3.5 Simple Extensions

Definition 3.5.1. Let $K_{|F}$ be a field extension. K is called a **simple extension** of F if $K = F(\alpha)$ for some $\alpha \in K$ and this α is called a primitive element for the extension.

Theorem 3.5.2 (Artin). *Let $E_{|F}$ be a finite degree field extension. Then $E = F(\alpha)$ for some $\alpha \in E$ if and only if there are only finitely many field K with $F \subseteq K \subseteq E$.*

Corollary 3.5.3. *Let $K_{|F}$ be a field extension. Assume that $K = F(\alpha)$ for some α which is algebraic over F. Then E is a simple extension for any field E such that $F \subseteq E \subseteq K$.*

Theorem 3.5.4. *If F is a field of characteristic 0 and if α and β are algebraic over F, then there is $\gamma \in F(\alpha, \beta)$ such that $F(\alpha, \beta) = F(\gamma)$.*