

Abstract Algebra
from the context of the courses
MTH 418H-419H: Honors Algebra

Kaedon Cleland-Host

February 10, 2022

Contents

1	Group Theory	2
1.1	Groups	2
1.2	Subgroups	2
1.2.6	Greatest Common Divisor	2
1.2.12	Least Common Multiple	3
1.2.16	Cyclic Groups	3
1.3	Homomorphisms	3
1.4	Cosets	4
1.4.5	Counting Formula	4
1.4.6	Lagrange's Theorem	4
1.5	Normal Subgroups	4
1.6	Quotient Groups	4
1.6.3	Correspondence Theorem	4
1.7	Product Groups	5
1.7.3	Multiplication Isomorphism	5
1.7.5	First Isomorphism Theorem	5
1.8	Group Actions	5
1.8.6	Orbit Stabilizer Theorem	5
1.9	Conjugation	6
1.10	p-Groups	6
1.10.3	Fixed Point Theorem	6
1.10.7	First Sylow Theorem	6
1.10.9	Second Sylow Theorem	6
1.10.11	Third Sylow Theorem	6
2	Field Theory	7
2.1	Rings and Fields	7
2.2	Ring Homomorphisms	7
2.3	Product Rings	7
2.4	Quotient Rings	8
2.5	Characteristic	8
2.6	Polynomial Rings	8
2.7	Ideals	8
2.8	Integral Domains	9
2.8.6	Principal Ideal Domain	9
2.8.7	Euclidean Domain	9
2.8.10	Unique Factorization Domain	9
2.9	Irreducibility	9
2.9.5	Gauss's Lemma	9
2.9.6	Eisenstein's Criterion	9
2.10	Field Extensions	9
2.10.17	Fundamental Theorem of Algebra	10
2.11	Symmetric Polynomials	10
2.11.3	Fundamental Theorem of Symmetric Polynomials	10
2.12	Noetherian Rings	10
2.12.4	Hilbert Basis Theorem	10
2.13	Modules	11
2.13.12	STFGMOPID	11

Chapter 1

Group Theory

1.1 Groups

Definition 1.1.1. A **law of composition** is a map $S^2 \rightarrow S$.

Remark. We will use the notation ab for the elements of S obtained as $a, b \rightarrow ab$. This element is the product of a and b .

Definition 1.1.2. A **group** is a set G together with a law of composition that has the following three properties:

1. **Identity** There exists an element $1 \in G$ such that $1a = a1 = A$ for all $a \in G$.
2. **Associativity** $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. **Inverse** For any $a \in G$, there exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = 1$.

Definition 1.1.3. An **abelian group** is a group with a commutative law of composition. That is for any $a, b \in G$, $ab = ba$.

Definition 1.1.4. The **order** of a group G is the cardinality of the set.

Proposition 1.1.5. Cancellation Law For $a, b, c \in G$ if $ab = ac$ then $b = c$.

Proposition 1.1.6. Let S be a set with an associative law of composition and an identity. The subset of elements of S that are invertible forms a group.

1.2 Subgroups

Definition 1.2.1. A group H is a **Subgroup** of G iff H is subset of G , H has the same law of composition as G , and H is also a group. In other words H a group iff it is a subset of G with the following properties:

1. **Closure** $a, b \in H$ then $ab \in H$.
2. **Identity** $1 \in H$.
3. **Inverse** For all $a \in H$, $a^{-1} \in H$.

Definition 1.2.2. A subgroup S of G is a **proper subgroup** iff $S \neq G$ and $S \neq \{1\}$.

Proposition 1.2.3. If H and K are subgroup of G , then $H \cap K$ is a subgroup.

Theorem 1.2.4. If S is a subgroup of \mathbb{Z}^+ , then either

- $S = \{0\}$
- $S = \mathbb{Z}a$, where a is the smallest elements of S .

Definition 1.2.5. For two integers $a, b \in \mathbb{Z}$ we stat that a **divides** b iff $\frac{b}{a} \in \mathbb{Z}$ denoted $a|b$.

1.2.6 Greatest Common Divisor

Definition 1.2.7. The **greatest common divisor** of two integers $a, b \in \mathbb{Z}$ is the integer $d \in \mathbb{Z}$ such that

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} | n = ra + sb \forall r, s \in \mathbb{Z}\}$$

Proposition 1.2.8. Properties of the greatest common divisor Let $a, b \in \mathbb{Z}$, not both zero, and let d be the greatest common divisor. Then

1. There are integers $r, s \in \mathbb{Z}$ such that $d = ra + sb$.
2. $d|a$ and $d|b$.
3. If $e \in \mathbb{Z}$ such that $e|a$ and $e|b$ then $e|d$.

Definition 1.2.9. Two integers $a, b \in \mathbb{Z}$ are **relatively prime** iff $\gcd(a, b) = 1$.

Corollary 1.2.10. A pair $a, b \in \mathbb{Z}$ is relatively prime if and only if there are integers $r, s \in \mathbb{Z}$ such that $ra + sb = 1$.

Corollary 1.2.11. Let p be a prime integer. If p divides a product ab of integers, then at least one of $p|a$ or $p|b$ holds.

1.2.12 Least Common Multiple

Definition 1.2.13. The **least common multiple** of two integers $a, b \in \mathbb{Z}$ is the integer $m \in \mathbb{Z}$ such that

$$\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$$

Proposition 1.2.14. Properties of least common multiple Let a, b be non-zero integers and let m be there least common multiple. Then

1. $a|m$ and $b|m$.
2. If $n \in \mathbb{Z}$ such that $b|n$ and $a|n$, then $m|n$.

Corollary 1.2.15. For $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$ then $ab = dm$.

1.2.16 Cyclic Groups

Definition 1.2.17. Let G be a group and $x \in G$. The **cyclic subgroup** generated by x denoted $\langle x \rangle$ is

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, 1, x^1, x^2, \dots\}$$

Remark. For any subgroup S that contains x we have $S \subset \langle x \rangle$.

Definition 1.2.18. The **order of an element** $x \in G$ is the order of the group $\langle x \rangle$. This is the smallest positive integer n such that $x^n = 1$.

Proposition 1.2.19. Let $\langle x \rangle \subset G$ and consider the set $S = \{k \in \mathbb{Z} | x^k = 1\}$

1. The set S is a subgroup of \mathbb{Z}^+
2. $x^r = x^s$ ($r \geq s$) if and only if $x^{r-s} = 1$.
3. If $S \neq \{0\}$, then $S = \mathbb{Z}n$ for some positive $n \in \mathbb{Z}$ and $\langle x \rangle = \{1, x^1, x^2, \dots, x^{n-1}\}$

Proposition 1.2.20. Let x be an element of finite order n in a group and let $k \in \mathbb{Z}$. Let $k = nq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

1. $x^k = x^r$
2. $x^k = 1$ if and only if $r = 0$.
3. The order of x^k is $n/\gcd(k, n)$.

1.3 Homomorphisms

Definition 1.3.1. A **homomorphism** $\varphi : G \rightarrow G'$ is a map from a group G to a group G' such that for any $a, b \in G$ we have

$$\varphi(ab) = \varphi(a)\varphi(b)$$

Proposition 1.3.2. Let $\varphi : G \rightarrow G'$ be a homomorphism

1. $\varphi(1) = 1$
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ for any $a \in G$

Definition 1.3.3. A homomorphism $\varphi : G \rightarrow G'$ is **injective** iff $\varphi(x) = \varphi(u) \Rightarrow x = u$

Definition 1.3.4. A homomorphism $\varphi : G \rightarrow G'$ is **surjective** iff for every $b \in G'$, there exists $a \in G$ such that $\varphi(a) = b$.

Definition 1.3.5. Let $\varphi : G \rightarrow G'$ be a homomorphism

1. The **kernal** of φ denoted $\ker(\varphi)$ is the set

$$\ker(\varphi) = \{a \in G | \varphi(a) = 1\}$$

2. The **image** of φ denoted $\text{Im}(\varphi)$ is the set

$$\text{im}(\varphi) = \{b \in G' | \exists a \in G, \varphi(a) = b\}$$

Corollary 1.3.6. A homomorphism $\varphi : G \rightarrow G'$ is injective if $\ker(\varphi) = \{1\}$

Corollary 1.3.7. A homomorphism $\varphi : G \rightarrow G'$ is surjective if $\text{Im}(\varphi) = G'$

Proposition 1.3.8. Let $\varphi : G \rightarrow G'$ be a homomorphism the $\ker(\varphi)$ and $\text{Im}(\varphi)$ are subgroups of G and G'

Definition 1.3.9. An **isomorphism** is a **bijective** homomorphism. A homomorphism is **bijective** iff it is both injective and surjective.

Proposition 1.3.10. If $\varphi : G \rightarrow G'$ is an isomorphism, then $\varphi^{-1} : G' \rightarrow G$ is also an isomorphism.

Definition 1.3.11. Two groups G and G' are **isomorphic** iff there is an isomorphism $\varphi : G \rightarrow G'$.

Definition 1.3.12. An **automorphism** is an isomorphism $\varphi : G \rightarrow G$.

1.4 Cosets

Definition 1.4.1. Let H be a subgroup of G . The **left coset** of H induced by an element $a \in G$ is the set

$$aH = \{ah | h \in H\}$$

The **right coset** of H induced by an element $a \in G$ is the set

$$Ha = \{ha | h \in H\}$$

Proposition 1.4.2. Let H be a subgroup of G . The left cosets partition G . The right cosets partition G .

Definition 1.4.3. For a subgroup H of G . The **index of H in G** denoted $[G : H]$ is the number of left cosets of H in G .

Lemma 1.4.4. All left cosets aH and all right cosets Ha of a subgroup H of a group G have the same order.

Lemma 1.4.5. Counting Formula. For a subgroup H of G we have

$$|G| = |H|[G : H]$$

Theorem 1.4.6. Lagrange's Theorem. Let H be a subgroup of a finite group G . The order of H divides the order of G .

Corollary 1.4.7. The order of an element of a finite group divides the order of the group.

Corollary 1.4.8. If G is a group of prime order then for $a \in G$ where $a \neq \mathbb{I}$, we have $G = \langle a \rangle$.

Corollary 1.4.9. If $\varphi : G \rightarrow G'$ is a homomorphism of finite groups then

$$|G| = |\ker(\varphi)||\text{Im}(\varphi)|$$

1.5 Normal Subgroups

Definition 1.5.1. A subgroup N of a group G is **normal** iff for every $a \in N$ and $g \in G$, $gag^{-1} \in N$.

Proposition 1.5.2. For any homomorphism $\varphi : G \rightarrow G'$ the $\ker(\varphi)$ is a normal subgroup of G .

Proposition 1.5.3. Let $H \subset G$ be a subgroup. Then the following are equivalent

1. H is a normal subgroup.
2. For all $g \in G$, $gHg^{-1} = H$
3. For all $G \in G$, $gH = Hg$
4. Every left coset of H in G is a right coset of H in G .

Corollary 1.5.4. If a group G has just one subgroup of order n , then that subgroup is normal.

1.6 Quotient Groups

Definition 1.6.1. Let $H \subset G$ be a subgroup. The **Quotient** is defined $G/H = \{\text{left cosets of } H\}$.

Proposition 1.6.2. If $H \subset G$ is a normal subgroup, then G/H is a group with law of composition $[aH][bH] = [abH]$.

Theorem 1.6.3. Correspondence Theorem Let $\varphi : G \rightarrow G'$ be a surjective homomorphism with kernel K . There is a bijective correspondence between subgroups of G' and subgroups of G that contain K .

$$\{\text{subgroups of } G \text{ that contain } K\} \leftrightarrow G/K$$

1.7 Product Groups

Definition 1.7.1. Let G and G' be groups, $G \times G'$ is the **product group** defined

$$G \times G' = \{(g, g') | g \in G, g' \in G'\}$$

with the law of composition

$$(a, a')(b, b') = (ab, a'b')$$

Proposition 1.7.2. Let G be a cyclic group of order mn where $\gcd(m, n) = 1$ then $G \cong C_m \times C_n$.

Proposition 1.7.3. Let H, K be subgroups of a group G . Consider the multiplication map

$$f : H \times K \rightarrow G$$

given by $f(h, k) = hk$. Then

1. f is a homomorphism if and only if $kh = hk$ for all $h \in H$ and $k \in K$
2. f is injective if and only if $H \cap K = \{1\}$
3. if H is normal the image HK of f is a subgroup of G .

In particular, $G \cong H \times K$ under f if and only if $H \cap K = \{1\}$, $HK = G$ and K and H are both normal.

Proposition 1.7.4. The map $\pi : G \rightarrow G/N$ defined by $\pi(x) = [aN]$ such that $x \in aN$ is a surjective homomorphism with kernel N .

Theorem 1.7.5. First Isomorphism Theorem Let $\varphi : G \rightarrow G'$ be a surjective homomorphism and let N be its kernel.

$$G' \cong G/N$$

1.8 Group Actions

Definition 1.8.1. An **action** of a group G on a set S is a map

$$G \times S \rightarrow S$$

$$(g, s) \mapsto g * s$$

such that

1. $1 * s = s$ for all $s \in S$.
2. **Associativity:** $(gg') * s = g * (g' * s)$ for all $g, g' \in G$ and $s \in S$.

Definition 1.8.2. Given an action of a group G on the set S , the **orbit** O_s of an element $s \in S$ is

$$O_s = \{gs \in S | g \in G\}$$

Definition 1.8.3. An action of G on S is **transitive** iff $S = O_s$ for some $s \in S$.

Definition 1.8.4. The **stabilizer** G_s of an element $s \in S$ is

$$G_s = \{g \in G | gs = s\}$$

Proposition 1.8.5. Let G be a subgroup of a group G .

1. The action of G on G/H is transitive.
2. The stabilizer $G_{[H]}$ of $[H]$ is the subgroup H .

Theorem 1.8.6. Orbit Stabilizer Theorem Let G be a group action on a set S . For any $s \in S$, there is a bijection

$$\epsilon : G/G_s \leftrightarrow O_s$$

$$[aG_s] \mapsto as$$

such that $\epsilon(g[C]) = g\epsilon([C])$ for all $g \in G$ and $[C] \in G/G_s$

Corollary 1.8.7. Let G be a group acting on a finite set S . Then for any $s \in S$

$$|G| = |O_s| |G_s|$$

1.9 Conjugation

Definition 1.9.1. The **conjugate** of $a \in G$ by $g \in G$ is gag^{-1} .

Definition 1.9.2. The **conjugation action** is the action of a group G defined by $G \times G \rightarrow G$ with $(g, x) \mapsto gxg^{-1}$.

Lemma 1.9.3. G is abelian \Leftrightarrow conjugation map is the identity

Definition 1.9.4. The **centralizer** of x is the stabilizer of x under conjugation.

$$Z(x) = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$$

Definition 1.9.5. The conjugacy class of x is the orbit of x under conjugation.

$$C(x) = \{gxg^{-1} \in G | g \in G\}$$

Definition 1.9.6. The **center** of a group G is the subgroup

$$Z = \{z \in G | zg = gz \text{ for all } g \in G\}$$

Corollary 1.9.7. The center of a group is a normal subgroup.

Corollary 1.9.8. Every centralizer contains the center.

Proposition 1.9.9. The Class Equation The orbits of of conjugation partition the group.

$$|G| = \sum_{\text{conjugacy classes } C} |C|$$

1.10 p-Groups

Definition 1.10.1. A p -group is a group of order p^n for some prime p .

Proposition 1.10.2. The center of a p -group is non-trivial.

Theorem 1.10.3. Fixed Point Theorem Let G be a p -group action on a finite set S If $|S|$ is not divisible by p , then there is a fixed point for the action of G on S .

Proposition 1.10.4. Every group of order p^2 is abelian.

Corollary 1.10.5. A group of order p^2 is either cyclic or a product of two cyclic groups

Definition 1.10.6. A subgroup $H \subset G$ of order p^e is called a **Sylow p -subgroup**.

Theorem 1.10.7. First Sylow Theorem A finite group whose order is divisible by a prime contains a Sylow p -subgroup.

Corollary 1.10.8. A group whose order is divisible by a prime p contains an element of order p .

Theorem 1.10.9. Second Sylow Theorem Let G be a finite group whose order is divisible by a prime p .

1. The Sylow p -subgroups of G are conjugate subgroups.
2. Every subgroup of G that is a p -group is contained in a Sylow p -subgroup.

Corollary 1.10.10. A group G has just one Sylow p -subgroup H if and only if H is normal.

Theorem 1.10.11. Third Sylow Theorem Let G be a finite group whose order $n = p^e m$, with p prime and p not dividing m . Let s be the number of Sylow p -subgroups of G . Then s divides m and $s \equiv 1 \pmod{p}$.

Chapter 2

Field Theory

2.1 Rings and Fields

Definition 2.1.1. A ring R is a set with two laws of composition denoted $+$ and \times that satisfy the following axioms:

- **Identity** \exists elements denoted $0, 1 \in R$ such that $1 \times a = a$ and $0 + a = a$, $\forall a \in R$.
- **Additive Inverse** For all $a \in R$, there exists an element $-a \in R$ such that $-a + a = 0$.
- **Associativity** For all $a, b, c \in R$, $a \times (b \times c) = (a \times b) \times c$ and $a + (b + c) = (a + b) + c$.
- **Commutativity** For all $a, b \in R$, $a \times b = b \times a$ and $a + b = b + a$.
- **Distributivity** For all $a, b, c \in R$, $a \times (b + c) = (a \times b) + (a \times c)$.

Definition 2.1.2. A field F is a ring with at least two elements where every nonzero element has a multiplicative inverse.

- **Multiplicative Inverse** For all nonzero $a \in F$, there exists an element $a^{-1} \in F$ such that $a \times a^{-1} = 1$.

Definition 2.1.3. A subring H is a subset of a ring R with the following properties

- **Closure** For all $a, b \in H$, $a \times b, a + b \in H$.
- **Identity** $0, 1 \in H$.
- **Additive Inverse** For all $a \in H$, $-a \in H$.

Definition 2.1.4. A subfield H is a subring of a field F with at least two elements that contains multiplicative inverses of nonzero elements.

- **Multiplicative Inverse** For all $a \in H$, $a^{-1} \in H$.

Proposition 2.1.5. Let R be a ring. $0 = 1$ in R if and only if R is the zero ring.

2.2 Ring Homomorphisms

Definition 2.2.1. A ring homomorphism $\varphi : R \rightarrow R'$ is a map such that for all $a, b \in R$

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\varphi(b)$
3. $\varphi(1) = 1$

Definition 2.2.2. A ring isomorphism is a bijective ring homomorphism.

Proposition 2.2.3. Let F be a field. If $f : F \rightarrow R$ is a ring homomorphism and R is nonzero, then f is injective.

Corollary 2.2.4. Any homomorphism between fields is injective.

2.3 Product Rings

Definition 2.3.1. Let R and R' be rings, $R \times R'$ is the **product ring** defined

$$R \times R' = \{(r, r') | r \in R, r' \in R'\}$$

with the laws of composition

$$\begin{aligned}(a, a') + (b, b') &= (a + b, a' + b') \\ (a, a')(b, b') &= (a \times b, a'b')\end{aligned}$$

2.4 Quotient Rings

Definition 2.4.1. The **quotient ring** R/I where I is an ideal of the ring R is the ring of cosets of I with ring structure

$$(a + I) + (b + I) = (a + b + I)$$

$$(a + I)(b + I) = (ab + I)$$

Proposition 2.4.2. Let $f : R \rightarrow S$ be a ring homomorphism and R/I be a quotient ring, f defines a ring homomorphism $R/I \rightarrow S$ if and only if $I \subset \ker(f)$.

2.5 Characteristic

Definition 2.5.1. A field F has **characteristic** n iff $\sum^n 1 = 0$. If no such sum is possible a field has characteristic 0.

Proposition 2.5.2. The characteristic of a field must be prime.

Definition 2.5.3. For prime $p \in \mathbb{N}$, let \mathbb{F}_p denote the field $\mathbb{Z}/(p)$.

Proposition 2.5.4. If a field F has characteristic $p > 0$ then there exists a unique homomorphism $\mathbb{F}_p \rightarrow F$ and if $p = 0$ then there exists a unique homomorphism $\mathbb{Q} \rightarrow F$.

2.6 Polynomial Rings

Definition 2.6.1. A **polynomial** with coefficients $a_i \in R$ in a ring R is a finite linear combination of powers of x^i

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

Definition 2.6.2. The **degree** of a polynomial f is the largest n such that $a_n \neq 0$.

Definition 2.6.3. A polynomial f is **monic** iff $a_n = 1$ where $n = \deg f$.

Definition 2.6.4. For a ring R the **polynomial ring** denoted $R[x_1, \dots, x_r]$ is the ring of polynomials constructed from linear combinations of powers of the variables x_1, \dots, x_r .

Proposition 2.6.5. Let $x = (x_1, \dots, x_m)$ and $y = (y_1, \dots, y_n)$ be sets of variables. There is a unique isomorphism

$$R[x, y] \rightarrow R[x][y]$$

which is the identity on R and sends $x \mapsto x, y \mapsto y$.

2.7 Ideals

Definition 2.7.1. An **ideal** I of a ring R is an additive subgroup such that for all $s \in I$ and $r \in R$, $rs \in I$.

Definition 2.7.2. A **principal ideal** generated by an element $a \in R$ in a ring R is the ideal

$$(a) = aR = Ra = \{ra \mid r \in R\}$$

Proposition 2.7.3. The kernel of a ring homomorphism is an ideal.

Definition 2.7.4. An **ideal generated by** a set of elements $a_1, \dots, a_n \in R$ in a ring R is the ideal

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

Definition 2.7.5. An ideal is **proper** iff it is neither $\{0\}$ nor R .

Proposition 2.7.6. A ring R is a field if and only if the only proper ideal is the zero ideal.

Definition 2.7.7. A **maximal ideal** M of a ring R is an ideal such that $M \neq R$ and there are no ideals I such that $M \subsetneq I \subsetneq R$.

Proposition 2.7.8. An ideal is maximal if and only if R/I is a field.

2.8 Integral Domains

Definition 2.8.1. A **domain** is a ring R such that $\forall a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$

Proposition 2.8.2. Any field is a domain.

Proposition 2.8.3. Any finite domain is a field.

Definition 2.8.4. An ideal I of a ring R is called **prime** iff R/P is a domain

Proposition 2.8.5. Any maximal ideal is prime.

Definition 2.8.6. A **principal ideal domain** is a domain R in which every ideal is principal.

Definition 2.8.7. A **euclidean domain** is a domain R a function $N : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ such that

1. $\forall x, y \in R, y \neq 0, \exists q, r \in R \text{ s.t. } y = xq + r$
2. $\forall x, y \in R, y \neq 0, N(x) \leq N(xy)$

Theorem 2.8.8. Any euclidean domain is a principal ideal domain

Proposition 2.8.9. Let $p(x) \in F[x]$ and $\alpha \in F$ if $p(\alpha) = 0$ then $p(x) = (x - \alpha)q(x)$ for some $q(x) \in F[x]$

Definition 2.8.10. A **unique factorization domain** is a domain R such that any $x \in R$ can be factorized into irreducible elements uniquely up to units. That is there exists irreducible elements $\tau_1, \tau_2, \dots, \tau_n \in R$ such that $x = \tau_1 \tau_2 \dots \tau_n$. Any for any other factorization $t_1, t_2, \dots, t_k \in R, n = k$ and $\exists \sigma \in S_n$ such that $t_i = u_i \tau_i$ for some unit $u_i \in R$.

Theorem 2.8.11. Any principle ideal domain is a unique factorization domain.

Theorem 2.8.12. If R is a unique factorization domain, then $R[x]$ is a unique factorization domain.

Corollary 2.8.13. If R is a unique factorization domain then $R[x_1, x_2, x_3, \dots]$ is a unique factorization domain.

2.9 Irreducibility

Definition 2.9.1. A **unit** is a ring R is an element which has a multiplicative inverse.

Proposition 2.9.2. If $x \in R, x$ is a unit if and only if $(x) = R$.

Definition 2.9.3. An **irreducible** element $r \in R$ is a nonzero nonunit element where $x = ab$ implies a or b is a unit.

Theorem 2.9.4. If R is a principle ideal domain then a nonzero $I = (x)$ is maximal if and only if x is irreducible.

Lemma 2.9.5. Gauss's Lemma - If $p(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ then $p(x)$ is still irreducible in $\mathbb{Q}[x]$.

Lemma 2.9.6. Eisenstein's Criterion Let $p(x) \in \mathbb{Z}[x]$, let $\beta \in \mathbb{Z}$ be a prime. $p(x) = \sum_{i=0}^n a_i x^i$ If

$$\beta \nmid a_n, \quad \beta \mid a_0, a_1, \dots, a_{n-1}, \quad \beta^2 \nmid a_0$$

then $p(x)$ is irreducible.

2.10 Field Extensions

Definition 2.10.1. A **field extension** is an (injective) homomorphism between fields.

Proposition 2.10.2. If $F \rightarrow K$ is a field extension then K is a vector space over F .

Definition 2.10.3. An extension $F \rightarrow K$ is **simple algebraic** iff

$$K \cong F[x]/(p(x)) \quad \dim_F K = \deg p(x)$$

Definition 2.10.4. An extension $F \rightarrow K$ is **simple transcendental** iff

$$K \cong F(x) \quad \dim_F K = \infty$$

Definition 2.10.5. A element of a field $\alpha \in K$ is **algebraic** iff for some extension $F \rightarrow K, F \rightarrow F(\alpha)$ is simple algebraic

Definition 2.10.6. A element of a field $\alpha \in K$ is **transcendental** iff for some extension $F \rightarrow K, F \rightarrow F(\alpha)$ is simple transcendental.

Definition 2.10.7. An extension $F \rightarrow K$ is **algebraic** iff every element is $\alpha \in K$ is algebraic over F . In other words, $\exists p_\alpha(x) \in F[x]$ such that $p_{\alpha\alpha}(\alpha) = 0$.

Proposition 2.10.8. If $F \rightarrow K$ is algebraic and $K \rightarrow L$ is algebraic then the composition $F \rightarrow L$ is algebraic.

Definition 2.10.9. The **degree** of a field extension is the dimension of the vector space formed.

Proposition 2.10.10. If $F \rightarrow K$ is a degree n field extension and $K \rightarrow L$ is a degree m extension, then $F \rightarrow K \rightarrow L$ is a degree mn extension.

Proposition 2.10.11. Every finite degree extension is a composition of simple algebraic extensions.

Proposition 2.10.12. Every finite degree extension is algebraic.

Definition 2.10.13. A polynomial $p(x) \in F[x]$ **splits** iff it factors into

$$c(x - r_1)(x - r_2) \dots (x - r_n) \quad r_i \in F$$

Proposition 2.10.14. Let F be a field, \exists field extension $F \rightarrow \Omega$ such that $p(x)$ splits as an element of $\Omega[x]$.

Definition 2.10.15. A field Ω is called algebraically closed iff every polynomial $p(x) \in \Omega[x]$ has a root in Ω .

Proposition 2.10.16. The following are equivalent:

1. Ω is algebraically closed.
2. Any polynomial $p(x) \in \Omega[x]$ splits.
3. The only irreducible polynomials in Ω are linear.
4. If $\Omega \rightarrow L$ is a finite field extension then $\Omega = L$.

Theorem 2.10.17. Fundamental Theorem of Algebra - \mathbb{C} is algebraically closed.

Theorem 2.10.18. Any field can be embedded into any algebraically closed field.

Definition 2.10.19. An **algebraic closure** of a field F is an algebraic extension of F which is algebraically closed.

Theorem 2.10.20. Any field has an algebraic closure.

Definition 2.10.21. A **field automorphism** is an isomorphism from a field F to itself.

Proposition 2.10.22. If $\mathbb{Q} \rightarrow K$ is a finite field extension then

$$|\text{Aut}(K)| \leq [K : \mathbb{Q}]$$

where $\text{Aut}(K)$ is the set of automorphisms on K .

2.11 Symmetric Polynomials

Definition 2.11.1. A polynomial $f \in K(x_1, x_2, \dots, x_n)$ is **symmetric** iff $\forall \sigma \in S_n$,

$$f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

Definition 2.11.2. The **elementary symmetric polynomial** $e_k \in F(x_1, x_2, \dots, x_n)$ for $k \geq 0$ is the symmetric polynomial

$$e_k(x_1, x_2, \dots, x_n) = \sum_{1 \leq j_1 < j_2 < \dots < j_k \leq n} x_{j_1} x_{j_2} \dots x_{j_k}$$

Theorem 2.11.3. Fundamental Theorem of Symmetric Polynomials Any symmetric polynomial $f \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ can be written uniquely as a linear combination of elementary symmetric polynomials with \mathbb{Z} coefficients.

2.12 Noetherian Rings

Definition 2.12.1. A ring R is **noetherian** iff any ideal $I \subseteq R$ is finitely generated. That is $I = (r_1, r_2, \dots, r_n)$ for $r_i \in R$.

Proposition 2.12.2. A ring R is noetherian if and only if any ascending chain of ideals stabilizes. That is if $I_1 \subseteq I_2 \subseteq \dots \subseteq R$ is an infinite chain of ideals then for some $n \in \mathbb{N}$, $I_m = I_{m+1} \quad \forall m > n$.

Proposition 2.12.3. If R is a noetherian ring, then for any ideal $I \subseteq R$ any quotient R/I is noetherian.

Theorem 2.12.4. The **Hilbert Basis Theorem** states that if R is noetherian then $R[x]$ is noetherian.

Corollary 2.12.5. If R is noetherian and n is finite, then for any ideal $I \in R[x_1, x_2, \dots, x_n]$, $R[x_1, x_2, \dots, x_n]/I$ is noetherian.

Definition 2.12.6. A ring R is an **F-algebra** iff there exists a ring homomorphism $F \hookrightarrow R$ from some field F .

Definition 2.12.7. An F-algebra $F \hookrightarrow R$ is a **finitely generated F-algebra** if $\exists a_1, a_2, \dots, a_n \in R$ such that any $r \in R$ can be produced by multiplying and adding elements of F and a_1, a_2, \dots, a_n .

Corollary 2.12.8. Any finitely generated F-algebra is noetherian.

2.13 Modules

Definition 2.13.1. Let R be a ring. An **R-module** M is an abelian group with scalar multiplication $\times : R \times M \rightarrow M$ such that the following properties hold

1. $1 \times m = m, \quad \forall m \in M$
2. $r_1 \times (r_2 \times m) = (r_1 r_2) \times m, \quad \forall m \in M, r_1, r_2 \in R$
3. $r \times (m_1 + m_2) = r \times m_1 + r \times m_2, \quad \forall m_1, m_2 \in M, r \in R$
4. $(r_1 + r_2) \times m = r_1 \times m + r_2 \times m, \quad \forall m \in M, r_1, r_2 \in R$

Definition 2.13.2. Let R be a ring. An **R-submodule** $N \subseteq M$ is an abelian subgroup such that $r \times n \in N \quad \forall r \in R, n \in N$

Definition 2.13.3. We say an R -module M is **finitely generated** if there are elements $m_1, m_2, \dots, m_n \in M$ such that for any $x \in M$ there exists $r_i \in R$ such that $x = \sum_{i=1}^n r_i m_i$.

Definition 2.13.4. An **R-module homomorphism** $\varphi : M \rightarrow N$ is a map such that

1. φ is a group homomorphism.
2. $\varphi(r \times m) = r \times \varphi(m), \forall r \in R$ and $\forall m \in M$.

Definition 2.13.5. The **direct sum** denoted \oplus is the product group of two R -modules. Let M and N be R -modules the direct sum module is

$$M \oplus N = \{(m, n) | m \in M, n \in N\}$$

with the standard law of composition and scalar multiplication

$$r \times (m, n) = (r \times m, r \times n)$$

Definition 2.13.6. A **free R-module** is an R -module that is isomorphic to $R^n = R \oplus R \oplus R \oplus \dots \oplus R$

Proposition 2.13.7. An R -module M is finitely generated if and only if there exists a surjective homomorphism $R^n \twoheadrightarrow M$.

Definition 2.13.8. A **basis** is a set of elements m_1, m_2, \dots, m_n in an R -module M where every element in M is uniquely generated by a linear combination of m_1, m_2, \dots, m_n .

Proposition 2.13.9. An $R[x]$ -module uniquely determines and is determined by an R -module M and a homomorphism $T : M \rightarrow M$.

Definition 2.13.10. An R -module M is **Noetherian** if and only if any submodule $N \subset M$ is finitely generated.

Proposition 2.13.11. If R is Noetherian and m is a finitely generated R -module then M is Noetherian.

Theorem 2.13.12. Structure Theorem for Finitely Generated Modules Over a PID - If M is a finitely generated R -module where R is a principal ideal domain, then M is isomorphic to

$$M \cong R^n \oplus R/(d_1) \oplus R/(d_2) \oplus R/(d_3) \oplus \dots \oplus R/(d_n)$$

for some $n, k > 0$ and $d_1, \dots, d_k \in R$.

Corollary 2.13.13. If $R = \mathbb{Z}$, then any finitely generated \mathbb{Z} -module M is isomorphic to

$$M \cong \mathbb{Z}^n \oplus \mathbb{Z}/(d_1) \oplus \mathbb{Z}/(d_2) \oplus \dots \oplus \mathbb{Z}/(d_k)$$

for some $n, k > 0$ and $d_1, \dots, d_k \in \mathbb{Z}$.

Corollary 2.13.14. If $R = F[x]$ for some field F , then any finitely generated $F[x]$ -module M is isomorphic to

$$M \cong F[x]^n \oplus F[x]^n/(p_1) \oplus F[x]^n/(p_2) \oplus \dots \oplus F[x]^n/(p_k)$$

for some $n, k > 0$ and $d_1, \dots, d_k \in \mathbb{Z}$.

Proposition 2.13.15. Any R -module homomorphism $\varphi : R^n \rightarrow R^m$ equivalent to multiplication by some matrix A .

Proposition 2.13.16. An $n \times n$ matrix A with entries in a ring R is invertible if and only if $\det(A)$ is a unit in R .

Proposition 2.13.17. For an $n \times m$ matrix A left multiplication by an $n \times n$ matrix S performs row operations on A and right multiplication by an $m \times m$ matrix T performs column operations on A .

Proposition 2.13.18. An invertible $n \times n$ matrix A with entries in R induces an isomorphism $R^n/K \rightarrow R^n/A(K)$ for some $K \subseteq R$.