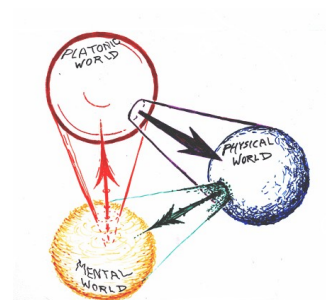


Algebra

Author: Maki

Date: July 21, 2022



Contents

1	Group Theory	1
1.1	Groups	1
1.2	Orders of Elements and Cyclic Groups	2
1.3	Direct Products of Groups	2
1.4	Subgroups	2
1.5	Normal Subgroups	3
1.6	Cosets and Quotient Groups	4
1.7	Group Homomorphisms and Group Isomorphisms	5
1.8	Isomorphism Theorems of Groups	5
1.9	Group Actions	6
1.10	The Class Equation	7
1.11	Sylow Theorems	8
1.12	Symmetric Groups and Alternating Groups	9
1.13	Semidirect Products of Groups	10
1.14	Abelianization of Groups	10
1.15	Solvable Groups	11
1.16	Nilpotent Groups	11
1.17	More Exercises	12
2	Ring Theory	13
2.1	Monoids	13
2.2	Rings	13
2.3	Subrings	14
2.4	Direct Products of Rings	15
2.5	Ideals	15
2.6	Ring Homomorphisms and Ring Isomorphisms	15
2.7	Quotient Rings	16
2.8	Isomorphism Theorems of Rings	16
2.9	Operations on Ideals	16
2.10	Integral Domain	17
2.11	Prime Ideals and Maximal Ideals	18
2.12	The Chinese Remainder Theorem	18
2.13	Localizations of Rings	19
2.14	Principal Ideal Domains	19
2.15	Divisions in Integral Domains	20
2.16	Greatest Common Divisor Domain	20
2.17	Unique Factorization Domains	21
2.18	Noetherian Rings	22
2.19	Artinian Rings	22
2.20	Euclidean Domains	22
2.21	Polynomial Rings	23
2.22	Polynomial Rings over Fields	24
2.23	Polynomial Rings over Unique Factorization Domains	24
2.24	Rings of Formal Power Series	24
2.25	Eisenstein's Criterion	25

2.26	Nilradicals of Rings	25
2.27	The Radicals of Ideals	25
2.28	The Jacobson Radicals of Ring	26
2.29	More Exercises	26
3	Module Theory	28
3.1	Modules	28
3.2	Submodules	28
3.3	Module Homomorphisms and Module Isomorphisms	28
3.4	Quotient Modules	29
3.5	Isomorphism Theorems of Modules	29
3.6	Direct Products of Modules	29
3.7	Direct Sums of Modules	30
3.8	Tensor Products of Modules	30
3.9	Torsion Modules	31
3.10	Torsion-free Modules	31
3.11	Pure Submodules	31
3.12	Finitely Generated Modules	32
3.13	Simple Modules	32
3.14	Semisimple Modules	32
3.15	Free Modules	33
3.16	Projective Modules	33
3.17	Fundamental Theorem of Finitely Generated Modules over Principal Ideal Domains	33
3.18	Jordan Canonical Form	34
3.19	Characteristic Polynomials and Minimal Polynomials	34
3.20	Rational Canonical Form	35
3.21	More Exercises	36
4	Representation Theory	37
4.1	Representation	37
4.2	Subrepresentations	37
4.3	Irreducible Representations	37
4.4	Completely Reducible Representations	37
4.5	Morphisms of Representations	38
4.6	Isomorphisms of Representations	39
4.7	Algebras over Fields	39
4.8	Group Algebras	39
4.9	Representations of Algebras	39
4.10	Characters	40
4.11	Schur Orthogonality Relations	41
4.12	Class Functions	42
4.13	First Orthogonality Relations	42
4.14	Regular Representations and Second Orthogonality Relations	43
4.15	More Exercises	45
5	Commutative Algebra and Algebraic Geometry	46
5.1	Vanishing/Zero Sets	46
5.2	The Zariski Topology on \mathbb{A}^n	46
5.3	Vanishing Ideals	47

5.4	Coordinate Rings	47
5.5	Hilbert Basis Theorem	48
5.6	Morphisms of Affine Varieties	48
5.7	Irreducible Varieties	49
5.8	Integrality	49
5.9	Noether Normalization and Zariski's Lemma	50
5.10	Hilbert's Nullstellensatz	51
6	Field Theory and Galois Theory	52
6.1	Fields	52
6.2	Polynomials over Fields	52
6.3	Field Extensions	52
6.4	Characteristics of Fields	53
6.5	Simple Extensions	53
6.6	Algebraic Extensions	54
6.7	Splitting Fields	54
6.8	Constructible Numbers	55
6.9	Cyclotomic Fields	55
6.10	Algebraic Closure	55
6.11	Separable Polynomials	56
6.12	Perfect Field	56
6.13	Separable Extensions	57
6.14	Finite Fields	57
6.15	Galois Groups	57
6.16	Fixed Fields	58
6.17	Normal Extensions	59
6.18	The Fundamental Theorem of Galois Theory	60
6.19	Applications of the Fundamental Theorem of Galois Theory	60
6.20	Cyclotomic Extensions	60

Chapter 1 Group Theory

1.1 Groups

Definition 1.1

We say (G, \cdot) is a monoid, if

1. $\forall x, y, z \in G, x(yz) = (xy)z$
2. $\exists e \in G, ex = xe = x$

where e is called an identity element.



Here, e is unique, since if e' is another identity element, then

$$e = ee' = e'.$$

Definition 1.2

We say (G, \cdot) is a group, if

1. $\forall x, y, z \in G, x(yz) = (xy)z$
2. $\exists e \in G, ex = xe = x$
3. $\forall x \in G, \exists x^{-1} \in G, xx^{-1} = x^{-1}x = e$

where x^{-1} is called the inverse of x .

We say G is abelian, if moreover $\forall x, y \in G, xy = yx$.

We say G is finite, if it is finite as a set. If so, we denote $|G|$ by the order of G , meaning the number of elements of G .



Here, x^{-1} is unique for all x , since if y, z are inverses of x , then

$$y = ye = y(xz) = (yx)z = ez = z.$$

Also, $(x^{-1})^{-1} = x$, since by definition,

$$x^{-1}x = xx^{-1} = e.$$

And, $(xy)^{-1} = y^{-1}x^{-1}$, since

$$(xy)y^{-1}x^{-1} = y^{-1}x^{-1}(xy) = e.$$

From now on, all the sets G are assumed to be groups and all the elements are assumed to be in a group unless otherwise specified.

Definition 1.3

For $n \in \mathbb{N}$, We denote x^n by $x \cdots x$, $x^0 = e$, and x^{-n} by $(x^{-1})^n$.



We may show that for all $m, n \in \mathbb{Z}$, we have

1. $x^{m+n} = x^m x^n$
2. $x^{mn} = (x^m)^n$.

Example 1.1 Additive groups contain $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Multiplicative groups contain $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, where the superscript $+$ means the positive elements and $*$ means nonzero elements. All of these groups are abelian.

Example 1.2 $GL(n, \mathbb{R})$ is the set of invertible $n \times n$ matrices over \mathbb{R} . $SL(n, \mathbb{R})$ is those matrices which have determinant

1. Both are nonabelian multiplicative groups.

Example 1.3 \mathbb{Z}_n is the set of congruence classes mod n . \mathbb{Z}_n^\times is the set of invertible congruence classes mod n . Both are finite abelian groups. Here, $|\mathbb{Z}_n| = n$ and $|\mathbb{Z}_n^\times| = \phi(n)$, the Euler ϕ function.

Definition 1.4

The symmetric group, or the permutation group of S , is given by $\text{Perm}(S) = \{\sigma : S \rightarrow S \text{ bijection}\}$. This is a group under composition.

In particular, we denote S_n by $\text{Perm}(\{1, \dots, n\})$

Definition 1.5

We define $Z(G)$ to be the center of G , by

$$Z(G) = \{x \in G : \forall g \in G, gx = xg\}$$

1.2 Orders of Elements and Cyclic Groups

Definition 1.6

If there exists $n \in \mathbb{N}_1$ such that $x^n = e$, then the smallest such n is called the order of x , denoted $|x|$. Otherwise, we say $|x| = \infty$.

If $|x| = n$, then by elementary number theory, $|x^m| = n/\gcd(m, n)$.

If G is abelian, and $|x|$ is coprime to $|y|$, then we have $|xy| = |x||y|$.

Definition 1.7

We say that G is cyclic, if there is an element $x \in G$, such that $G = \{x^n : n \in \mathbb{Z}\}$, denoted $\langle x \rangle$.

In fact, if G is finite, then G is isomorphic to \mathbb{Z}_n where $n = |G|$. Otherwise, G is isomorphic to \mathbb{Z} .

In particular, if x has a finite order, then $|\langle x \rangle| = |x|$.

1.3 Direct Products of Groups

Definition 1.8

If G_i is a group for all $i \in I$, then the direct product $\prod_i G_i$ is a group under the following multiplication,

$$(x_i)_{i \in I} (y_i)_{i \in I} = (x_i y_i)_{i \in I}$$

where the identity element is $(e_i)_{i \in I}$, and the inverse of $(x_i)_{i \in I}$ is $(x_i^{-1})_{i \in I}$.

In particular, we may define a finite product $G_1 \cdots G_n$ by $\prod_{i=1}^n G_i$.

1.4 Subgroups

Definition 1.9

We say H is a subgroup(of G), denoted $H < G$, if

1. $H \subset G$
2. H is a group under the multiplication in G .

Actually, we may show that H is a subgroup iff

1. $e \in H$
2. H is closed under multiplication, i.e., $\forall x, y \in H, xy \in H$
3. H is closed under inversion, i.e., $\forall x \in H, x^{-1} \in H$.

Also, this is equivalent to

1. H is nonempty

2. $\forall x, y \in H, xy^{-1} \in H$.

Definition 1.10

If $S \subset G$, then the subgroup generated by S , denoted $\langle S \rangle$, is defined by the smallest subgroup containing S .

Example 1.4

1. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$
 2. $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$.

We can show that the intersection of subgroups is again a subgroup by definition, and the trivial group (the group containing only the identity, unique up to an isomorphism) is a subgroup of every group.

Example 1.5 If G is abelian, then any subgroup is abelian.

Example 1.6 If $H_i < G_i$ for all $i \in I$, then $\prod_{i \in I} H_i < \prod_{i \in I} G_i$.

Example 1.7 We can show that any subgroup of a cyclic group $\langle x \rangle$ is cyclic with the form $\langle x^m \rangle$, where m is the smallest positive integer such that x^m is in the subgroup.

1.5 Normal Subgroups

Definition 1.11

Let N be a subgroup of G . We say N is a normal subgroup, denoted $N \triangleleft G$, if any of the following criterion holds (all equivalent)

1. $gN \subset Ng$ for all $g \in G$
2. $gN = Ng$ for all $g \in G$
3. $gNg^{-1} = N$ for all $g \in G$
4. $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.

The key is that $gN \subset Ng \iff g^{-1}N \supset Ng^{-1}$, so by symmetry we just need $gN \subset Ng$ for all $g \in G$.

Similarly, the intersection of normal subgroups is again a normal subgroup by definition.

Example 1.8 In an abelian group, every subgroup is a normal subgroup, since any two elements commute.

Example 1.9 The center $Z(G)$ is a normal subgroup of G .

Definition 1.12

If $S \subset G$ is a subset, then the centralizer and normalizer of S are defined to be

$$C_G(S) = \{x \in G : \forall s \in S, xs = sx\}$$

$$N_G(S) = \{x \in G : xS = Sx\}$$

Both $C_G(S)$ and $N_G(S)$ are subgroups of G and clearly $C_G(S) \subset N_G(S)$. In fact, we can show that $C_G(S) \triangleleft N_G(S)$.

Definition 1.13

If $H, K < G$, then H and K are called conjugate, if there is some $g \in G$, such that

$$K = gHg^{-1}$$

Example 1.10 If $H < G$, then $gHg^{-1} = g'Hg'^{-1} \iff g^{-1}g' \in N_G(H)$.

Example 1.11 If G is finite, and $H < G$ is a proper subgroup, then G is not a union of conjugacy subgroups of H .

Proof Assume not. Assume $|N_G(H)| = m, |H| = k$, and $|G| = n$, then $mk = n$. By the previous example, $mk = n = m(k-1) + 1$ for some $k \in \mathbb{N}_0$. Thus $m = 1$, so $H = G$, contradiction.

Example 1.12 $\Delta = \{(g, g) : g \in G\}$ is a normal subgroup of $G \times G$ iff G is abelian.

Proof Let $x, g \in G$, the condition forces $xgx^{-1} = ege^{-1} = g$, i.e., G is abelian.

Definition 1.14

G is called a *simple group* if it is nontrivial and the only normal subgroups are the trivial group and the group itself.



1.6 Cosets and Quotient Groups

Definition 1.15

If $H < G$, we define the *left and right cosets* of x to be

$$xH = \{xh : h \in H\}$$

$$Hx = \{hx : h \in H\}$$

Moreover, we define

$$G/H = \{xH : x \in G\}$$

$$H \backslash G = \{Hx : x \in G\}.$$



It is easy to show that $xH = yH \iff x^{-1}y \in H$ and $Hx = Hy \iff xy^{-1} \in H$. In particular, $xH = H \iff x \in H$. Thus, all left cosets (or right cosets) form a partition of G .

Example 1.13 If $H < G$ are finite groups, then $|H|$ divides $|G|$.

Example 1.14 If G is a finite group, then $|x|$ divides $|G|$, since $|\langle x \rangle| = |x|$. In particular, $x^{|G|} = e$ for all $x \in G$.

Proof In the finite case, we may partition G into finitely many $x_i H$, each having the same order as $|H|$.

Definition 1.16

If $H < G$ are finite groups, we define the *index* of H in G , denoted $[G : H]$, by

$$[G : H] = \frac{|G|}{|H|}.$$



In particular, we have

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

Example 1.15 If $K < H < G$ are finite groups, then

$$[G : K] = [G : H][H : K].$$

Example 1.16 If $H, K < G$ are finite subgroups, then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof It suffices to show that $[HK : K] = [H : H \cap K]$. To show this, we can show that for any $h, h' \in H$, $hK = h'K \iff h(H \cap K) = h'(H \cap K)$. Thus the representatives of the left cosets are equal.

By definition, a normal subgroup N is exactly one that makes all left and right cosets equal.

Definition 1.17

If $N \triangleleft G$, then $G/N = N \backslash G$ is a group, called the *quotient group*, under the following well-defined multiplication,

$$(xN)(yN) = (xy)N.$$



1.7 Group Homomorphisms and Group Isomorphisms

Definition 1.18

If G and G' are groups, then $f : G \rightarrow G'$ is a group homomorphism, if

$$\forall x, y \in G, f(xy) = f(x)f(y).$$

From now on, we will assume f is a group homomorphism unless otherwise specified.

We have $f(e) = e'$ and $f(x^{-1}) = f(x)^{-1}$ since

$$\begin{aligned} f(e) &= f(ee) = f(e)f(e) \\ f(x^{-1})f(x) &= f(x)f(x^{-1}) = f(e) = e'. \end{aligned}$$

Example 1.17 The projection $\pi_j : \prod_i G_i \rightarrow G_j$, sending $(x_i)_{i \in I}$ to x_j , is a surjective group homomorphism.

Definition 1.19

1. $\ker(f) = \{x \in G : f(x) = e'\}$
2. $\text{im}(f) = \{f(x) \in G' : x \in G\}$

$\ker(f)$ is a normal subgroup of G , and $\text{im}(f)$ is a subgroup of G' , by definition.

We can show that f is injective iff $\ker(f) = \{e\}$. The key step is that $f(x) = f(y) \implies xy^{-1} \in \ker(f)$.

Definition 1.20

We say $f : G \rightarrow G'$ is a group isomorphism, if

1. f is a group homomorphism
2. f is bijective.

If such a map exists, we say G is isomorphic to G' , denoted $G \simeq G'$.

Isomorphism is an equivalence relation by definition. Also, for an isomorphism f , its inverse is again an isomorphism.

Definition 1.21

The set of isomorphisms of G onto itself, called automorphisms of G , form a group, denoted $\text{Aut}(G)$.

Definition 1.22

Let $g \in G$, the conjugation by g is an automorphism on G , say ϕ_g , defined by

$$\phi_g(h) = ghg^{-1}.$$

These automorphisms are called the inner automorphisms.

In particular, the set of inner automorphisms, denoted $\text{Inn}(G)$, is a subgroup of $\text{Aut}(G)$, since

$$\phi_g \circ \phi_{g'} = \phi_{gg'}, \quad (\phi_g)^{-1} = \phi_{g^{-1}}$$

Example 1.18 If $H, K < G$ such that $G = HK$ and $H \cap K = \{e\}$, then $G \simeq H \times K$.

Proof Let $f : H \times K \rightarrow G = HK$ by $f(h, k) = hk$.

1.8 Isomorphism Theorems of Groups

Proposition 1.1

If $f : G \rightarrow G'$ is a group homomorphism, then

$$G/\ker(f) \simeq \text{im}(f).$$

Proof Let $N = \ker(f)$ and define $\tilde{f}(aN) = f(a)$. Then this is a well-defined group isomorphism from G/N to $\text{im}(f)$.

Proposition 1.2

If $N \triangleleft G, H < G$, then $H \cap N \triangleleft H, N \triangleleft HN$ and

$$H/H \cap N \simeq HN/N.$$

Proof Define $f : H \rightarrow HN/N$ by $f(h) = hN$. It is a surjective homomorphism with kernel $H \cap N$, so $H/H \cap N \simeq HN/N$.

Proposition 1.3

If $N, M \triangleleft G$ and $M < N$, then $M \triangleleft N, N/M \triangleleft G/M$, and

$$(G/M)/(N/M) \simeq G/N.$$

Proof Define $f : G/M \rightarrow G/N$ by $f(aM) = aN$. It is a well-defined surjective homomorphism with kernel N/M , so $(G/M)/(N/M) \simeq G/N$.

Example 1.19 By using properties of the determinant, we can show that $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \simeq \mathbb{R}^*$.

Example 1.20 $G/Z(G) \simeq Inn(G)$.

Proof Define $f : G \rightarrow Inn(G)$ by $f(g) = \phi_g$, the conjugation by g . f is clearly a surjective homomorphism. The kernel is the center $Z(G)$.

Example 1.21 If $Aut(G)$ is cyclic, then G is abelian.

Proof Since $G/Z(G) \simeq Inn(G) < Aut(G)$, so $G/Z(G)$ is cyclic. So we may take $a \in G$, such that $G = \langle a \rangle Z(G)$. Let $g = a^m x, g' = a^n y \in G$, then we have

$$gg' = a^m x a^n y = a^{m+n} xy = a^{m+n} yx = g'g$$

So G is abelian.

Example 1.22 If G is finite, then $[G : Z(G)]$ is not a prime.

Proof If $[G : Z(G)]$ is a prime, then $G/Z(G)$ is cyclic. Thus, G is abelian and $[G : Z(G)] = 1$.

Example 1.23 If $S \subset G$ is a subset, then $C_G(S) \triangleleft N_G(S)$ and $N_G(S)/C_G(S)$ is isomorphic to a subgroup of $Perm(S)$.

Proof Define $f : N_G(S) \rightarrow Perm(S)$ by $(f(x))(y) = xyx^{-1}$. By definition of $N_G(S)$, this is a well-defined homomorphism. Its kernel is $C_G(S)$, so we are done.

1.9 Group Actions

Definition 1.23

If G is a group, S is a set, then a left group action is a map from $G \times S$ to S , such that

1. $\forall x \in S, e \cdot x = x$
2. $\forall g, h \in G, \forall x \in S, g \cdot (h \cdot x) = (gh) \cdot x$

In this case, we call S a G -set.

Equivalently, we can define a left group action by a group homomorphism from G to $Perm(S)$. Besides, we can define right group action in a similar way.

Example 1.24 Group action by left multiplication on G is a group action of G on itself. We define $g \cdot h$ by gh .

Example 1.25 Group action by conjugation on G is a group action of G on itself. We define $g \cdot h$ by ghg^{-1} .

Example 1.26 If $N \triangleleft G$, then we have a group action by conjugation of G on N by $g \cdot n = gng^{-1} \in N$.

Example 1.27 If $H < G$, we can define a group action of G on G/H by $g \cdot g'H = (gg')H$.

From now on, we assume \cdot is a group action of G on S unless otherwise specified.

Definition 1.24

If $x \in S$, then the orbit and stablizer of x are defined by

$$Orb(x) = \{gx \in S : g \in G\}$$

$$Stab(x) = \{g \in G : gx = x\}.$$

The orbits form a partition of G , and each stablizer is a subgroup of G by definition.

Proposition 1.4

Let G be a finite group. If $x \in S$, then $|G| = |\text{Stab}(x)| \cdot |\text{Orb}(x)|$

Proof Define $f : G \rightarrow \text{Orb}(x)$ by $f(g) = gx$. This is a surjection. Note that $gx = hx \iff g^{-1}h \in \text{Stab}(x)$. So the preimage of every element in the orbit has the same cardinality. Therefore, $|G| = |\text{Stab}(x)| \cdot |\text{Orb}(x)|$.

Example 1.28 If G is finite, $x \in S$, then $|\text{Stab}(x)|$ divides $|G|$.

Definition 1.25

A left group action is called *transitive*, if for any $x, y \in S$, there exists some $g \in G$, such that $gx = y$. Equivalently, this means there is only one orbit.

Example 1.29 If $|G| = p^k$, and $p \nmid |S|$, then there is a fixed point, i.e., some element of S fixed by the entire G .

Proof The size of each orbit must divide p^k , hence p^i for some $i \geq 0$. Since $p \nmid |S|$, so we can find some orbit that has size $p^0 = 1$, and so the corresponding stablizer is the entire group.

Example 1.30 If $|G| = 55$ and $|S| = 24$, then there is a fixed point.

Proof The size of each orbit must divide 55, hence is 1, 5, or 11. Assume not. Since the orbits partition the set. So we must find $x, y \in \mathbb{N}_0$, such that $5x + 11y = 24$. Exhausting the case of $y = 0, 1, 2$, we find out that it is not possible. This concludes the proof.

Definition 1.26

If S, S' are G -sets, then $f : S \rightarrow S'$ is called a G -set morphism, if

$$\forall g \in G, \forall x \in S, g \cdot (f(x)) = f(g \cdot x).$$

f is called a G -set isomorphism, if it is a bijective morphism.

Example 1.31 If $H, K < G$, then the G -sets G/H and G/K are isomorphic iff H is conjugate to K .

Proof If $f : G/H \rightarrow G/K$ is an isomorphism, then assume $f(xH) = K$. $\text{Stab}(xH) = \text{Stab}(K)$, we get $K = xHx^{-1}$. On the other hand, if $K = xHx^{-1}$, we just need to define $f(gH) = gx^{-1}K$ to get an isomorphism.

1.10 The Class Equation

Proposition 1.5

If G is finite, then we may choose some representatives x_i such that

$$|G| = \sum_i |\text{Orb}(x_i)|$$

Proof This is directly from the fact that orbits form a partition of S .

Proposition 1.6

If G is finite, then we may choose some representatives x_i such that

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

Proof Consider the group action by conjugation. The orbit of x is $\{gxg^{-1} : g \in G\}$. The stablizer of x is by definition $C_G(x)$. Hence the size of $\text{Orb}(x)$ is $[G : C_G(x)]$. In particular, the orbit of x has size 1 exactly when $gxg^{-1} = x$ for all $g \in G$, i.e., the elements in the center. Putting these elements together, so then all the other $[G : C_G(x_i)] \geq 2$ and also $[G : C_G(x_i)]$ divides $|G|$.

Example 1.32 If $|G| = p^n$ for some $n \geq 1$, then $Z(G)$ is nontrivial.

Proof Since $[G : C_G(x_i)] \geq 2$ and $[G : C_G(x_i)]$ divides $|G|$, so each $[G : C_G(x_i)] = p^{m_i}$ for some $m_i \geq 1$. Also, p divides $|G|$. Thus, p divides $Z(G)$.

Example 1.33 If $|G| = p^n$ and $N \triangleleft G$ is a nontrivial normal subgroup, then $N \cap Z(G)$ is nontrivial.

Proof Consider the group action by conjugation of G on N . The orbit of n is 1 iff $gng^{-1} = n$ for all $g \in G$, i.e., when $n \in N \cap Z(G)$. Similar to the previous class equation, all the sizes of other orbits are multiples of p , and $|N|$ is also a multiple of p , so $N \cap Z(G)$ is nontrivial.

Example 1.34 If G is finite and p is the smallest prime divisor of $|G|$, then any normal subgroup of order p is contained in the center of G .

Proof Let N be a normal subgroup of order p and consider the group action by conjugation of G on N . The orbit of n is 1 iff $n \in N \cap Z(G)$. Since all the other orbits have sizes at least p , so there are no nontrivial orbits. Thus, $N = N \cap Z(G)$, i.e., $N \subset Z(G)$.

Proof By the previous group action, we have a group homomorphism from G to $\text{Inn}(N) < \text{Aut}(N)$. The size of the kernel must divide $|G|$ and also $p - 1$, so this map is trivial. In other words, $gn = ng$ for all $g \in G, n \in N$.

Example 1.35 Let G be a simple group such that p^2 divides $|G|$. Show that $[G : H] \geq 2p$.

Proof Consider the group action by conjugation of G on G/H . It induces a map from G to $\text{Perm}(G/H)$. The kernel must be $\{e\}$ or G . Assume the kernel is G , then p^2 divides $|G|$ and again divides $[G : H]!$, so $[G : H] \geq 2p$. If the kernel is $\{e\}$, then $gH = H$ for all $g \in G$, contradiction.

Example 1.36 If $H < G$ such that $[G : H] = n$, then there is a normal subgroup K contained in H .

Proof Consider the group action by conjugation of G on G/H . It induces a map from G to $\text{Perm}(G/H)$. Let K be the kernel. Then $|K|$ divides the $|\text{Perm}(G/H)| = n!$. If $k \in K$, then $x^{-1}kx \in H$, so $K = x^{-1}Kx \subset H$.

1.11 Sylow Theorems

Definition 1.27

G is called a p -group if $|G| = p^n$ for some n .

Proposition 1.7

If $|G| = p^n s$ where $p \nmid s$, then there is a subgroup of order p^n , called a Sylow p -subgroup of G .

Proposition 1.8

If H, K are Sylow p -subgroups of G , then they are conjugate to each other.

Proposition 1.9

If $|G| = p^n s$ where $p \nmid s$, and n_p is defined to be the number to Sylow p -subgroups, then

$$n_p \equiv 1 \pmod{p}, \quad n_p | s.$$

In fact, $n_p = [G : N_G(P)]$ where P is some Sylow p -subgroup.

Proof We have shown that $gPg^{-1} = hPh^{-1} \iff g^{-1}h \in N_G(P)$, so $n_p = [G : N_G(P)]$ and hence divides $|G|$. Since p does not divide n_p , so n_p divides s .

Example 1.37 If $|G| = p^n q$ where $p > q$ are prime numbers, then G has a unique normal subgroup of index q .

Proof $n_p | q, n_p \equiv 1 \pmod{p}$. n_p cannot be q since $q - 1 < p$, so $n_p = 1$. In particular, this means the unique Sylow p -subgroup P is normal.

Example 1.38 There are no simple groups of order 63.

Proof $63 = 3^2 \cdot 7$. $n_7 | 3, n_7 \equiv 1 \pmod{7}$, so $n_7 = 1$. There is a unique Sylow 7-subgroup, thus normal.

Example 1.39 There are no simple groups of order 70.

Proof $70 = 2 \cdot 5 \cdot 7$. $n_7 | 10, n_7 \equiv 1 \pmod{7}$, so $n_7 = 1$. There is a unique Sylow 7-subgroup, thus normal.

Example 1.40 There are no simple groups of order 200.

Proof $200 = 2^3 \cdot 5^2$. $n_5 | 8$, $n_5 \equiv 1 \pmod{5}$, so $n_5 = 1$. There is a unique Sylow 5-subgroup, thus normal.

1.12 Symmetric Groups and Alternating Groups

Definition 1.28

We define the symmetric group S_n to be the permutation group on $\{1, \dots, n\}$, so that each element (i.e., permutation) is a bijection on $\{1, \dots, n\}$.

Definition 1.29

If i_1, \dots, i_m are distinct in $\{1, \dots, n\}$, then $(i_1 i_2 \dots i_m)$ denotes the permutation that sends each i_j to i_{j+1} except that i_m is sent to i_1 and all the other elements are preserved.

Each permutation has a unique decomposition into a product of disjoint cyclic permutations. It can be easily seen that σ is a product of disjoint $(i, \sigma(i), \dots, \sigma_{m-1}(i))$.

Definition 1.30

If $1 \leq i < j \leq n$, then $(i j)$ is called a transposition.

Let $f : A^n \rightarrow A$ is a function, then $\sigma_f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ gives a group action. In particular, taking $f = \Delta = \prod_{i < j} (x_j - x_i)$, and τ a transposition, we can get $\tau(\Delta) = -\Delta$. Let $\epsilon : S_n \rightarrow \{\pm 1\}$ to be the sign before Δ , then this is a surjective homomorphism. This map is called the sign map.

Definition 1.31

We define the alternating group to be $A_n = \{\sigma \in S_n : \epsilon(\sigma) = 1\}$, then this is a normal subgroup of S_n .

A useful lemma says that $\sigma(i_1 \dots i_m)\sigma_{-1} = (\sigma(i_1) \dots \sigma(i_m))$. This quickly proves that any embedded S_m ($m < n$) (by fixing the other $n - m$ elements) is not normal in S_n .

Example 1.41 The Klein 4-group $K \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ can be embedded as a normal subgroup in A_4 , with index 3.

Proof By the previous lemma, $\{e, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\}$ is normal in A_4 where no element has order 4, and we are done.

Proposition 1.10

If $n \geq 5$, then A_n is simple.

Example 1.42 Let $n \geq 5$. Then the only nontrivial proper normal subgroup of S_n is A_n .

Proof Let $N \triangleleft S_n$. Notice that $N \cap A_n$ can only be $\{e\}$ or A_n (not possible), so $S_n \simeq A_n \times N$, but S_n has no normal subgroups of order 2, by the previous lemma.

Example 1.43 Let $n \geq 5$. Then the only nontrivial proper subgroup of index $< n$ in S_n is A_n .

Proof Consider the action of S_n on $\text{Aut}(S_n/H)$. The kernel must have order $< n! = |S_n|$, so the action is trivial (thereby $G = H$, not possible), or the kernel is A_n , so the subgroup must be A_n .

Proof A_m can be embedded in A_n if $m < n$.

Proof Just treat A_m as permutations fixing the last $n - m$ numbers, and we are done.

Example 1.44 Find a subgroup of S_4 of order 8.

Proof The subgroup generated by $(1 2 3 4)$ and $(1 3)$ is isomorphic to D_4 .

Example 1.45 If G is simple and has n Sylow p -subgroups, then there is an embedding of G into A_n .

Proof Consider the group action by conjugation of G on the set of Sylow p -subgroups. We have a homomorphism from G to S_n . Moreover, compose this map with the sign map, the kernel must be trivial, so G can be embedded into A_n .

Example 1.46 Find $x, y \in A_4$ such that they are conjugate in S_4 but not in A_4 .

Proof Consider $(1 2 3)$ and $(1 3 2)$. If $(1 2 3) = (\sigma(1) \sigma(2) \sigma(3))$, then $\sigma \notin A_4$.

1.13 Semidirect Products of Groups

Lemma 1.1

If $G = HK$ where $H, K \triangleleft G$ and $H \cap K = \{e\}$, then $G \simeq H \times K$.

Proof Let $h \in H, k \in K$. Then $hkh^{-1}k^{-1} \in H \cap K$, so $hk = kh$. In particular, this shows that $(h, k) \mapsto hk$ is a group homomorphism, and we are done.

Definition 1.32

If $G = NH$ where $N \triangleleft G, H < G$ and $N \cap H = \{e\}$, then G is called a semidirect product of N and H , denoted $G = N \rtimes H$.

The semidirect product is generally not unique, for example, $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$ can be either \mathbb{Z}_6 or S_3 .

Proposition 1.11

The semidirect product $N \rtimes H$ is uniquely determined by the action $H \rightarrow \text{Aut}(N)$ given by conjugation.

Proof Given an action $\phi : H \rightarrow \text{Aut}(N)$, we can define a group structure on (N, H) by $(n, h)(n', h') = (n\phi_h(n'), hh')$. Define $f : G = NH \rightarrow (N, H)$ by $f(nh) = (n, h)$. It is a well-defined group isomorphism, and we are done.

Example 1.47 Classify all groups of order 30.

Proof By Sylow's Theorem, we can show that $n_3 \in \{1, 10\}, n_5 \in \{1, 6\}$. They cannot both take the larger value, since otherwise 20 elements will have order 3 and 24 elements will have order 5. Let P, Q be Sylow subgroups of order 3 and 5. Since $5 \nmid 1 \neq 3$, so we can always have a normal subgroup of order 15, say N since it has index 2. Thus, $G \simeq \mathbb{Z}_{15} \rtimes \mathbb{Z}_2$. Let $\phi : \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_{15}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$ be a group homomorphism. $\phi(1)$ has order 2, so there are 4 possibilities. $\mathbb{Z}_{30}, \mathbb{Z}_5 \times S_3, D_{15}, \mathbb{Z}_3 \times D_5$ are these groups.

Example 1.48 Give an example when $G = HK, H, K < G, H \cap K = \{e\}$ but G is not a semidirect product of them.

Proof This is equivalent to saying that H, K are not normal subgroups. Take $G = S_5, H = S_4, K = \langle (1 \cdots n) \rangle$. Both H and K are not normal, and we are done.

1.14 Abelianization of Groups

Definition 1.33

The commutator subgroup of a group G is the normal subgroup generated by all commutators $[a, b] = aba^{-1}b^{-1}$, and is denoted $[G, G]$.

It is natural to have that $G/[G, G]$ is an abelian group, since $aba^{-1}b^{-1} \in [G, G]$.

Lemma 1.2

If $N \triangleleft G$, then G/N is normal iff $[G, G] \subset N$.

Proof The key is that $abN = baN$ iff $aba^{-1}b^{-1} \in N$ and that N is normal.

Proposition 1.12

Let H be an abelian group, then every group homomorphism $f : G \rightarrow H$ factors through $G/[G, G]$.

Proof It suffices to show that $[G, G] \in \ker(f)$. Note that $f(aba^{-1}b^{-1}) = e'$ and $f(gag^{-1}) = f(a)$, and we are done.

Example 1.49 There are exactly two different group homomorphisms from S_n to \mathbb{C}^* .

Proof The abelianization of S_n is \mathbb{Z}_2 , since abelianization forces all transpositions be equal, so the question is equivalent to asking for homomorphism from \mathbb{Z}_2 to \mathbb{C}^* , which is trivial.

Example 1.50 Find homomorphisms from A_4 to \mathbb{C}^* .

Example 1.51 The abelianization of A_4 is \mathbb{Z}_3 with the commutator subgroup isomorphic to K by enumerating all normal subgroups and their quotients. Thus, there are 3 such homomorphisms.

1.15 Solvable Groups

Definition 1.34

A subnormal series of G is a series of subgroups $N_i < G$ such that

$$\{e\} = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_m = G$$



Definition 1.35

A composition series of G is a series of subgroups $N_i < G$ such that

$$\{e\} = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_m = G$$

where each N_{i-1} is the maximal normal subgroup of N_i



Proposition 1.13 (Jordan Holder's Theorem)

If G is finite, then the composition series is unique up to an isomorphism, in the sense that the length of the series is equal and the quotient groups N_i/N_{i-1} are equal up to a rearrangements.



Definition 1.36

G is called solvable, if there is a subnormal series

$$\{e\} = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_m = G$$

where each N_i/N_{i-1} is abelian.



Example 1.52

Example 1.53 S_4 is solvable.

Proof Note that $\{e\} \triangleleft \mathbb{Z}_2 \triangleleft K \triangleleft A_4 \triangleleft S_4$, and we are done.

Example 1.54 S_n is not solvable for $n \geq 5$.

Proof Let $n \geq 5$, then A_n is the only nontrivial normal subgroup of S_n . Note that in this case A_n is a simple nonabelian group, and we are done.

1.16 Nilpotent Groups

Definition 1.37

G is called nilpotent if there is a lower central series terminating in the trivial group in finitely many steps, i.e.,

$$G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{e\}$$

where $G_i = [G, G_{i-1}]$.



Nilpotent groups are closed under direct product.

Example 1.55 Abelian groups are nilpotent.

Example 1.56 Finite p -groups are nilpotent.

Proof We have shown that $\mathbb{Z}(G)$ is nontrivial, and nilpotent since it is abelian. By induction, $G/Z(G)$ is nilpotent and we are done.

1.17 More Exercises

Example 1.57 S_5 has more than one Sylow 2-subgroups.

Proof D_4 can be embedded into S_4 . By choosing different 4 elements in $\{1, \dots, 5\}$, we are done.

Example 1.58 The group of rotations of the cube is isomorphic to S_4 .

Proof Any rotation is determined by the 4 main diagonals, so the group of rotations can be embedded into S_4 . Note that the group of rotations fixing 1 main diagonal is isomorphic to S_3 and that the order of any main diagonal has size 4, so the order of this group is 24. Thus, it is isomorphic to S_4 .

Example 1.59 Any finite group with order larger than 3 has a nontrivial automorphism.

Proof Since $G/Z(G) \simeq \text{Inn}(G) < \text{Aut}(G)$, so if G is nonabelian, then $\text{Aut}(G)$ is nontrivial. On the other hand, if G is abelian, then $x \mapsto x^{-1}$ is an automorphism.

Example 1.60 Give a counterexample to the statement: if $G=KH$, where $K, H < G$ and $H \cap K = \{e\}$, then $(k, h) \mapsto kh$ is a bijection.

Proof If so, then G is the inner direct product of K and H . In D_3 , take $\{e, f_1\}\{e, f_2\}$ to get a counterexample where f_i 's are different reflections.

Example 1.61 If p is an odd prime, and $G = GL(2, \mathbb{F}_p)$, then $n_p = p + 1$.

Proof Since $|G| = (p-1)^2 p(p+1)$, so

$$P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

generates a Sylow p -subgroup. It suffices to prove $[G : N_G(P)] = (p-1)^2(p+1)$. Note that $APA^{-1} \in \langle P \rangle$ iff A has the third entry equal to 0, and we are done.

Example 1.62 In $G = S_{2p}$ where p is an odd prime, a Sylow p -subgroup is abelian and isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, and $n_p = \binom{2p}{p}/2$.

Proof $Z(G)$ cannot be trivial or has prime order, so $P = S_{2p}$ is abelian, thus $\mathbb{Z}_p \times \mathbb{Z}_p$. To find a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, we need to find σ, τ in a partition of $\{1, \dots, 2p\}$ into two subsets of order p . Thus, $n_p = \binom{2p}{p}/2$, and this satisfies the third Sylow's Theorem.

Example 1.63 Classify groups of order 1001.

Proof By Sylow's Theorem, $n_7 = n_{11} = n_{13} = 1$. Take the three normal subgroups N, M, K , so $G \simeq \mathbb{Z}_{1001}$.

Example 1.64 Consider the group action of D_6 on the cartesian product of the vertices with itself by action on each coordinate. Find the orbits and sizes of stabilizers.

Proof Let $\{1, \dots, 6\}$ be the vertices in order. By geometry, it is easy to see that there are four orbits, with representatives $(1, 1), (1, 2), (1, 3), (1, 4)$. The sizes of orbits are 6, 12, 12, 6 and the sizes of stabilizers are 6, 3, 3, 6 by the orbit-stabilizer theorem.

Example 1.65 If G is finite, $H < G$ is a p -subgroup, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

Proof Consider the action of H on G/H by left multiplication and use the class equation. Note that gH is fixed by all $h \in H$ iff $g \in N_G(H)$ and $gH = g'H$ iff $g^{-1}g' \in H$. So $[G : H] = [N_G(H) : H] + pm$ for some $m \in \mathbb{Z}$, and we are done.

Chapter 2 Ring Theory

2.1 Monoids

Definition 2.1

We say (M, \cdot) is a monoid, if

1. $\forall x, y, z \in M, x(yz) = (xy)z$
2. $\exists e \in M, \forall x \in M, ex = xe = x$

Moreover, we say (M, \cdot) is a commutative ring, if \cdot is commutative.



Similarly, the identity is always unique. In a monoid, x is called an invertible element if there exists $y \in M$, such that $xy = yx = e$.

Lemma 2.1

If (M, \cdot) is a monoid, then the set of all invertible elements forms a group.



Proof e is invertible since $ee = e$. If x is invertible such that $xy = yx = e$, then y is also invertible.

Example 2.1 \mathbb{N}_0 is a monoid.

Example 2.2 The $n * n$ matrices over \mathbb{R} forms a monoid under multiplication.

2.2 Rings

Definition 2.2

We say $(R, +, \cdot)$ is a ring, if

1. $(R, +)$ is an abelian group.
2. (R, \cdot) is a monoid.
3. $\forall x, y, z \in R, x(y + z) = xy + xz, (x + y)z = xz + yz$.

Moreover, we say $(R, +, \cdot)$ is a commutative ring, if \cdot is commutative.



We usually denote 0 as the additive identity, and 1 as the multiplicative identity. In some books, 1 is not necessary, and the one with 1 is called a unital ring.

Example 2.3 \mathbb{Z}, \mathbb{Z}_n are commutative rings.

Example 2.4 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings.

Example 2.5 The $n * n$ matrices over \mathbb{R} , denoted $M_n(\mathbb{R})$, is a non-commutative ring.

From now on, R is assumed to be a ring (with 1) unless otherwise specified.

It is easy to show that $a0 = 0a = 0$, $a(-b) = (-a)b = -(ab)$, and $(-a)(-b) = ab$ for all $a, b \in R$.

Lemma 2.2

$R = \{0\} \iff 0 = 1$.



Proof The key is that $a = 1a = 0a = 0$ will force every element to be 0 .

Definition 2.3

A multiplicative invertible element of R is called a unit.

The group of units is called the multiplicative group of R , denoted R^\times .



Definition 2.4

R is called a *division ring*, if every nonzero element is a unit, i.e., $R^\times = R^*$.
Moreover, it is called a *field*, if it is a commutative division ring.

Example 2.6 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Equivalently, $(R, +, \cdot)$ is a field, iff

1. $(R, +)$ is an abelian group.
2. (R^*, \cdot) is an abelian group.
3. $\forall x, y, z \in R, x(y + z) = xy + xz$.

Definition 2.5

The center $Z(R)$ is defined to be

$$Z(R) = \{x \in R : \forall y \in R, xy = yx\}$$

Given $x \in R$, the centralizer of x is

$$C_R(x) = \{y \in R : xy = yx\}$$

$Z(R)$ is always a commutative ring, and $C_R(x)$ is always a ring.

Example 2.7 The center of $M_n(\mathbb{R})$ is generated by the identity matrix.

Example 2.8 The center of a division ring is a field.

Example 2.9 A division ring is a vector space over its center.

Proposition 2.1 (Wedderburn's little Theorem)

A finite division ring is a field.

Proof Let $q = |Z(R)|$ and $x \in R$, so $|R| = q^n$ for some $n \in \mathbb{N}_1$, and $C_R(x) = q^d$ for some $d \in \mathbb{N}_1$. In the multiplicative group R^* , consider the group action by conjugation. Using the class equation, we have

$$q^n - 1 = q - 1 + \sum_i \left(\frac{q^n - 1}{q^{d_i} - 1} \right)$$

Using cyclotomy theory, consider $x_m - 1 = \prod_{d|m} \Phi_d(x)$ where Φ_d is the d -th cyclotomic polynomial. So we must have $\Phi_n(q) | (q - 1)$. However, if $n > 1$, by comparing the primitive n -th roots of unity and q , we should have $|\Phi_n(q)| > q - 1$, leading to a contradiction. Thus, $n = 1$ and $R = Z(R)$, so R is a field.

Proposition 2.2

If F is a field, then F^* is cyclic.

Proof Let $q = |F^*|$. Let $d|q$. Note that the number of elements in F^* with order d is either 0 or $\phi(d)$. We denote this number by $\psi(d)$. Since $\sum_{d|n} \phi(d) = n$, so $\psi(d) = \phi(d)$ for all $d|n$. In particular, F^* is cyclic.

Example 2.10 Find criterion that -1 is a square in a finite field F .

Proof It is true iff there is an element of order 4, which is again equivalent to saying that $4|(q - 1)$ where $q = |F|$.

2.3 Subrings

Definition 2.6

S is a *subring* of R , denoted $S < R$, if

1. $S \subset R$
2. S is a ring under the same addition and multiplication.

In fact, if $S \subset R$, then $S < R$ iff

1. $0, 1 \in S$

2. $\forall a, b \in S, a + b, -a, ab \in S$

2.4 Direct Products of Rings

Definition 2.7

If R_i is a ring for all $i \in I$, then the direct product of R_i 's, denoted $\prod_{i \in I} R_i$, is defined by

$$\begin{aligned}(x_i)_{i \in I} + (y_i)_{i \in I} &= (x_i + y_i)_{i \in I} \\ (x_i)_{i \in I} (y_i)_{i \in I} &= (x_i y_i)_{i \in I}\end{aligned}$$

The direct product of rings is still a ring. In particular, we can define the finite product of rings.

2.5 Ideals

Definition 2.8

$I \subset R$ is called a left (resp., right) ideal, if

1. $(I, +) < (R, +)$.
2. $RI \subset I$ (resp., $IR \subset I$).

Moreover, I is called an ideal (or two-sided ideal), denoted $I \triangleleft R$, if it is both a left ideal and a right ideal.

An ideal is a subring iff it is the entire ring, since $1 \in I$ will make $r = r1 \in I$ for all $r \in R$.

Example 2.11 If R is a commutative ring, then left ideals, right ideals and ideals coincide.

Example 2.12 $n\mathbb{Z} \triangleleft \mathbb{Z}$.

Definition 2.9

If $S \subset R$, then the ideal generated S , denoted by (S) , is defined by the smallest ideal containing S .

(S) is always an ideal.

Example 2.13 If $a \in R$, then the ideal generated by a is denoted by $(a) = (\{a\})$. These ideals are called principal ideals.

Example 2.14 If R is commutative, $a \in R$, then the principal ideal (a) is Ra .

Example 2.15 If $a_1, \dots, a_n \in R$, then the ideal generated by a_1, \dots, a_n is denoted by $(a_1, \dots, a_n) = (\{a_1, \dots, a_n\})$. These ideals are called finitely generated ideals.

Example 2.16 If R is commutative, $a_1, \dots, a_n \in R$, then the finitely generated ideal (a_1, \dots, a_n) is $Ra_1 + \dots + Ra_n$.

2.6 Ring Homomorphisms and Ring Isomorphisms

Definition 2.10

If R, R' are rings, then $f : R \rightarrow R'$ is a ring homomorphism, if

1. $f(1) = 1'$
2. $\forall a, b \in R, f(a + b) = f(a) + f(b)$
3. $\forall a, b \in R, f(ab) = f(a)f(b)$.

Moreover, f is called a ring isomorphism, if it is a bijective ring homomorphism.

The kernel $\ker(f)$ is an ideal of R , and the image $\text{im}(f)$ is a subring of R' .

If f is a ring isomorphism, then f^{-1} is also a ring isomorphism.

2.7 Quotient Rings

Definition 2.11

If $I \triangleleft R$, then the quotient ring, denoted by $R/I = \{a + I : a \in R\}$, is defined by the well-defined operation

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I \\ (a + I)(b + I) &= (ab) + I\end{aligned}$$



We have that the quotient ring R/I is a ring.

2.8 Isomorphism Theorems of Rings

Proposition 2.3

If $f : R \rightarrow R'$ is a ring homomorphism, then

$$R/\ker(f) \simeq \text{im}(f).$$



Proposition 2.4

If $S \subset R, I \triangleleft R$, then $S + I \subset R, S \cap I \triangleleft S, I \triangleleft S + I$, and

$$S/S \cap I \simeq (S + I)/I.$$



Proposition 2.5

If $I, J \triangleleft G$ and $I \subset J$, then $I \triangleleft J, J/I \triangleleft R/I$, and

$$(R/I)/(J/I) \simeq R/J.$$



The proofs are essentially the same as the isomorphism theorems of groups.

2.9 Operations on Ideals

From now on, I, J, K are assumed to be ideals of R unless otherwise specified. In this section, R is assumed to be commutative.

Definition 2.12

The sum of I and J is defined by $I + J = \{a + b : a \in I, b \in J\}$.



The sum of ideals is an ideal, and it is generated by $I \cup J$, i.e., $I + J = (I \cup J)$.

Definition 2.13

The product of I and J is defined by $IJ = \{a_1b_1 + \cdots + a_nb_n : a_1, \dots, a_n \in I, b_1, \dots, b_n \in J\}$.



The product of ideals is an ideal, and by definition, it is generated by $\{ab : a \in I, b \in J\}$.

Proposition 2.6

We have the following laws of operations on ideals.

1. $I + J = J + I$
2. $IJ = JI$
3. $I + (J + K) = (I + J) + K$
4. $I(JK) = (IJ)K$

5. $I(J + K) = IJ + IK$
6. $I = RI = IR$

Note that the intersection of ideals are still an ideal.

Lemma 2.3

$$IJ \subset I \cap J \subset I + J.$$

Proof The key is that $IJ \subset IR = I$ and $I \cap J \subset I \subset I + J$.

Lemma 2.4

$$(I \cap J)(I + J) \subset IJ.$$

Proof Note that $(I \cap J)(I + J) \subset JI + IJ = IJ$, and we are done.

Definition 2.14

We say I, J are coprime in R , if $I + J = R$, i.e., there exists $a \in I, b \in J$, such that $a + b = 1$.

Proposition 2.7

If I, J are coprime, then $IJ = I \cap J$.

Proof First, $IJ \subset I \cap J$. Also, $I \cap J = (I \cap J)R = (I \cap J)(I + J) \subset IJ$, and we are done.

Example 2.17 $I \cap (J + K) \supset I \cap J + I \cap K$.

Proof It suffices to show $I \cap J \subset I \cap (J + K)$, which is trivial.

Example 2.18 If $J \subset K$, then $I \cap (J + K) = I \cap J + I \cap K$.

Proof If $J \subset K$, then $I \cap (J + K) = I \cap K \subset I \cap J + I \cap K$, and we are done.

2.10 Integral Domain

Definition 2.15

x is called a left (resp., right) zero divisor, if there exists some $y \neq 0$ such that $xy = 0$ (resp., $yx = 0$). Moreover, it is called a zero divisor, or two-sided zero divisor, if it is both a left and right zero divisor.

Definition 2.16

R is called an integral domain, if

1. R is commutative
2. R is not the zero ring, i.e., $0 \neq 1$
3. $\forall x, y \in R, xy = 0 \implies x = 0$ or $y = 0$; Equivalently, R has no nonzero zero divisors.

Example 2.19 A finite integral domain is a field.

Proof Let $a \in R^*$. The map $x \mapsto ax$ is a bijection, since if $ax = bx$, then $(a - b)x = 0$ while $x \neq 0$, so $a = b$. Thus, there is some $b \in R$ such that $ab = ba = 1$. Since R is an integral domain, so $b \in R^*$, and we are done.

2.11 Prime Ideals and Maximal Ideals

Definition 2.17

We say $\mathfrak{p} \triangleleft R$ is a prime ideal, if

1. $\mathfrak{p} \neq R$
2. $\forall x, y \in R, xy \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}$.

Example 2.20 If R is commutative, then R is integral iff (0) is prime.

Definition 2.18

We say $\mathfrak{m} \triangleleft R$ is a maximal ideal, if

1. $\mathfrak{m} \neq R$
2. $\forall I \triangleleft R, I \supset \mathfrak{m} \implies I = R$.

Example 2.21 If R is commutative, then R is integral iff (0) is maximal.

Proof The key is that if $a \in R^*$, then $1 \in (a)$ and thus $(a) = R$.

Example 2.22 The only two ideals of a field are (0) and itself.

Proposition 2.8

Let R be a commutative ring, then

1. \mathfrak{p} is a prime ideal iff R/\mathfrak{p} is an integral domain.
2. \mathfrak{m} is a maximal ideal iff R/\mathfrak{m} is a field.

Proof This can be proved by the previous two examples and the correspondence between ideals in R/I and ideals in R containing I .

Example 2.23 Every field is an integral domain.

Proof Let $a, b \in R^*$. Take a^{-1}, b^{-1} so that $(ab)(a^{-1}b^{-1}) = 1$, so $ab \neq 0$.

Example 2.24 Every maximal ideal is a prime ideal.

Proof If the quotient ring is a field, then it is an integral domain.

Example 2.25 In a finite commutative ring, every prime ideal is maximal.

Proof The quotient ring is a finite integral domain, so it is a field, and we are done.

2.12 The Chinese Remainder Theorem

In this section, R is assumed to be commutative.

Proposition 2.9

If R_1, \dots, R_n are pairwise coprime then the map $R \rightarrow \prod R/I_i$ is surjective. Thus,

$$R / \bigcap_{i=1}^n I_i \simeq \prod_{i=1}^n (R/I_i)$$

Proof It suffices to show $(1, 0, \dots, 0)$ is in the image. The key is to take $a_i \in I_1$ and $b_i \in I_i$ such that $a_i + b_i = 1$ ($2 \leq i \leq n$). Since $b_2 \cdots b_n$ is sent to $(1, 0, \dots, 0)$, so we are done.

Example 2.26 $\mathbb{Z}/(p_1^{\alpha_1} \cdots p_k^{\alpha_k} \mathbb{Z}) \simeq \mathbb{Z}/p_1^{\alpha_1} \mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k} \mathbb{Z}$.

Example 2.27 $\left(\mathbb{Z}/(p_1^{\alpha_1} \cdots p_k^{\alpha_k} \mathbb{Z}) \right)^\times \simeq \left(\mathbb{Z}/p_1^{\alpha_1} \mathbb{Z} \right)^\times \times \cdots \times \left(\mathbb{Z}/p_k^{\alpha_k} \mathbb{Z} \right)^\times$.

Proof These are exactly the units of the previous ring.

Example 2.28 $R \simeq \prod_{i=1}^n (R/I_i) \iff \bigcap_{i=1}^n I_i = \{0\}$.

2.13 Localizations of Rings

In this section, R is assumed to be commutative.

Definition 2.19

S is called a *multiplicative subset*, if

1. $S \subset R^*$
2. S is closed under multiplication.

Example 2.29 R^* is a multiplicative subset (the largest one).

Example 2.30 If \mathfrak{p} is a prime ideal, then $S = R \setminus \mathfrak{p}$ is a multiplicative subset of R .

Definition 2.20

If S is a multiplicative subset, then the *localization of R by S* , denoted $S^{-1}R$, is defined by

$$S^{-1}R = \left\{ \frac{r}{s} : r \in R, s \in S \right\} / \sim$$

where

$$\frac{r}{s} \sim \frac{r'}{s'} \iff \exists t \in S, t(rs' - r's) = 0$$

and

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + sr'}{ss'}$$

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$

The localization is always a commutative ring. The proof is very long, but not hard.

Example 2.31 If R is an integral domain, then

$$\frac{a}{b} \sim \frac{c}{d} \iff ad - bc = 0$$

Definition 2.21

If R is an integral domain, then the *field of fractions of R* , denoted by $\text{Frac}(R)$, is defined by $\text{Frac}(R) = S^{-1}R$ where $S = R^*$.

Example 2.32 The field of fractions of an integral domain is a field.

Example 2.33 \mathbb{Q} is the field of fractions of \mathbb{Z} .

2.14 Principal Ideal Domains

In this section, R is assumed to be commutative.

Definition 2.22

R is called a *principal ideal domain* (abbrev., *PID*), if

1. R is an integral domain.
2. Every ideal of R is principal.

Example 2.34 \mathbb{Z} is a PID.

Proof It suffices to show the only subgroups of \mathbb{Z} are $n\mathbb{Z}$'s.

Example 2.35 Every field is a PID.

Example 2.36 If R is a PID, then every nonzero prime ideal is a maximal ideal.

Proof Let \mathfrak{p} be a prime ideal, but not maximal. Take $\mathfrak{p} = (p) \subsetneq (a) \subsetneq R$, so a is not a unit. Then $p = ab$ for some $b \in R$ where b is not a unit. Since $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, so in any case, one of a, b must be a unit, and we are done.

Example 2.37 \mathbb{Z}_p is a field for prime p .

Proof $p\mathbb{Z}$ is prime, thus maximal in the PID \mathbb{Z} , and we are done.


Example 2.38 Find a PID with an ascending chain of 2000 distinct prime ideals.

Proof Note that $\mathbb{Z}[x_1, \dots, x_{2000}]/[x_1, \dots, x_m]$ is an integral domain for all $1 \leq m \leq 2000$, and we are done.

2.15 Divisions in Integral Domains


In this section, R is assumed to be an integral domain.

Definition 2.23

$x \in R^*$ is called *reducible*, if it can be written as a product of two non-units in R ; otherwise, it is called *irreducible*. 

Definition 2.24

For nonzero elements a, b , we say $a|b$ if there is an element c , such that $b = ac$.


Moreover, we say $a \sim b$, if $a|b$ and $b|a$. 

Example 2.39 If $a, b \neq 0$, then $a|b \iff (b) \subset (a)$.

Example 2.40 $a \sim b \iff (a) = (b) \iff \exists$ a unit $u, a = ub$.

Example 2.41 $|$ is a partial relation, and \sim is an equivalence relation.

Definition 2.25

$p \in R^*$ is called *prime*, if for any $a, b \in R, p|ab \implies p|a$ or $p|b$. 

Example 2.42 $p \in R$ is a prime element, iff $p \neq 0$ and (p) is a prime ideal in R .

Example 2.43 Every prime element is irreducible.

Proof The key is that $p = xy, p|x$ implies that y is a unit.

Example 2.44 In $\mathbb{Z}[\sqrt{-5}]$, 3 is irreducible, but not prime.

2.16 Greatest Common Divisor Domain

In this section, R is assumed to be an integral domain.

Definition 2.26

Let $a, b \neq 0$. We say d is a *greatest common divisor* of a and b , denoted $d = \gcd(a, b)$, if

1. $d|a, d|b$,
 2. $\forall e \in R, (e|a, e|b \implies e|d)$
- 

Similarly, we can define the least common multiple.


Example 2.45 If $a, b \neq 0$, then $\gcd(a, b)$ and $\text{lcm}(a, b)$ are both unique up to a unit.

Example 2.46 If $a, b \neq 0$, and one of $\gcd(a, b)$ and $\text{lcm}(a, b)$ exists, then the other also exists and $\gcd(a, b) \text{lcm}(a, b) \sim ab$.

Proof The key is to use the definition, which is similar to the proof in elementary number theory.

Definition 2.27

R is called a *greatest common divisor domain* (abbrev, *GCD domain*), if

1. R is an integral domain.
 2. For all $a, b \neq 0$, $\gcd(a, b)$ exists.
- 

Example 2.47 Every PID is a GCD domain. In particular, if $a, b \neq 0$, then write $(a) + (b) = (d)$ and $(a) \cap (b) = (m)$ and we will have $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$.

Proof This is again just by definition.

Example 2.48 If p is irreducible and $p \nmid a$, then $\gcd(a, p) = 1$.

Proof Assume $d = \gcd(a, p)$ is a non-unit. Since $d \mid p$, so $d \sim p$. Thus, $p \mid a$, and we are done.

Example 2.49 If R is a UFD, then every irreducible element is a prime.

Proof Assume p is irreducible such that $p \mid ab$. Assume $p \nmid a$, then $\gcd(a, p) = 1$. Write $ax + py = 1$, so $abx + pby = b$. Thus, $p \mid y$, and we are done.

2.17 Unique Factorization Domains

In this section, R is assumed to be an integral domain.

Definition 2.28

R is called a *unique factorization domain* (abbrev., *UFD*), if

1. R is an integral domain.
2. Every nonzero can be written as a product of a unit and finitely many irreducible elements. Moreover, this decomposition is unique in the sense that if it has two decompositions, then the irreducible are the same up to a unit and a rearrangement.

By definition, a UFD is always an integral domain.

Lemma 2.5

In a UFD, irreducible elements are prime.

Proof Assume p is irreducible and $p \mid ab$. We have $px = ab$ for some x . Since R is a UFD, then p must divide either a or b , and we are done.

We may choose a representative in each equivalence class of prime/irreducible elements. Thus, every element x in a UFD is equivalent to a unique factorization into these products, i.e.,

$$x \sim \prod_p p^{v_p(x)}$$

Lemma 2.6

Every UFD is a GCD domain.

Proof The key is to choose $v_p(a, b) = \min(v_p(a), v_p(b))$. All the details are the same as in elementary number theory.

Proposition 2.10

Every PID is a UFD.

Proof First, we show the existence. Let S be the set of element that does not have such a decomposition. We consider the ascending chain of (principal) ideals. The union of ideals in the ascending chain is still an ideal, forcing the chain to terminate in finitely many steps, say (a) . (a) cannot be irreducible, so $a = bc$ for non-unit b, c , and we are done.

Next, we show the uniqueness. The proof is essentially the same as showing the factorization of an integer into primes is unique (by cancelling primes from both sides one by one).

Example 2.50 If R is a UFD such that every nonzero prime ideal is maximal, then every nonzero prime ideal is principal.

Proof Let \mathfrak{p} be a nonzero non-principal prime ideal. If $x = up_1 \cdots p_k \in \mathfrak{p}$, then there is at least one $p_i \in \mathfrak{p}$. If \mathfrak{p} contains some non-multiples of p_i , then it is the entire ring, and we are done.

2.18 Noetherian Rings

Definition 2.29

R is called left (resp., right) Noetherian, if every ascending chain of left (resp., right) ideals terminates in a finitely many steps.

Moreover, R is called Noetherian, if it is both left and right Noetherian.

Example 2.51 Every PID is Noetherian.

Lemma 2.7

R is Noetherian iff every ideal is finitely generated.

Proof If R is Noetherian and I is not finitely generated, then we may have an infinite ascending chain by adding a new element each time to the previous ideal.

If every ideal is finitely generated, and $I_1 \subset I_2 \subset \dots$ is an ascending chain, then their union is an ideal and thus generated by finitely many elements, but all of them must belong to some I_n , and we are done.

Example 2.52 If F is field, then $F[x_1, \dots]$ is not Noetherian.

Proof Note that (x_1, \dots) is not finitely generated, and we are done.

Proposition 2.11 (Hilbert's Basis Theorem)

The polynomial ring over a Noetherian ring is Noetherian.

Example 2.53 $\mathbb{Z}[x_1, \dots, x_n]$ is always Noetherian.

2.19 Artinian Rings

Definition 2.30

R is called left (resp., right) Artinian, if every descending chain of left (resp., right) ideals terminates in a finitely many steps.

Moreover, R is called Artinian, if it is both left and right Artinian.

Example 2.54 \mathbb{Z} is not Artinian, since $(2) \supsetneq (4) \supsetneq \dots$, and we are done.

Proposition 2.12

An Artinian integral domain is a field.

Proof Let $a \neq 0$. Consider $(a) \supset (a^2) \supset \dots$. Say $(a^n) = (a^{n+1})$, then a is a unit, and we are done.

Example 2.55 Find a commutative Artinian ring that is not a field.

Proof Consider $\mathbb{Z}/4\mathbb{Z}$, and we are done.

2.20 Euclidean Domains

Definition 2.31

R is called a Euclidean Domain (abbrev., ED), if

1. R is an integral domain.
2. There exists a map, called a Euclidean map, $f : R \setminus \{0\} \rightarrow \mathbb{N}_0$, such that, for all $a \in R$ and $b \in R \setminus \{0\}$, we can find $q, r \in R$, such that $a = qb + r$ and that either $r = 0$ or $f(r) < f(b)$.

Example 2.56 \mathbb{Z} is an ED, with $f(x) = |x|$.

Lemma 2.8

Every ED is a PID.

Proof The proof is essentially the same as showing that \mathbb{Z} is PID (by using the Euclidean division).

Example 2.57 Every field is an ED.

Proof There are no remainders in any division, and we are done.

Definition 2.32

If R is an integral domain, then $N : R \rightarrow \mathbb{R}^{\geq 0}$ is called a norm, if

1. $N(x) = 0 \iff x = 0$
2. $N(x) = 1 \iff x$ is a unit
3. $\forall a, b \in R, N(ab) = N(a)N(b)$.

Example 2.58 In $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, $N(a + bi) = a^2 + b^2$ is a norm.

Example 2.59 $\mathbb{Z}[i]$ is an ED.

Proof The main idea is to use the division to find the closest point in $\mathbb{Z}[i]$, and show that the remainder is smaller than the divisor.

Example 2.60 $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Proof $3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, where all of the elements are irreducible non-units, and we are done.

2.21 Polynomial Rings

When we are discussing polynomial rings over R , R is always assumed to be commutative.

Definition 2.33

A polynomial over R is a formal notation $f(x) = a_0 + a_1x + \cdots + a_nx^n$ where $a_n \neq 0$, and n is called the degree of f , denoted by $\deg(f)$; equivalently, $f(x) = \sum_{n=1}^{\infty} a_nx^n$ where all but finitely many a_n are zero.

For simplicity, we will use $a_n(f)$ to represent the coefficient before x^n .

Definition 2.34

The polynomial ring over R , denoted by $R[x]$, is defined by

$$\begin{aligned} a_n(f + g) &= a_n(f) + a_n(g) \\ a_n(fg) &= \sum_{i=0}^n a_i(f)a_{n-i}(g). \end{aligned}$$

The polynomial ring is always a commutative ring.

Example 2.61 If $f, g \neq 0$, then $\deg(f + g) \leq \max(\deg(f), \deg(g))$.

Moreover, if $\deg(f) \neq \deg(g)$, then the equality holds.

Example 2.62 If R is an integral domain, and $f, g \neq 0$, then $\deg(fg) = \deg(f) + \deg(g)$.

Example 2.63 If R is an integral domain, then $R[x]$ is also an integral domain.

Example 2.64 Given $a \in R$, then the map $f(x) \mapsto f(a)$ is a ring homomorphism from $R[x]$ to R , called the substitution homomorphism.

Example 2.65 If $f : R \rightarrow R'$ is a ring homomorphism, then the map $R[x] \rightarrow R'[x]$, sending every coefficient to the image under f , is again a ring homomorphism. It is called the ring homomorphism induced by f .

Definition 2.35

$R[x_1, \dots, x_n]$ can be defined inductively by $R[x_1, \dots, x_{n-1}][x_n]$, or otherwise directly by the multivariate polynomials. All the procedure are similar to the univariate polynomials.

We can introduce the multi-index $\alpha = (\alpha_1, \dots, \alpha_n)$. If $x = (x_1, \dots, x_n)$, then we define $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Every multivariate polynomial can be written as $f(x) = \sum_{\alpha} a_{\alpha} x^{\alpha}$ where all but finitely many a_{α} are zero.

$R[x_1, \dots, x_n]$ are always commutative rings.

2.22 Polynomial Rings over Fields

In this section, F are assumed to be fields.

Lemma 2.9

$F[x]$ is a PID.

Proof We take the degree to be the Euclidean map. This is proved directly by the algorithm of long division of polynomials. The key is that the leading coefficient is nonzero, thus a unit.

Example 2.66 $\mathbb{R}[x_1, \dots, x_n]$ is not a PID.

Proof Note that (x_1, \dots, x_n) cannot be generated by one element, and we are done.

2.23 Polynomial Rings over Unique Factorization Domains

In this section, R is assumed to be a UFD.

Definition 2.36

The content of a polynomial $f(x)$, denoted $\text{cont}(f)$, is defined by the greatest common divisor of all the coefficients.

Definition 2.37

$f(x)$ is called primitive, if $\text{cont}(f) = 1$.

Example 2.67 Every $f(x) \in R[x]$ can be written as a constant and a primitive polynomial.

Proof Note that $\frac{\gcd(a_0, \dots, a_n)}{\text{cont}(f)} = \gcd\left(\frac{a_0}{\text{cont}(f)}, \dots, \frac{a_n}{\text{cont}(f)}\right)$, and we are done.

Proposition 2.13 (Gauss's Lemma)

The product of primitive polynomial is still primitive.

Proof If $\text{cont}(f) = \text{cont}(g) = 1$ but $\text{cont}(fg) \neq 1$, then take $p \mid \text{cont}(fg)$. The key is to take the smallest i, j such that $p \nmid a_i(f)$ and $p \nmid a_j(g)$. Then $p \mid a_{i+j}(fg)$ and we are done.

Example 2.68 If $f, g \neq 0$, then $\text{cont}(fg) = \text{cont}(f) \text{cont}(g)$.

Proposition 2.14

The polynomial ring over a UFD is a UFD.

Example 2.69 If R is a UFD, then $R[x_1, \dots, x_n]$ is a UFD.

2.24 Rings of Formal Power Series

In this section, R is assumed to be commutative.

Definition 2.38

The ring of formal power series over R , denoted $R[[x]]$, is defined by $R[[x]] = \{f(x) = \sum_n a_n x^n\}$ where the operations are essentially the same as those in $R[x]$.

Clearly, $R[x] \subset R[[x]]$. Also, $R[[x]]$ is always a commutative ring. Moreover, if R is an integral domain, then so is $R[[x]]$.

Example 2.70 The invertible elements in $R[[x]]$ are those with invertible a_0 in R .

Proof On one hand, consider $a_0 b_0 = 1$. On the other hand, if a_0 is invertible, we can deduce the coefficient of the reciprocal by an easily-found algorithm.

Example 2.71 $\mathbb{R}[[x]]$ is not a field.

Proof Note that x is not invertible, and we are done.

Example 2.72 Give a counterexample to the statement: the ring of formal power series over a PID is a PID.

Proof Note that $(2, x)$ is not a principal domain over \mathbb{Z} , and we are done.

2.25 Eisenstein's Criterion

Proposition 2.15 (Eisenstein's Criterion)

Let R be a UFD and $F = \text{Frac}(R)$. If $f(x) \in R[x]$ is a non-constant polynomial, $n = \deg(f)$, and p is prime in R such that $p|a_0, \dots, a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$, then $f(x)$ is irreducible in $F[x]$.

Proof The key is that if $gh = f$, then we may assume $p \nmid b_0$ and $p|a_0$, and by induction all b_k are multiples of p , and we are done.

Example 2.73 If a primitive polynomial f satisfies the Eisenstein's condition, then it is irreducible in $R[x]$.

2.26 Nilradicals of Rings

In this section, R is assumed to be commutative.

Definition 2.39

The nilradical of R , denoted $\text{Nil}(R)$, consists of all nilpotent elements of R .

The nilradical is always an ideal.

Proposition 2.16

The nilradical is the intersection of all prime ideals in R .

Proof On one hand, if $a \in \text{Nil}(R) \setminus \mathfrak{p}$ for some \mathfrak{p} , then $0 = a^n \notin \mathfrak{p}$ for some $n \in \mathbb{N}_1$, and we are done.

On the other hand, let $x \notin \text{Nil}(R)$. We can take the maximal ideal \mathfrak{m} among those ideals J such that $x^n \notin J$ for all $n \in \mathbb{N}_1$, by Zorn's lemma. \mathfrak{m} is prime since if $ab \in \mathfrak{m}$, $a, b \notin \mathfrak{m}$, then we can have $x^m \in \mathfrak{m} + (a)$ and $x^n \in \mathfrak{m} + (b)$ for some a, b , but this will lead to the fact that $x^{m+n} \in \mathfrak{m} + (ab) = \mathfrak{m}$. Thus, x is not in this prime ideal \mathfrak{m} , and we are done.

Example 2.74 $f(x)$ is invertible in $R[x]$ iff the constant term is invertible and all the other coefficients are nilpotent.

Proof If R is an integral domain, then f is invertible iff a_0 is invertible, and all other a_n are 0. Given any prime ideal \mathfrak{p} and $n \geq 1$, R/\mathfrak{p} is an integral domain, so $a_n \in \mathfrak{p}$ in every \mathfrak{p} , thus a_n is nilpotent.

On the other hand, if f satisfies this condition, then for some large n , f^n is an invertible constant, and we are done.

2.27 The Radicals of Ideals

In this section, R is assumed to be commutative.

Definition 2.40

The radical of an ideal I , denoted by $\text{Rad}(I)$, is defined by $\text{Rad}(I) = \sqrt{I} = \{a \in R : \exists n, a^n \in I\}$.

The radical of I is always an ideal, since it is precisely the preimage of the nilradical of R/I under the canonical homomorphism.

Example 2.75 $I \subset \text{Rad}(I)$.

Definition 2.41

I is called *primary*, if for all $a, b \in R$, we have $ab \in I \implies a \in I$ or $b \in \text{Rad}(I)$.

Example 2.76 Every prime ideal is primary.

Example 2.77 If I is prime, then $\text{Rad}(I) = I$.

Proof If $a^n \in I$, then $a \in I$, and we are done.

Example 2.78 Show that I is prime iff $I = \text{Rad}(I)$ and I is primary.

Proof It suffices to show the second direction. Assume $I = \text{Rad}(I)$ and I is primary. Let $a, b \in I$, then $a \in I$ or $b \in \text{Rad}(I) = I$, and we are done.

2.28 The Jacobson Radicals of Ring

In this section, R is assumed to be commutative.

Definition 2.42

The *Jacobson radical* of R , denoted $J(R)$, is defined by the intersection of all maximal ideals.

By definition, $J(R) \supset \text{Nil}(R)$.

2.29 More Exercises

Example 2.79 Show $\{f \in \mathbb{R}[x] : a_0(f) \in \mathbb{Q}\}$ is not Noetherian.

Proof Note that $(x) \subsetneq (x, \pi x) \subsetneq (x, \pi x, \pi^2 x) \subsetneq \dots$, and we are done.

Example 2.80 Give a counterexample to the statement: every subring of a PID is a PID.

Proof Note that $k[x_1, \dots] \subset k(x_1, \dots)$, and we are done.

Note that $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ and we are done.

Example 2.81 Give a counterexample to the statement: the quotient ring of a PID is a PID

Proof Note that $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, and we are done.

Example 2.82 Give a counterexample to the statement: the polynomial ring over an ED is an ED.

Proof Note that $\mathbb{R}[x, y]$ is not Euclidean, and we are done.

Example 2.83 Find invertible elements and zero divisors of $\left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$.

Proof We use (a, b, c) to represent the matrix. Then we have $(a, b, c)(d, e, f) = (ad, ae + bd, af + be + cd)$, and the multiplicative identity is $(1, 0, 0)$.

Invertible elements: It suffices to let $a = \pm 1$ to have determinant equal to 1, so invertible elements are $(\pm 1, b, c)$ where $b, c \in \mathbb{Z}$.

Zero divisors (left zero divisors): by linear algebra and taking the determinant, the zero divisors are $(0, b, c)$ where $b, c \in \mathbb{Z}$.

Example 2.84 Show that R is a PID iff it is a UFD and for every $a, b \neq 0$, $\gcd(a, b) \in (a, b)$.

Proof It suffices to show the second direction. Let I be an ideal. Take any $a \in I \setminus \{0\}$ and do the prime factorization. Among all the elements dividing a , take the smallest one, in the sense of the \gcd of all the elements. Then this element must generate the entire I .

Example 2.85 Find all the irreducible elements in $\mathbb{Z}[i]$.

Proof Let π be an irreducible element. If $N(\pi) = p$, then we are done, so $\pi = a + bi$ where $a^2 + b^2$ is a prime.

If $p|N(\pi)$ and $p \equiv 3 \pmod{4}$, then $p|\pi\bar{\pi}$, so $p|\pi$. In this case, $p \equiv 3 \pmod{4}$ is a prime in $\mathbb{Z}[i]$, and then $\pi \sim p$.

If $N(\pi)$ is a product of some $p \equiv 1 \pmod{4}$, then we can find $z \in \mathbb{Z}[i]$ such that $z|z\bar{z} = p|N(\pi)$ where z is a prime and $z \sim \pi$, and we are done.

Example 2.86 If R is a commutative ring such that for each $a \in R$, there exists some $n \geq 2$ such that $a^n = a$, then every prime ideal of R is maximal.

Proof Let \mathfrak{p} be a prime ideal, and take $\bar{a} = a + \mathfrak{p} \neq \bar{0}$ (i.e., $a \notin \mathfrak{p}$). R/\mathfrak{p} is an integral domain, so $\overline{aa^{n-1}} = \bar{a}$ implies $\overline{aa^{n-2}} = \bar{1}$. Thus, R/\mathfrak{p} is a field, and we are done.

Example 2.87 Let R be a Noetherian integral domain with the property that for all ideals $a \subset b \subset R$, we have an ideal c such that $a = bc$. Then we have the following properties.

1. If $x \neq 0$ and $(x)a = (x)b$, then $b = c$.

Proof If $y \in a$, then $xy = xrb$ for some $r \in R$, and we are done.

2. If $x \in a$, then $(x) = ab$ for some ideal b .

Proof This is true directly by the assumptions.

3. If $a \neq 0$ and $ab=ac$, then $b=c$.

Proof Take $x \in a$ and $(x) = ad$, and we are done.

4. Every nonzero prime ideal is maximal.

Proof Assume a prime ideal $\mathfrak{p} \subsetneq I$, so $\mathfrak{p} = IJ$. Take $i \in I \setminus \mathfrak{p}$, and $j \in J$. Since $ij \in \mathfrak{p}$, so $j \in \mathfrak{p}$. Thus, $\mathfrak{p} = IJ \subset J \subset \mathfrak{p}$, and then $\mathfrak{p} = \mathfrak{p}R = \mathfrak{p}I$. Therefore, $I = R$, and we are done.

5. Every nontrivial ideal a can be decomposed into a prime ideal \mathfrak{p} and an ideal $a \subsetneq b$ such that $a = \mathfrak{p}b$.

Proof This can be proved by Zorn's lemma and note that R is Noetherian.

6. Every nonzero ideal can be factored into finitely many prime ideals

Proof By Induction and note that R is Noetherian, we are done.

7. Prove that the factorization into prime ideals is unique up to a rearrangement.

Proof Cancel all the prime divisors one by one, and we are done.

Chapter 3 Module Theory

In this section, R is assumed to be a commutative ring unless otherwise specified.

3.1 Modules

Definition 3.1

M is called a left R -module, if there is map $R \times M \rightarrow M$ such that for all $m, n \in M$ and $a, b \in R$, we have

1. $(M, +)$ is an abelian group
2. $1m = m$
3. $a(bm) = (ab)m$
4. $a(m + n) = am + an$
5. $(a + b)m = am + bm$.

Example 3.1 A module over a field is exactly a vector space over this field.

Example 3.2 If $I \triangleleft R$, then I is a module over R .

Example 3.3 If $I \triangleleft R$, then R/I is a module over R .

Example 3.4 If V is a vector space over F , and $T : V \rightarrow V$ is linear, V is a module over $F[x]$, by defining $(\sum_n a_n x^n) v = \sum_n a_n T^n(v)$

Example 3.5 The set of $n * n$ matrices over R , denoted $M_n(R)$, is a module over R .

From now on, M is assumed to be a left R -module, unless otherwise specified.

3.2 Submodules

Definition 3.2

We say N is a submodule of M , denoted $N < M$, if

1. $N \subset M$
2. N is a module under the same operations.

If $N \subset M$, then N is a submodule iff N is preserved under addition and scalar multiplication.

Example 3.6 If V is a vector space over a field F , then every submodule is exactly a vector subspace over F .

Example 3.7 If $n \in \mathbb{N}_1$, then $n\mathbb{Z}$ is a submodule of \mathbb{Z} .

3.3 Module Homomorphisms and Module Isomorphisms

Definition 3.3

If M, M' are two left R -modules, then $f : M \rightarrow M'$ is a module homomorphism, if

1. $\forall m, n \in M, f(m + n) = f(m) + f(n)$
2. $\forall r \in R, \forall m \in M, f(rm) = rf(m)$

Moreover, $f : M \rightarrow M'$ is a module isomorphism, if f is a bijective module homomorphism.

Example 3.8 If V, V' are vector spaces over a field F , then every linear map from V to V' is exactly a module homomorphism.

The kernel $\ker(f)$ is a submodule of M , and the image $\text{im}(f)$ is submodule of M' .

Definition 3.4

The set of R -module homomorphisms from M to M' forms an R -module, denoted by $\text{Hom}_R(M, M')$ and defined by

$$\begin{aligned}(f + g)(m) &= f(m) + g(m) \\ (rf)(m) &= rf(m)\end{aligned}$$



Example 3.9 $\text{Hom}_R(R, M) \simeq M$.

Proof The key is that every $f : R \rightarrow M$ is uniquely determined by $f(1)$. We may define $\phi : M \rightarrow \text{Hom}(R, M)$ by $(\phi(m))(r) = rm$, and we are done.

Example 3.10 $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \simeq \mathbb{Z}_d$, where $d = \gcd(m, n)$.

3.4 Quotient Modules

Definition 3.5

If N is a submodule of M , then the quotient module, defined by M/N , is defined by

$$\begin{aligned}(a + N) + (b + N) &= (a + b) + N \\ r(a + N) &= ra + N.\end{aligned}$$



The quotient module is always a module.

Example 3.11 $\mathbb{Z}/n\mathbb{Z}$ is a module over \mathbb{Z} . For simplicity, we denote $\mathbb{Z}/n\mathbb{Z}$ by \mathbb{Z}_n .

3.5 Isomorphism Theorems of Modules

Proposition 3.1

If $f : M \rightarrow M'$ is a module homomorphism, then

$$M/\ker(f) \simeq \text{im}(f).$$

**Proposition 3.2**

If $A, B < M$, then $A + B < M$, $A \cap B < B$, $A < A + B$, and

$$(A + B)/A \simeq B/(A \cap B).$$

**Proposition 3.3**

If $A < B < M$, then $A < M$, $B/A < M/A$, and

$$(M/A)/(B/A) \simeq M/B.$$



The proofs are essentially the same as the isomorphism theorems of groups.

3.6 Direct Products of Modules

Definition 3.6

If M_i is a module for all $i \in I$, then the direct product of M_i 's, denoted $\prod_{i \in I} M_i$, is defined by

$$\begin{aligned}(x_i)_{i \in I} + (y_i)_{i \in I} &= (x_i + y_i)_{i \in I} \\ r(x_i)_{i \in I} &= (rx_i)_{i \in I}\end{aligned}$$



The direct product of modules is still a module. In particular, we can define the finite product of modules.

3.7 Direct Sums of Modules

Definition 3.7

If M_i is a module for all $i \in I$, then the direct sum of M_i 's, denoted $\bigoplus_{i \in I} M_i$, is defined by the submodule of $\prod_{i \in I} M_i$ which contains all $(x_i)_{i \in I}$ where all but finitely many x_i 's are zero.

The direct sum of modules is still a module. In particular, we can define the finite sum of modules.

Example 3.12 If $m, n \in \mathbb{N}_1$ and $\gcd(m, n) = 1$, then $\mathbb{Z}_m \oplus \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$.

Proof Define $f : \mathbb{Z}_m \oplus \mathbb{Z}_n \rightarrow \mathbb{Z}_{mn}$ by $f(a + m\mathbb{Z}, b + n\mathbb{Z}) = ab + mn\mathbb{Z}$. This is a well-defined surjective module homomorphism, and we are done.

3.8 Tensor Products of Modules

In this section, M, N are assumed to be R -modules.

From now on, an R -linear map is an R -module homomorphism, unless otherwise specified.

Definition 3.8

The tensor product of R -modules M, N , denoted by $M \otimes_R N$, is defined by $(M \oplus N)/K$, where K is a submodule defined by

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$

$$(rm, n) - r(m, n)$$

$$(m, rn) - r(m, n)$$

The tensor product of R -modules is always an R -module.

Example 3.13 If $m, n \in \mathbb{N}_1$ and $d = \gcd(m, n)$, then $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_d$.

Proof The map $a + m\mathbb{Z} \oplus b + n\mathbb{Z} \mapsto ab + d\mathbb{Z}$ is well-defined and linear, essentially because $a \oplus b = ab(1 \otimes 1)$. It has a well-defined inverse which is $c + d\mathbb{Z} \rightarrow c(1 \otimes 1)$, and we are done.

Example 3.14 If $\gcd(m, n) = 1$, then $\mathbb{Z}_m \otimes \mathbb{Z}_n \simeq \mathbb{Z}_1 \simeq 0$.

Example 3.15 $\mathbb{Z}_{12} \otimes \mathbb{Z}_{90} \simeq \mathbb{Z}_6$.

Example 3.16 The map $\pi : (x, y) \mapsto x \otimes y$ is a surjective R -linear map from $M \oplus N$ to $M \otimes N$.

Proof This is the canonical map, and we are done.

Definition 3.9

The map $f : M \oplus N \rightarrow L$ is called R -bilinear, if

1. For each $m \in M$, $n \mapsto f(m, n)$ is R -linear.
2. For each $n \in N$, $m \mapsto f(m, n)$ is R -linear.

Proposition 3.4 (The Universal Property of the Tensor Products of Modules)

For each R -bilinear map $f : M \oplus N \rightarrow L$, there is a unique map $g : M \otimes N \rightarrow L$ such that $f = g \circ \pi$.

Proof Clearly, we have to define $g(a \otimes b) = f(a, b)$. It suffices to show g is a well-defined R -linear map. The well-definedness comes from the definition of tensor product together with the R -bilinearity. The R -linearity comes from the R -bilinearity of f , and we are done.

Lemma 3.1

1. $M \otimes N \simeq N \otimes M$
2. $M \otimes (N \otimes L) \simeq (M \otimes N) \otimes L$
3. $M \otimes (N \oplus L) \simeq M \otimes N \oplus M \otimes L$
4. $M \otimes R \simeq M$.



Proof Using the universal property, all of these are easy to check.

Example 3.17 $\text{Hom}_R(M \otimes_R N, L) \simeq \text{Hom}_R(M, \text{Hom}_R(N, L))$.

Proof This is again easily checked by using the universal property.

Example 3.18 Let R be an integral domain and $Q(R) = \text{Frac}(R)$, the field of fractions of R . Then $Q(R) \otimes_R R^n \simeq Q(R)^n$.

Proof By the distributive law, $Q(R) \otimes_R R^n = (Q(R) \otimes_R R)^n \simeq Q(R)^n$.

Example 3.19 Find the tensor product of the $\mathbb{C}[x]$ -modules $\mathbb{C}[t, t^{-1}]$ and \mathbb{C} , where t acts on the second module by 0.

Proof Note that $p(t) \otimes r = t^{-1}p(t) \otimes tr = 0$, and we are done.

3.9 Torsion Modules

Definition 3.10

M is called a *torsion module*, if for every $m \in M$, there exists $r \in R \setminus \{0\}$ such that $rm = 0$.



Example 3.20 If $n \in \mathbb{N}_1$, then \mathbb{Z}_n is a torsion module over \mathbb{Z} .

Example 3.21 If $n \in \mathbb{N}_1$, then $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Lemma 3.2

Let R be an integral domain and $Q(R) = \text{Frac}(R)$, the field of fractions of R . If M is a torsion module, then $M_{Q(R)} = M \otimes_R Q(R) = 0$.



Proof Let $m \otimes_R q \in M \otimes_R Q(R)$. Take $r \in R \setminus \{0\}$ such that $0 = rm$. Then $m \otimes_R q = rm \otimes_R r^{-1}q = 0 \otimes_R r^{-1}q = 0$, and we are done.

3.10 Torsion-free Modules

Definition 3.11

M is called *torsion-free*, if for all $r \in R$ and $m \in M$, $rm = 0 \implies r = 0$ or $m = 0$.



Note that the notion of torsion-free modules is very similar to the notion of integral domains.

3.11 Pure Submodules

Definition 3.12

Assume R is commutative, then $N < M$ is called *pure*, if for all $r \in R$, $rN = N \cap rM$.



Example 3.22 Every direct summand of M is pure.

Proof One direction is trivial. The key to the other direction is that $n = rm = rm' + rm''$, and we are done.

Example 3.23 If R is an integral domain, and M/N is torsion-free, then N is pure.

Proof Write $n = rm$. Then $\overline{rm} = \overline{0}$, so $r = 0$ or $m \in N$, and we are done.

Example 3.24 If R is an integral domain, M is torsion-free and N is pure, then M/N is torsion-free.

Proof If $rm = n \in N$, then $n = rn'$ for some $n' \in N$. Assume $r \neq 0$. Then $r(m - n') = 0$, so $m = n'$, and we are done.

3.12 Finitely Generated Modules

Definition 3.13

We say M is *finitely generated*, if there exists a_1, \dots, a_m such that $M = Ra_1 + \dots + Ra_m$.
In particular, if M is generated by an element, then M is called a *cyclic module*.

Example 3.25 If V is a vector space over a field F , then V is finitely generated as a module iff it is a finite-dimensional space over F .

Example 3.26 The quotient module of a cyclic module is cyclic.

Proof Assume $M = Ra$, and $N < M$. Then $M/N = \{x+M : x \in M\} = \{ra+M : r \in R\} = \{r(a+M) : r \in R\} = R(a+M)$, and we are done.

Definition 3.14

Let $x \in M$, then the *annihilator of x* , denoted $\text{Ann}(x)$, is defined by $\text{Ann}(x) = \{r \in R : rx = 0\}$.

$\text{Ann}(x)$ is always an ideal in R .

Example 3.27 If $M = Ra$ (i.e., it is cyclic), then $M \simeq R/\text{Ann}(x)$.

Proof Note that $r \mapsto ra$ is R -linear, and we are done.

3.13 Simple Modules

Definition 3.15

M is called *simple* (or *irreducible*), if $M \neq 0$, and the only submodules of M are 0 and itself.

Example 3.28 A simple module over a field is exactly a 1-dimensional subspaces over the field.

Example 3.29 If f is an R -linear map between simple modules M and M' , then f is either zero or an isomorphism.

Proof It suffices to separate the kernel into two cases.

Example 3.30 Every simple module is cyclic.

Proof Take any $a \neq 0$. Then $M = Ra$, and we are done.

Example 3.31 M is simple iff M is isomorphic to some R/I where I is a maximal ideal in R .

Proof On one hand, write $M = Ra$ where $a \neq 0$. Then $M \simeq R/I$ where $I = \text{Ann}(a)$. Let $r \in R \setminus \text{Ann}(a)$. Since $ra \neq 0$, so $M = R(ra) = Ra$. Thus, there exists $s \in R$ such that $(sr - 1)a = 0$, and we are done.

On the other hand, it suffices to show that if R/I is a field, then it is simple as an R -module. Let $N < R/I$ be a nonzero submodule. Take any $a + I \in N$ where $a \notin I$. We can take $b \in R$ such that $b(a + I) = ab + I = 1 + I$. Thus, $N = R/I$, and we are done.

Example 3.32 The only isomorphism class of simple $\mathbb{C}[x]$ -modules is the isomorphism class of \mathbb{C} .

Proof Note that the maximal ideals in \mathbb{C} have the form $(x - a)$, and we are done.

3.14 Semisimple Modules

Definition 3.16

M is called *semisimple*, if it can be written as a direct sum of simple modules.

Example 3.33 Let A be an $n \times n$ matrix over \mathbb{C} . Consider \mathbb{C}^n as a $\mathbb{C}[x]$ -module, by defining $x \cdot v = Av$. Then it is semisimple iff A is diagonalizable.

Proof Note that the only $\mathbb{C}[x]$ -module is \mathbb{C} itself, so \mathbb{C}^n is a $\mathbb{C}[x]$ -module iff it has a basis (v_1, \dots, v_n) such that $Av_i \in \mathbb{C}v_i$, i.e., iff A is diagonalizable.

Example 3.34 The previous result is not true for \mathbb{R} .

Proof Consider $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and we are done.

3.15 Free Modules

Definition 3.17

M is called a *free module over R* , if there is a basis of M over R , i.e., a linearly independent list which generates M .

Example 3.35 Every finite-dimensional space over a vector space is a free module.

3.16 Projective Modules

Definition 3.18

P is called a *projective module*, if for every surjective homomorphism $f : N \rightarrow M$ and every homomorphism $g : P \rightarrow M$, there is a homomorphism $h : P \rightarrow N$ such that $g = fh$.

Example 3.36 Every free module is projective.

Proof For each basis element in P , pick an element in M and then an element in N , and we are done.

3.17 Fundamental Theorem of Finitely Generated Modules over Principal Ideal Domains

In this section, R is assumed to be a principal ideal domain.

Proposition 3.5 (Invariant Factor Decomposition)

If M is a finitely generated module over R , then there is a unique decreasing sequence of proper ideals (up to some units) $(d_1) \supset \cdots (d_n)$, such that

$$M \simeq \bigoplus_i R/(d_i) \simeq R/(d_1) \oplus \cdots R/(d_n).$$

In particular, this means that $d_1 | \cdots | d_n$. The d_i 's not equal to 1 are called *invariant factors*, the number of 1's among d_i 's are called the *free rank*.

Proposition 3.6 (Primary Decomposition)

If M is a finitely generated module over R , then there are unique primary ideals q_1, \dots, q_m such that

$$M \simeq \bigoplus_i R/(q_i) \simeq R/(q_1) \oplus \cdots R/(q_m).$$

In a PID, every primary ideal (q_i) is either equal to $(p_i^{k_i}) = (p_i)^{k_i}$ where p_i is a prime element and $k_i \geq 1$, or equal to (0) .

Thus, another notation is that

$$M \simeq R^f \oplus \bigoplus_i R/(p_i^{k_i}) \simeq R^f \oplus R/(p_1^{k_1}) \oplus \cdots R/(p_m^{k_m}).$$

These $q_i = p_i^{k_i}$'s are called the *elementary divisors* of this module.

Example 3.37 Decompose $(\mathbb{Z}_2 \oplus \mathbb{Z}_3) \otimes (\mathbb{Z}_4 \oplus \mathbb{Z}_6)$ into a direct sum of cyclic groups.

Proof This is isomorphic to $\mathbb{Z}_6 \otimes (\mathbb{Z}_4 \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_6 \otimes \mathbb{Z}_4 \oplus \mathbb{Z}_6 \otimes \mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6$.

Example 3.38 Decompose $\mathbb{Z}_{12} \oplus \mathbb{Z}_{90}$ into a direct sum of cyclic groups with each factor a divisor of the order of the next, in the usual way.

Proof $\mathbb{Z}_{12} \oplus \mathbb{Z}_{90} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_6 \oplus \mathbb{Z}_{180}$.

Example 3.39 Decompose $\mathbb{Z}_{12} \otimes \mathbb{Z}_{90}$ into a direct sum of cyclic groups with each factor a divisor of the order of the next, in the usual way.

Proof $\mathbb{Z}_{12} \otimes \mathbb{Z}_{90} \simeq \mathbb{Z}_6$, and we are done.

Example 3.40 Decompose $\mathbb{Z}_{20} \oplus \mathbb{Z}_{90}$ into a direct sum of cyclic groups with each factor a divisor of the order of the next, in the usual way.

Proof $\mathbb{Z}_{10} \oplus \mathbb{Z}_{180}$.

Example 3.41 Decompose $\mathbb{Z}_{20} \otimes \mathbb{Z}_{90}$ into a direct sum of cyclic groups with each factor a divisor of the order of the next, in the usual way.

Proof $\mathbb{Z}_{20} \otimes \mathbb{Z}_{90} \simeq \mathbb{Z}_{10}$, and we are done.

Lemma 3.3

$$U(\mathbb{Z}_{2^k}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}.$$

Example 3.42 Decompose $U(\mathbb{Z}_{60})$ into a direct sum of cyclic groups with each factor a divisor of the order of the next, in the usual way.

Proof $U(\mathbb{Z}_{60}) \simeq U(\mathbb{Z}_4) \times U(\mathbb{Z}_3) \times U(\mathbb{Z}_5) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, and we are done.

Example 3.43 Consider the subspace of $\mathbb{C}[x, y]$ spanned by $1, x, y, x^2, xy, y^2$. Consider $T = \partial/\partial x + \partial/\partial y$. Find the invariant factors and elementary divisors of T .

Proof Using the Smith Normal Form, we can find that the only invariant factor and the only elementary divisor is 2.

Example 3.44 Consider the subspace of $P_3 = P_3(R)$ spanned by $1, x, x^2, x^3$. Consider $T = (x^2 + x)f_{xx} - 4xf_x + 3f$. Find the invariant factors and elementary divisors of T .

Proof Using the Smith Normal Form, we can find that the free rank is 1, and the invariant factors are 3, 3, 9. Thus, the elementary divisors are also 3, 3, 9, and we are done.

Example 3.45 Classify the $\mathbb{F}_2[x]$ -modules such that $\dim_{\mathbb{F}_2[x]} M = 2$.

Proof Consider the irreducible polynomials of degree at most 2 in $\mathbb{F}_2[x]$. They are $x, x+1, x^2+x+1$. Thus M is isomorphic to $\mathbb{F}_2[x]/(x^2+x+1)$ or $\mathbb{F}_2[x]/(x) \oplus \mathbb{F}_2[x]/(x)$ or $\mathbb{F}_2[x]/(x) \oplus \mathbb{F}_2[x]/(x+1)$ or $\mathbb{F}_2[x]/(x+1) \oplus \mathbb{F}_2[x]/(x+1)$.

3.18 Jordan Canonical Form

In this section, F is assumed to be an algebraically closed field (i.e., every polynomial has a root in this field), V is assumed to be a finite-dimensional vector space over F (i.e., $V \simeq F^n$ for some $n \in \mathbb{N}_1$), and T is assumed to be a linear map from V to V .

Let $R = F[x]$. We consider the $F[x]$ -module V where $x \cdot v = Tv$.

Proposition 3.7 (Jordan Canonical Form)

Under the previous assumptions, $V \simeq F[x]/(x - \lambda_1)^{k_1} \oplus \cdots \oplus F[x]/(x - \lambda_m)^{k_m}$ where $k_1, \dots, k_m \geq 1$.

Proof Note that the prime ideals are exactly the maximal ideals, i.e., of the form $(x - \lambda)$ where $\lambda \in F$ and that if the free rank is at least 1, then V will be infinite dimensional.

Example 3.46 If $A^n = I$, then A is diagonalizable.

Proof Note that every eigenvalue is a root of the separable polynomial $x^n - 1$, and we are done.

3.19 Characteristic Polynomials and Minimal Polynomials

In this section, F is assumed to be a field, and A is assumed to be an $n \times n$ matrix over F .

Definition 3.19

The characteristic polynomial of A over F , denoted by char_A , is defined by

$$\text{char}_A(x) = \det(A - xI)$$

Note that the eigenvalues of A are exactly the roots of $\text{char}(A)$.

Lemma 3.4

$$\text{char}_A(A) = 0.$$

Proof Let (e_1, \dots, e_n) be a basis of F^n , say. Let E be the matrix where column vectors are e_i 's. Consider the $F[x]$ -module, defined by $x \cdot v = Av$. Then $(xI - A)E = 0$. By multiplying the adjugate matrix, we get $\det(xI - A)I \cdot E = \text{char}_A(x)I \cdot E = 0$. In particular, this means that $\text{char}_A(x) \cdot e_j = \text{char}_A(A)e_j = 0$ for all j . Then $\text{char}_A(A) = 0$, and we are done.

Definition 3.20

The minimal polynomial of A over F , denoted by m_A , is defined by the monic polynomial p with the smallest degree such that $p(A) = 0$.

Lemma 3.5

The minimal polynomial must divide the characteristic polynomial.

Proof By the division algorithm, this is trivial.

3.20 Rational Canonical Form

In this section, F is assumed to be a field, and A is assumed to be an $n \times n$ matrix over F .

Definition 3.21

Let d be a polynomial over F where $d(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$. Define

$$C(d) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & & & \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Proposition 3.8 (Rational Canonical Form)

Consider the $F[x]$ -module as defined in the previous sections where $x \cdot v = Av$. Then A is similar to $D[C[d_1], \dots, C[d_m]]$ which denotes the matrix consisting of the diagonal blocks $C[d_1], \dots, C[d_m]$, where $d_1 | \dots | d_m$, $d_1 \cdots d_m = \text{char}_A$, and $d_m = m_A$. Also, $V \cong F[x]/(d_1) \oplus \dots \oplus F[x]/(d_m)$, which is in the invariant factor form.

Proof This can be done by considering $x \cdot v = m_A(x)v$ together with the structure theorem for modules over a PID where $F[x]$ is the PID.

Example 3.47 If $\dim_F V = 3$, classify all non-similar linear transformations $T : V \rightarrow V$ such that $T^2(T - 1) = 0$. Find those that have $\dim \ker(T) = 1$.

Proof By the primary decomposition, since x and $x - 1$ are different prime elements in $F[x]$, so there are two cases, where $T \sim D[C(x^2(x - 1))]$ or $T \sim D[C(x), C(x(x - 1))]$. It is to check that only the first one satisfies that $\dim \ker(T) = 1$, and we are done.

Example 3.48 Consider the usual $F[x]$ -module where $x \cdot v = T(v)$ where V is an n -dimensional vector space over F and $T : V \rightarrow V$ is a linear transformation. Take (e_1, \dots, e_n) to be a basis of $F[x]^n$. Consider the $F[x]$ -linear map

$\pi : F[x]^n \rightarrow V$ where $p(x) \cdot e_j = p(T)e_j$. Show that $\ker(\pi)$ has dimension at most n .

Proof Assume f_1, \dots, f_{n+1} are linearly independent, such that $f_i(T) = 0$ for all i . Since the minimal polynomial m_T has degree at most n , so we may assume that f_1, \dots, f_{n+1} has dimension at most $n - 1$, and we are done.

Example 3.49 Give a counterexample to the statement: if two real 4×4 matrices have the same characteristic polynomial and minimal polynomial, then they have the same rational canonical form.

Proof Consider $D(C(x^2), C(x^2))$ and $D(C(x^2), C(x), C(x))$, and we are done.

Example 3.50 Give a counterexample to the statement: if A, B are 5×5 real matrices with the same minimal polynomial $p(t) = t(t - 4)^3$, then they are similar.

Proof Consider $D(C(x), C(x(x - 4)^3))$ and $D(C(x - 4), C(x(x - 4)^3))$, and we are done.

3.21 More Exercises

Example 3.51 Find ideals in $\mathbb{Z}[x]/(2, x^3 + 26)$.

Proof The ring is $\mathbb{F}_2[x]/(x^3)$ and the units are $1, x + 1, x^2 + 1, x + 2 + x + 1$. If an ideal I is not the entire ring, then $I \subset \{0, x, x^2, x^2 + x\}$. Thus, the ideals are precisely $(1), (x), (x^2), (0)$.

Chapter 4 Representation Theory

In this chapter, G is assumed to be a finite group, F a field, V is a vector space over F , unless otherwise specified.

4.1 Representation

Definition 4.1

$\rho : G \rightarrow GL(V)$ is called a representation of G , if ρ is a group homomorphism.

If ρ is clear, we usually denote the representation by V , and denote $\rho(g)v$ by gv . If $V = F^n$ where $n \in \mathbb{N}_1$, then it is called a matrix representation. It is called faithful if ρ is injective, i.e., different g are sent to different invertible linear maps on V .

In this chapter, every V is assumed to be a representation of G over F .

Example 4.1 There is a representation of S_n on F^n , defined by $\rho(g)(a_1, \dots, a_n) = (a_{g(1)}, \dots, a_{g(n)})$.

Proof Note that $\rho(gg')(a_1, \dots, a_n) = (a_{gg'(1)}, \dots, a_{gg'(n)})$ and that $\rho(g)(\rho(g')(a_1, \dots, a_n)) = \rho(g)(a_{g'(1)}, \dots, a_{g'(n)}) = (a_{gg'(1)}, \dots, a_{gg'(n)})$, and we are done.

4.2 Subrepresentations

Definition 4.2

$\rho : G \rightarrow GL(W)$ is called a subrepresentation of $\rho : G \rightarrow GL(V)$, if

1. W is a subspace of V .
2. For all $g \in G$, $\rho(g)W \subset W$.

The second condition is equivalent to saying that W is G -invariant.

Example 4.2 V is always a subrepresentation of V .

Example 4.3 $\{0\}$ is always a subrepresentation of V .

Example 4.4 Consider the representation S_n of F^n . It has a subrepresentation $\{(a, \dots, a) : a \in F\}$ and a subrepresentation $\{(a_1, \dots, a_n) : a_1 + \dots + a_n = 0\}$.

Proof By definition, this is trivial.

4.3 Irreducible Representations

Definition 4.3

V is called irreducible, if it has no non-trivial subrepresentations.

Example 4.5 Every 1-dimensional representation is irreducible.

4.4 Completely Reducible Representations

Definition 4.4

V is called completely reducible, if V is a direct sum of irreducible representations.

Proposition 4.1 (Maschke's Theorem)

Let $p = \text{char}(k)$. If $p \nmid |G|$ or $p = 0$, then every subrepresentation of V has a complementary subrepresentation.

Proof Assume W is a subrepresentation. Take X such that $V = W \oplus X$. Define $p : V \rightarrow W$ by $p(w + x) = w$. Let

$$Q = \frac{1}{|G|} \sum_{g \in G} gPg^{-1},$$

which is linear, where g denotes $\rho(g)$. Note that $Qw = w$, $hQh^{-1} = Q$, $\text{im}(Q) \subset W$ and $Q^2 = Q$. Now, if $Q(v) = 0$, then $Q(gv) = g(Qv) = 0$, and we are done.

Lemma 4.1

If V is a representation of G over \mathbb{C} , then there is an inner product $\langle \cdot, \cdot \rangle$ on V , such that for all $g \in G$,

$$\langle gv_1, gv_2 \rangle = \langle v_1, v_2 \rangle.$$

Proof Define

$$\langle v_1, v_2 \rangle = \frac{1}{|G|} \sum_{g \in G} (gv_1, gv_2),$$

and we are done.

Lemma 4.2

Under the previous assumptions, if $p \nmid |G|$ or $p = 0$, then V is completely reducible.

Proof The key is that we may use Gram-Schmidt process to find an orthonormal basis and every subspace has a complement subspace, and we are done.

Example 4.6 If $G = S_2$, then the usual representation is not completely reducible, since there is only one subrepresentation.

4.5 Morphisms of Representations

Definition 4.5

$\phi : V \rightarrow W$ is a G -representation morphism, if

1. $\phi : V \rightarrow W$ is linear.
2. For all $g \in G$ and $v \in V$, $\phi(gv) = g\phi(v)$.

Example 4.7 Consider the representation of \mathbb{Z}_4 on \mathbb{R}^2 by the rotations. Then $\text{Hom}_{\mathbb{Z}_4}(\mathbb{R}^2, \mathbb{R}^2) \simeq \mathbb{C}$.

Proof The transformations that commutes with the rotation of 90 degrees are exactly those with $a = d$, $b = -c$, and we are done.

Proposition 4.2 (Schur's Lemma)

Assume F is algebraically closed and V, W are irreducible.

1. $\text{Hom}_G(V, V)$ is 1-dimensional, i.e., the multiples of identities.
2. Every nonzero $\phi \in \text{Hom}_G(V, W)$ is an isomorphism.

Proof Consider an eigenvalue λ of $\phi \in \text{Hom}_G(V, V)$ such that $\phi(v) = \lambda v$ where v is in the eigenspace of λ . Note that $\phi(gv) = g\phi(v) = g(\lambda v) = \lambda gv$, so $E_\lambda = V$ and $\phi = \lambda I$. The second statement follows directly from the irreducibility.

Example 4.8 If F is algebraically closed and V, W are irreducible and not isomorphic, then every morphism between them is 0.

Example 4.9 If F is algebraically closed and V, W are irreducible and isomorphic, then $\text{Hom}_G(V, W)$ is 1-dimensional.

Example 4.10 If F is algebraically closed, V is irreducible and $g \in Z(G)$, then $g = \lambda I$ for some λ , so V is one-dimensional.

4.6 Isomorphisms of Representations

Definition 4.6

The G -representations V and W are called *isomorphic or equivalent*, if there is an isomorphism $f : V \rightarrow W$, such that for all $g \in G$, $gf = fg$.

The isomorphism of representations gives an equivalence relation. Note that f is an isomorphism of representations iff it is a bijective morphism from V to W .

4.7 Algebras over Fields

Definition 4.7

A is called an *algebra over a field F* , if

1. A is a vector space over F
2. There is a bilinear multiplication on A .

Example 4.11 The endomorphisms of V , denoted by $\text{End}(V)$, is an algebra over F .

Definition 4.8

If A, A' are algebras over a field F , then $f : A \rightarrow A'$ is an F -algebra homomorphism, if

1. f is F -linear.
2. For every $a, a' \in A$, $f(aa') = f(a)f(a')$.

4.8 Group Algebras

Definition 4.9

If G is a group and F is a field, then the group algebra $F[G]$ is defined to be

$$F[G] = \left\{ \sum'_{g \in G} a_g g : a_g \in F \right\},$$

where \sum' means that all but finitely many a_g 's are zero.

The group algebra $F[G]$ is always an algebra over F .

Lemma 4.3

If $\rho : G \rightarrow GL(V)$ is a representation of G , then it can be extended to $\rho : F[G] \rightarrow \text{End}(V)$, given by

$$\rho \left(\sum a_g g \right) v = \sum a_g \rho(g)v.$$

Example 4.12 The previous $\rho : F[G] \rightarrow \text{End}(V)$ is an F -algebra homomorphism.

4.9 Representations of Algebras

In this section, A is assumed to be an algebra over F .

Definition 4.10

$\rho : A \rightarrow \text{End}(V)$ is called a *representation of A over V* , if ρ is an F -algebra homomorphism.

Definition 4.11

W is called a *subrepresentation* of A , if

1. $W \subset A$
2. $\forall a \in A, aW \subset W$.

**Definition 4.12**

W is called *irreducible* if it has no non-trivial subrepresentations.

**Definition 4.13**

V is called *semisimple* or *completely reducible*, if it can be written as a direct sum of irreducible subrepresentations.

**Definition 4.14**

V is called *indecomposable*, if it cannot be written as a direct sum of two subrepresentations.

**Definition 4.15**

A is called *semisimple*, if for every representation V and a subrepresentation W , we can find a subrepresentation X such that $V \simeq W \oplus X$.



Example 4.13 Every irreducible representation is indecomposable.

Example 4.14 Every representation can be written as a direct sum of indecomposable representations.

Example 4.15 In a semisimple algebra, every indecomposable representation is irreducible.

Example 4.16 In a semisimple algebra, every representation is completely reducible.

Example 4.17 If $\text{char}(F) \nmid |G|$, then $F[G]$ is semisimple.

Definition 4.16

If A is an algebra, then the *left-regular representation* of A is defined by the left-multiplication.



Example 4.18 $F[x]/(x^2)$ is not semisimple, since the subrepresentation (x) has no complementary subrepresentation.

Example 4.19 If $\text{char}(F)$ divides $|G|$, then $F[G]$ is not semisimple.

Proof The complement of the subrepresentation $\{\sum a_g g : \sum a_g = 0\}$, $\{a \sum g : a \in F\}$, is equal to $\{0\}$, and we are done.

Proposition 4.3

If F is algebraically closed, V is a completely reducible A -representation, then

1. $V = \bigoplus_W W \otimes_F \text{Hom}_A(W, V)$, where W is the set of all irreducible representations of V and we define $a(w \otimes f) = aw \otimes f$.



4.10 Characters

In this section, F is assumed to be \mathbb{C} .

Definition 4.17

If $\rho : G \rightarrow GL(V)$ is a representation of G on V , then the *character* of ρ , denoted by χ_ρ , is a map from G to \mathbb{C} , given by $g \mapsto \text{Tr}(\rho(g))$.



Note that we may choose any basis and calculate the character, since χ_ρ is a class function, i.e., it is invariant under conjugation.

Definition 4.18

χ is called an *irreducible character*, if it is a character of an irreducible representation.



Example 4.20 If $\rho : G \rightarrow GL_n(\mathbb{C})$ is given by $\rho_g = (\rho_{ij}(g))$, then

$$\chi_\rho(g) = \sum_i \rho_{ii}(g).$$

Example 4.21 $\chi_\rho(1) = \deg(\rho)$.

Proof Note that $\rho(1) = id$, and we are done.

Example 4.22 The characters of equivalent representations are the same.

Proof Note again that trace is invariant under conjugation, and we are done.

Example 4.23 Let S be a finite set and assume that G acts on S . This induces a left-regular representation from G to the vector space over \mathbb{C} with the basis $\{v_s\}_{s \in S}$. Let $\chi : G \rightarrow \mathbb{C}$ be the character. Define another action of G on $S \times S$ by $g \cdot (s, t) = (gs, gt)$. Then the character induced by the second action is χ^2 .

Proof Note that $\chi(g) = \sum_{s:gs=s} 1$, so $\chi'(g) = \sum_{s,t:gs=s,gt=t} 1 = \chi(g)^2$, and we are done.

Example 4.24 If χ is the character of an n -dimensional complex representation of G , then $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$.

Proof Choose a basis, and write $\rho(g) = A$. Then $A^n = \rho(g^n) = \rho(1) = I$, so every eigenvalue is an n -th root of unity. Write A in the Jordan canonical form, and we are done.

4.11 Schur Orthogonality Relations

We have the inner product on $\mathbb{C}[G]$, given by

$$\left\langle \sum_g a_g g, \sum_g b_g g \right\rangle = \frac{1}{|G|} \sum_g \overline{a_g} b_g.$$

Let $U_n(\mathbb{C})$ denote the group of $n \times n$ unitary matrices over \mathbb{C} .

Lemma 4.4

Let $\phi : G \rightarrow GL(V)$ and $\rho : G \rightarrow GL(W)$ be representations and assume that $T : V \rightarrow W$ is a linear transformation. Let

$$T^\# = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \phi_g.$$

Then

1. $T^\# \in \text{Hom}_G(\phi, \rho)$.
2. If $T \in \text{Hom}_G(\phi, \rho)$, then $T^\# = T$.
3. The map $P : \text{Hom}(V, W) \rightarrow \text{Hom}_G(\phi, \rho)$ by $P(T) = T^\#$ is an onto linear map.



Proof All of these can be easily deduced by definition.

Lemma 4.5

Under the previous conditions,

1. If $\phi \approx \rho$, then $T^\# = 0$.
2. If $\phi = \rho$, then

$$T^\# = \frac{\text{Tr}(T)}{\deg(\phi)} I.$$



Proof By Schur's lemma, we can show the first one and also that

$$T^\# = \frac{\text{Tr}(T^\#)}{\deg(\phi)} I.$$

By computing the trace, we can prove the rest.

Note that $\text{Hom}(V, W) = M_{mn}(\mathbb{C})$, so P can be viewed a linear transformation from $M_{mn}(\mathbb{C})$ to itself. Thus, we will care about the basis matrices E_{ij} .

Lemma 4.6

$$(E_{ji})_{ij}^\# = \langle \rho_{kl}, \phi_{ij} \rangle.$$

Proof This is again just by definition.

Proposition 4.4 (Schur Orthogonality Relations)

If $\phi : G \rightarrow U_n(\mathbb{C})$ and $\rho : G \rightarrow U_m(\mathbb{C})$ are inequivalent irreducible unitary representations, then

1. $\langle \phi_{kl}, \rho_{ij} \rangle = 0$.
2. $\langle \phi_{kl}, \phi_{ij} \rangle$ is n^{-1} if $i = k$ and $j = l$, and 0 otherwise.

Proof Note that in the second case, we have

$$A^\# = \frac{\text{Tr}(E_{ki})}{n} I,$$

and we are done.

Thus, if ϕ is an irreducible unitary representation of G of degree d , then the d^2 functions $\sqrt{d}\phi_{ij}$ form an orthonormal set.

Moreover, if ϕ_1, \dots, ϕ_s is a complete set of representatives of equivalent irreducible representations of G , then the $d_1^2 + \dots + d_s^2$ functions $\sqrt{d_k}\phi_{ij}^k$ form an orthonormal set in $\mathbb{C}[G]$. In particular, $s \leq d_1^2 + \dots + d_s^2 \leq |G|$.

4.12 Class Functions

Definition 4.19

$f : G \rightarrow \mathbb{C}$ is called a *class function*, if it is invariant under conjugation.
The space of class functions is denoted $Z(\mathbb{C}[G])$.

$Z(\mathbb{C}[G])$ is always a subspace of $\mathbb{C}[G]$. Let $Cl(G)$ be the set of conjugacy classes of G . For each $C \in Cl(G)$, define δ_C to be the indicator of C .

Lemma 4.7

The set of δ_C forms a basis of $Z(\mathbb{C}[G])$.

Proof They are linearly independent, since

$$\langle \delta_C, \delta_{C'} \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\delta_C(g)} \delta_{C'}(g) = \begin{cases} \frac{|C|}{|G|} & C = C' \\ 0 & C \neq C' \end{cases}$$

Let $f \in Z(\mathbb{C}[G])$. Clearly, it is determined by the values in each conjugacy class, and we are done.

4.13 First Orthogonality Relations

Proposition 4.5 (First Orthogonality Relations)

If ϕ, ψ are irreducible representations, then

$$\langle \chi_\phi, \chi_\rho \rangle = \begin{cases} 1 & \phi \sim \rho \\ 0 & \phi \not\sim \rho. \end{cases}$$

In particular, the irreducible characters of G form an orthonormal set of class functions.

Proof

$$\begin{aligned}
 \langle \chi_\varphi, \chi_\rho \rangle &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_\varphi(g)} \chi_\rho(g) \\
 &= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^n \overline{\varphi_{ii}(g)} \sum_{j=1}^m \rho_{jj}(g) \\
 &= \sum_{i=1}^n \sum_{j=1}^m \frac{1}{|G|} \sum_{g \in G} \overline{\varphi_{ii}(g)} \rho_{jj}(g) \\
 &= \sum_{i=1}^n \sum_{j=1}^m \langle \varphi_{ii}(g), \rho_{jj}(g) \rangle.
 \end{aligned}$$

Using the Schur Orthogonality Relations, we are done.

Example 4.25 There are at most $|CI(G)|$ equivalence class of irreducible representations of G .

Proof The first orthogonal relations give that nonequivalent irreducible representations form a basis of $\mathbb{Z}(\mathbb{C}[G])$, which has the dimension $|CI(G)|$, and we are done.

From now on, we assume that ϕ_1, \dots, ϕ_s are the nonequivalent irreducible representations of G , unless otherwise specified.

Lemma 4.8

Every representation ρ on G can be written as $\rho \sim m_1 \phi_1 \oplus \dots \oplus m_s \phi_s$. Each m_i is called the multiplicity of ϕ_i in ρ .

Proof This is immediately from the theory of semisimple modules.

From now on, we assume that $\rho \sim m_1 \phi_1 \oplus \dots \oplus m_s \phi_s$, unless otherwise specified.

In particular, $\deg(\rho) = m_1 d_1 + \dots + m_s d_s$, since the character of direct sum is the sum of characters and we may take the value at 1.

Moreover, the multiplicity m_i is equal to $\langle \chi_{\phi_i}, \chi_\rho \rangle$, by the first orthogonality relation.

As a result, ρ is irreducible iff $\langle \chi_\rho, \chi_\rho \rangle = 1$, since $\langle \chi_\rho, \chi_\rho \rangle = m_1^2 + \dots + m_s^2$.

Example 4.26 Show that the representation of S_4 on $\{(a, b, c, d) : a + b + c + d = 0\}$ is irreducible.

Proof Choose a basis, and check that

$$\langle \chi_\rho, \chi_\rho \rangle = \frac{1}{24} (3^2 + 6 + 6 + 3) = 1,$$

and we are done.

Example 4.27 If ρ be an irreducible representation over \mathbb{C} , then

$$\deg(\rho) \leq \sqrt{\frac{|G|}{|Z|}},$$

where Z is the center of G .

Proof Let $z \in Z$. Then ρ_z is an isomorphism between ρ and itself, so ρ_z is a multiple of I . Moreover, every eigenvalue is a root of unity, so $\overline{\rho_z} \rho_z = 1$. Apply $1 = \langle \chi_\rho, \chi_\rho \rangle$, and we are done.

4.14 Regular Representations and Second Orthogonality Relations

Recall that the left-regular representation of G is given by

$$L_g \sum_h a_h h = \sum_h a_h gh = \sum_k a_{g^{-1}k} k.$$

This is a unitary representation, i.e., $\langle L_g v_1, L_g v_2 \rangle = \langle v_1, v_2 \rangle$.

Lemma 4.9

The character of L is $|G|$ if $g = 1$, and 0 otherwise.

Lemma 4.10

If ϕ_1, \dots, ϕ_s are the inequivalent irreducible unitary representations of G and $d_i = \deg \phi_i$, then L is isomorphic to $d_1\phi_1 \oplus \dots \oplus d_s\phi_s$.

Proof Let $\chi_i = \chi_{\phi_i}$. Then the inner product of χ_i and χ_L is $|G|^{-1} \overline{\chi_i(1)} |G| = \deg(\phi_i) = d_i$, and we are done.

Example 4.28 Under the previous assumptions, $|G| = d_1^2 + \dots + d_s^2$.

Proof Evaluate the value of the characters on both sides at 1, and we are done.

Proposition 4.6

$\sqrt{d_k} \phi_{ij}^k$ form an orthonormal basis in $\mathbb{C}[G]$.

Proof Note that the size of the list is exactly $d_1^2 + \dots + d_k^2 = |G|$, and we are done.

Proposition 4.7

χ_1, \dots, χ_s form an orthonormal basis in $Z(\mathbb{C}[G])$.

Proof The first orthogonality relations tell us that they form an orthonormal set. Let $f \in Z(\mathbb{C}[G])$. Write $f = \sum_{i,j,k} c_{ij}^k \phi_{ij}^k$. Then

$$\begin{aligned} f(x) &= \frac{1}{|G|} \sum_{g \in G} f(g^{-1}xg) \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{i,j,k} c_{ij}^{(k)} \varphi_{ij}^{(k)}(g^{-1}xg) \\ &= \sum_{i,j,k} c_{ij}^{(k)} \frac{1}{|G|} \sum_{g \in G} \varphi_{ij}^{(k)}(g^{-1}xg) \\ &= \sum_{i,j,k} c_{ij}^{(k)} \left[\frac{1}{|G|} \sum_{g \in G} \varphi_{g^{-1}}^{(k)} \varphi_x^{(k)} \varphi_g^{(k)} \right]_{ij} \\ &= \sum_{i,j,k} c_{ij}^{(k)} \left[\left(\varphi_x^{(k)} \right)^\# \right]_{ij} \\ &= \sum_{i,j,k} c_{ij}^{(k)} \frac{\text{Tr} \left(\varphi_x^{(k)} \right)}{\deg \varphi^{(k)}} I_{ij} \\ &= \sum_{i,k} c_{ii}^{(k)} \frac{1}{d_k} \chi_k(x), \end{aligned}$$

and we are done.

Example 4.29 The number of nonequivalent irreducible representations of G is the number of conjugacy classes of G .

Example 4.30 A finite group G is abelian iff it has $|G|$ equivalence classes of irreducible representations.

Definition 4.20 (Character Table)

Let G be a finite group with irreducible characters χ_1, \dots, χ_s and conjugacy classes C_1, \dots, C_s . Then the character table of G is given by a matrix (X_{ij}) where $X_{ij} = \chi_i(C_j)$.

Proposition 4.8 (Second Orthogonality Relations)

Let $C, C' \in Cl(G)$ and $g \in C, g' \in C'$. Then

$$\sum_{i=1}^s \overline{\chi_i(g)} \chi_i(h) = \begin{cases} \frac{|G|}{|C|} & C = C' \\ 0 & C \neq C'. \end{cases}$$

Proof Note that

$$\begin{aligned}
 \delta_C(h) &= \sum_{i=1}^s \langle \chi_i, \delta_C \rangle \chi_i(h) \\
 &= \sum_{i=1}^s \frac{1}{|G|} \sum_{x \in G} \overline{\chi_i(x)} \delta_C(x) \chi_i(h) \\
 &= \sum_{i=1}^s \frac{1}{|G|} \sum_{x \in C} \overline{\chi_i(x)} \chi_i(h) \\
 &= \frac{|C|}{|G|} \sum_{i=1}^s \overline{\chi_i(g)} \chi_i(h),
 \end{aligned}$$

and we are done.

Example 4.31 Show that the character table of A_4 is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & 1 \\ 3 & 0 & 0 & -1 \end{pmatrix}$$

Proof It is easy to see that the A_4 has a 3-dimensional irreducible character as S_4 does. Thus, it has three 1-dimensional irreducible characters. By looking at the orders of each element in the conjugacy classes, we have only one case, which is the character table shown in the graph.

Example 4.32 If $x \neq e$, then there is some j such that $\chi_j(x) \neq \chi_j(e)$.

Proof Prove by contradiction. Use the Second Orthogonality Relations, and we are done.

4.15 More Exercises

Example 4.33 Let g be an element of a finite group G . Prove that g is conjugate g^{-1} iff for every irreducible complex-valued character χ , $\chi(g) \in \mathbb{R}$.

Proof The first direction is trivial. The second direction follows from the Second Orthogonality Relations.

Example 4.34 If $x \neq e$, then there is some j such that $\chi_j(x) \neq \chi_j(e)$.

Proof By the Second Orthogonality Relations, we are done.

Example 4.35 If $y \in G$ such that $\rho_j(y)$ commutes with $\rho_j(x)$ for all $x \in G$ and j , then $y \in Z(G)$.

Proof Use the previous exercise, and we are done.

Example 4.36 Let ρ be an irreducible representation of G on V and H be a subgroup of G . Write $H = n_1\chi_1 + \cdots + n_r\chi_r$ where χ_1, \dots, χ_r are the nonequivalent irreducible representations of H . Then $n_1^2 + \cdots + n_r^2 \leq |G|/|H|$.

Proof Consider $\langle \chi_G, \chi_G \rangle$ and $\langle \chi_H, \chi_H \rangle$, and we are done.

Chapter 5 Commutative Algebra and Algebraic Geometry

In this chapter, R is assumed to be a commutative ring, k is assumed to be a field.

5.1 Vanishing/Zero Sets

Definition 5.1

If $f \in k[x_1, \dots, x_n]$, then the vanishing/zero set of f , denoted by $Z(f)$, is defined by $Z(f) = \{a \in k^n : f(a) = 0\}$.

Example 5.1 If $k = \mathbb{R}$, then $Z(x^2 + y^2 - 1)$ is the unit circle.

Proof This is trivial.

We usually denote \mathbb{A}_k^n to be k^n .

Definition 5.2

If $S \subset k[x_1, \dots, x_n]$, then the vanishing/zero set of S , denoted by $Z(S)$, is defined by $Z(S) = \{a \in \mathbb{A}^n : \forall f \in S, f(a) = 0\}$.

Example 5.2 $Z(S) = \bigcap_{f \in S} Z(f)$.

Definition 5.3

$A \subset \mathbb{A}^n$ is called an affine algebraic variety, if it can be written as $Z(S)$ for some $S \subset k[x_1, \dots, x_n]$.

Example 5.3 Every singleton $\{a\}$ is an affine variety in \mathbb{A}^n .

Proof $\{a\} = Z(x_1 - a_1, \dots, x_n - a_n)$.

Example 5.4 \mathbb{A}^n is an affine variety in itself.

Proof $\mathbb{A}^n = Z(\emptyset)$.

Example 5.5 \emptyset is an affine variety in \mathbb{A}^n .

Proof $\emptyset = Z(x_1, x_1 - 1)$.

Example 5.6 If $S \subset T$, then $Z(S) \supset Z(T)$.

Example 5.7 $Z(S \cup T) = Z(S) \cap Z(T)$. Moreover, $Z(\cup_i T_i) = \cap_{i \in I} Z(T_i)$.

Example 5.8 The arbitrary intersection of affine varieties is an affine variety.

Example 5.9 $Z(ST) = Z(S) \cup Z(T)$.

Proof $(ST)(a) = 0 \iff S(a) = 0 \text{ or } T(a) = 0$, and we are done.

Example 5.10 The finite union of affine varieties is an affine variety.

Example 5.11 If k is a finite field, then every subset of \mathbb{A}^n is an affine variety.

Proof Every subset in this case is a finite union of singletons, and we are done.

5.2 The Zariski Topology on \mathbb{A}^n

Definition 5.4

The Zariski topology on \mathbb{A}^n is the topology where closed sets are exactly the affine varieties.

The Zariski topology is always a topology, trivially by the previous examples.

On the other hand, $U \subset \mathbb{A}^n$ is an open set iff the complement U^C is an affine variety.

Example 5.12 Every affine variety in \mathbb{R}^n is a closed set in the Euclidean topology.

Proof Note that $Z(S) = \bigcap_{f \in S} Z(f)$, and we are done.

Example 5.13 The affine varieties in $\mathbb{A}_{\mathbb{R}}^1$ are exactly those finite sets or the entire set.

Proof Note that every nonzero polynomial in $\mathbb{R}[x]$ has finitely many zeros. Every $Z(S)$ can be written as $Z(I)$ where I is the ideal generated by S . But $\mathbb{R}[x]$ is Noetherian, so I is finitely generated. $Z(I) = Z(f_1 \cup \dots \cup f_m) = Z(f_1) \cap \dots \cap Z(f_m)$, and we are done.

5.3 Vanishing Ideals

Definition 5.5

If $A \subset \mathbb{A}^n$, then the vanishing/zero set of A , denoted by $I(A)$, is defined by $I(A) = \{f \in k[x_1, \dots, x_n] : \forall a \in A, f(a) = 0\}$.

The vanishing set is always an ideal in $k[x_1, \dots, x_n]$.

Example 5.14 If $A \subset B$, then $I(A) \supset I(B)$.

Example 5.15 $I(\mathbb{A}^n) = \{0\}$.

Example 5.16 $I(\emptyset) = k[x_1, \dots, x_n]$.

Example 5.17 If $a \in \mathbb{A}^n$, then $I(a) = I(\{a\}) = (x_1 - a_1, \dots, x_n - a_n)$.

Proof $(x_1 - a_1, \dots, x_n - a_n)$ is clearly in $I(a)$. Note that the quotient ring is k , so this ideal is maximal, and we are done.

Example 5.18 $I(A \cup B) = I(A) \cap I(B)$. Moreover, $I(\cup_i A_i) = \cap_{i \in I} I(A_i)$.

Example 5.19 If A is the union of x and y axis, then $I(A) = (xy)$.

Example 5.20 (x^2) is not a vanishing ideal.

Proof If $(x^2) = I(A)$. Then $A = \{0\}$. But $I(A) = (x)$, and we are done.

Recall that $I \subset R$ is a radical ideal, if $a^n \in I \implies a \in I$ for all $a \in R$ and $n \in \mathbb{N}_1$.

Lemma 5.1

If $A \subset \mathbb{A}^n$, then $I(A)$ is a radical ideal in $k[x_1, \dots, x_n]$.

Proof Assume $f^n \in I(A)$. Let $a \in A$. Then $f^n(a) = 0$. $f(a) = 0$ for all $a \in A$, so $f \in I(A)$, and we are done.

Example 5.21 If $S \subset k[x_1, \dots, x_n]$, then $I(Z(S)) \supset S$.

Proof Let $a \in Z(S)$ and $f \in S$. Then $f(a) = 0$. Thus, $f \in I(Z(S))$, and we are done.

Example 5.22 If $A \subset \mathbb{A}^n$, then $Z(I(A)) \supset A$.

Proof Let $f \in I(A)$ and $a \in A$. Then $f(a) = 0$. Thus, $a \in Z(I(A))$, and we are done.

5.4 Coordinate Rings

Definition 5.6

Let $X \subset \mathbb{A}^n$ with vanishing ideal $I(X) \subset k[x_1, \dots, x_n]$, then the coordinate ring of X , denoted by $k(X)$ or $\mathcal{O}(X)$, is defined by the quotient ring $k(X) = \mathcal{O}(X) = k[x_1, \dots, x_n]/I(X)$.

Every element in $\mathcal{O}(X)$ can be thought of a polynomial from X to k . Let $[f] = [f'] \in \mathcal{O}(X)$. Then $f - f' \in I(X)$, so $f(x) = f'(x)$ for all $x \in X$.

Example 5.23 Let X be the x -axis in \mathbb{A}^2 . Then $\mathcal{O}(X)$ represents the polynomial from X to k , i.e., $\mathcal{O}(X) = k[x, y]/(I(X)) = k[x, y]/(y) = k[x]$.

Definition 5.7

R is called reduced or nilpotent free, if $a^n = 0 \implies a = 0$ for all $a \in R$ and $n \in \mathbb{N}_1$.

Lemma 5.2

If R is reduced, then R/I is reduced iff I is radical.

Proof On one hand, if R/I is reduced and $a^n \in I$, then $[a]^n = [0]$, so $a \in I$.

On the other hand, if I is radical and $[a]^n = [0]$, then $a^n \in I$ and $[a] = [0]$, and we are done.

Example 5.24 Every integral domain is reduced. Thus, every field is reduced.

Example 5.25 The coordinate ring $\mathcal{O}(X)$ is always reduced, since $I(X)$ is always radical.

Example 5.26 The coordinate ring of \mathbb{A}^n is $k[x_1, \dots, x_n]$.

Proof Note that $I(\mathbb{A}) = \{0\}$, and we are done.

Example 5.27 The coordinate ring of \emptyset is $\{0\}$.

Proof Note that $I(\emptyset) = k[x_1, \dots, x_n]$, and we are done.

Example 5.28 The coordinate ring of $\{a\}$ is k .

Proof Note that $I(a) = I(\{a\}) = (x_1 - a_1, \dots, x_n - a_n)$, and we are done.

5.5 Hilbert Basis Theorem

Proposition 5.1 (Hilbert Basis Theorem)

If R is Noetherian, then $R[x]$ is Noetherian.

Proof Let $I \triangleleft R[x]$. It suffices to show that I is finitely generated. Assume not, then choose $f_1 \in I$ of minimal degree, and inductively, choose $f_{k+1} \in I \setminus (f_1, \dots, f_k)$. Let $f_i = a_{n_i}x^{n_i} + \dots + a_{i_0}$, so $n_1 \leq n_2 \leq \dots$. Consider the chain of ideals $(a_{n_1}) \subset (a_{n_1}, a_{n_2}) \subset \dots$. Since R is Noetherian, so there is some $m \in \mathbb{N}_1$ such that $a_{n_{m+1}} = r_1 a_{n_1} + \dots + r_m a_{n_m}$ for $r_i \in R$. However, we may subtract an $R[x]$ -linear combination of f_1, \dots, f_m from f_{m+1} to have a polynomial in $I \setminus (f_1, \dots, f_m)$ with smaller degree than f_{m+1} , and we are done.

Lemma 5.3

If R is Noetherian, then for all $n \in \mathbb{N}_1$, $R[x_1, \dots, x_n]$ is Noetherian.

Example 5.29 Every affine variety is the zero locus of finitely many polynomials.

Proof If $A = Z(S)$, then $A = Z(I)$ where $I = (S)$ is finitely generated, and we are done.

Example 5.30 Every quotient ring of a Noetherian ring is Noetherian.

Proof An ideal in R/I is the image of an ideal in R under the canonical surjection, hence finitely generated.

5.6 Morphisms of Affine Varieties

Definition 5.8

If X, Y are affine varieties with coordinate rings $\mathcal{O}(X)$ and $\mathcal{O}(Y)$, then $f : X \rightarrow Y$ is called a morphism of affine varieties, if for every $f \in \mathcal{O}(Y)$, $\phi^(f) = f \circ \phi$ is in $\mathcal{O}(X)$.*

The set of all morphisms from X to Y is denoted by $\text{Hom}_{\text{Var}}(X, Y) = \text{Hom}(X, Y)$.

Example 5.31 If $X = Y = \mathbb{A}$, then $\text{Hom}(X, Y) \simeq k[x]$.

Proof First, $\mathcal{O}(X) = k[x]$ and $\mathcal{O}(Y) = k[y]$. If $\phi : X \rightarrow Y$ is a morphism of varieties, then $\phi^*(y) = y \circ \phi \in k[x]$. Define $f(x) = \phi^*(y)$. Then for all $g \in \mathcal{O}(Y) = k[y]$, we have $g \circ \phi = g(y \circ \phi) = g \circ f \in k[x]$. Thus, $\text{Hom}(\mathbb{A}, \mathbb{A})$ is uniquely determined by $f \in k[x]$, and we are done.

Example 5.32 If X is an affine variety in \mathbb{A} , then $\text{Hom}(X, \mathbb{A}) \simeq \mathcal{O}(X)$.

Proof Let $\phi : X \rightarrow \mathbb{A}$ be a morphism. Let $f = y \circ \phi \in \mathcal{O}(X) = k[x_1, \dots, x_n]/I(X)$. Then for all $g \in \mathcal{O}(\mathbb{A}) = k[y]$, we have $g \circ \phi = g(y \circ \phi) = g \circ f \in \mathcal{O}(X)$. Thus, $\text{Hom}(X, \mathbb{A})$ is uniquely determined by $f \in \mathcal{O}(X)$, and we are done.

Lemma 5.4

Let X be an affine variety in \mathbb{A}^n and Y be an affine variety in \mathbb{A}^m . Then $f : X \rightarrow Y$ is a morphism of varieties iff there exists $T_1, \dots, T_m \in k[x_1, \dots, x_n]$, such that $\phi|_X = (\phi_1|_X, \dots, \phi_m|_X)$.

Proof Choose $f_i = \phi^*(y_i) = y_i \circ \phi \in \mathcal{O}(X)$ and $T_i \in k[x_1, \dots, x_n]$ such that $[T_i] = f_i$, and we are done.

Definition 5.9

If X, Y are affine varieties with coordinate rings $\mathcal{O}(X)$ and $\mathcal{O}(Y)$, then $f : X \rightarrow Y$ is called an isomorphism of affine varieties, if

1. $f : X \rightarrow Y$ is a bijection.
2. $f : X \rightarrow Y$ is a morphism of affine varieties.
3. $f^{-1} : Y \rightarrow X$ is a morphism of affine varieties.

Example 5.33 $Z(xy - z) \simeq \mathbb{A}^2$.

Proof Let $\pi : X \rightarrow \mathbb{A}^2$ by $\pi(x, y, xy) = (x, y)$. This is clearly a bijection and each coordinate is a polynomial, hence a morphism. On the other hand, $\pi^{-1}(x, y) = (x, y, xy)$ is also a morphism. Thus, π is an isomorphism from $Z(xy - z)$ to \mathbb{A}^2 .

Example 5.34 If $k = \mathbb{C}$, then $X = Z(x^2 + y^2 - 1) \simeq Z(uv - 1) = Y$.

Proof Define $\pi : Y \rightarrow X$ by $\pi(u, v) = (u + iv, u - iv)$. Then $\pi^{-1}(x, y) = \frac{1}{2}(u + v, -i(u - v))$. Note that π is a bijective morphism whose inverse is again a morphism, and we are done.

5.7 Irreducible Varieties

Definition 5.10

If X be an affine variety, then it is called irreducible if it cannot be written as the union of two proper closed subsets.

Example 5.35 \mathbb{A}_k^1 is irreducible in the Zariski topology, since every closed subset is finite.

Example 5.36 $Z(xy)$ is not irreducible (i.e., reducible), since $Z(xy) = Z(x) \cup Z(y)$.

Proposition 5.2

X is irreducible iff $I(X)$ is prime.

Proof One one hand, if $X = A \cup B$, then we may take $f \in I(A) \setminus I(X)$ and $g \in I(B) \setminus I(X)$ while $fg \in I(A)I(B) \subset I(A) \cap I(B) = I(A \cup B) = I(X)$. Thus, $I(X)$ is not prime.

On the other hand, if $I(X)$ not prime, then we may take $f, g \notin I(X)$ while $fg \in I(X)$. Let $A = Z(f) \cap X$ and $B = Z(g) \cap X$. Then $A \cup B = (Z(f) \cup Z(g)) \cap X = Z(fg) \cap X = X$, and we are done.

Example 5.37 TFAE.

1. X is irreducible.
2. $I(X)$ is prime.
3. $\mathcal{O}(X)$ is an integral domain.

Example 5.38 Find the irreducible components of the algebraic variety $Z(x^2z - y^2z)$.

Proof Clearly, they are $Z(x + y)$, $Z(x - y)$, $Z(z)$.

5.8 Integrality

In this section, $R \subset S$ are assumed to be two commutative rings.

Definition 5.11

s is called integral over R , if it is a root of some polynomial in $R[x]$. S is called integral over R if every element of S is integral over R .

Definition 5.12

R is called integrally closed in S , if no element of $R \setminus S$ is integral over R .

Definition 5.13

R is called *integrally closed*, if it is integrally closed in $Q(R)$.



Example 5.39 $k[x]$ is integrally closed.

Proof Note that $Q(k[x]) = k(x)$. If f/g is a root of some polynomial in $k[x]$ of degree n , then f^n is equal to g times a function in $k[x]$. Every polynomial divides g must divides f , and we are done.

Example 5.40 If R is a UFD, then R is integrally closed.

Proof The proof is essentially the same as in the previous example.

Definition 5.14

If R is an integral domain, then the *normalization* of R is defined to be the integral closure of R in $Q(R)$, i.e., the set of all elements in $Q(R)$ that are integral over R .



The normalization of R , or the integral closure of R , is always a subring of $Q(R)$.

Example 5.41 $R = k[x, y]/(x^2 - y^3)$ is not integrally closed, since x/y is a root of $u^2 - y \in R[u]$. Indeed, the normalization is $k[v]$ where $v = x/y$.

Example 5.42 If T is integral over S and S is integral over R , then T is integral over R .

Proof This is trivial.

Lemma 5.5

s is integral over R iff $R[s]$ is a finitely generated R -module.



Proof If s is integral over R , then s^r is a linear combination of $1, \dots, s^{r-1}$, so $R[s]$ is a finitely generated R -module.

If $R[s]$ is a finitely generated R -module. Let v_1, \dots, v_n be a basis. Consider the left multiplication of s , and we let the matrix be (r_{ij}) . Let $f(x) = \det(A - xI) \in R[x]$ which is a monic polynomial. Then $f(s)v_i = 0$ for all i , so $f(s) = 0$. Therefore, s is integral over R , and we are done.

Lemma 5.6

If S is an integral domain and S is integral over R , then R is a field iff S is a field.



Proof If S is a field. R is a subring of an integral domain, thus also an integral domain. It suffices to show R is closed under inversion. Let $r \in R$. Assume r^{-1} is a root of a polynomial in $R[x]$. By some simple algebraic manipulations, $r^{-1} \in R$.

If R is a field. Let $s \in S$. Assume $s^n + a_{n-1}s^{n-1} + \dots + a_k s^k = 0$ where $a_k \neq 0$. Now that $a_k \in R$ and R is a field, by some simple algebraic manipulations, we are done.

5.9 Noether Normalization and Zariski's Lemma

Proposition 5.3 (Noether Normalization)

If k is a field, and A is a finitely generated k -algebra, then there exists $y_1, \dots, y_n \in A$ that are algebraically independent over k such that A is integral over $k[y_1, \dots, y_n]$.

**Lemma 5.7 (Zariski's Lemma)**


If $k < L$ are two fields, and L is a finitely generated k -algebra, then L is algebraic over k .



Proof By Noether Normalization, take $y_1, \dots, y_n \in L$ that are algebraically independent over k such that L is integral over $k[y_1, \dots, y_n]$. L is a field, so $n = 0$, i.e., L is algebraic over k , and we are done.


5.10 Hilbert's Nullstellensatz

Lemma 5.8 (Weak Nullstellensatz I)

If k is algebraically closed, then every maximal ideal of $k[x_1, \dots, x_n]$ has the form $(x_1 - a_1, \dots, x_n - a_n)$. 


Proof Let \mathfrak{m} be a maximal ideal in $k[x_1, \dots, x_n]$. Then $L = k[x_1, \dots, x_n]/\mathfrak{m}$ is a field and is finitely generated. By Zariski's lemma, $L = k$. Thus, for each i , $x_i - a_i \in \mathfrak{m}$ for some $a_i \in k$, and we are done.

Lemma 5.9 (Weak Nullstellensatz II)

If $I \subset k[x_1, \dots, x_n]$ is a proper ideal, then $Z(I) \neq \emptyset$. 

Proof If I is a proper ideal, then I is contained in some maximal ideal, say $I \subset J = (x_1 - a_1, \dots, x_n - a_n)$. Thus, $Z(I) \supset Z(J) = \{a\}$, and we are done.

Proposition 5.4 (Nullstellensatz)

There is a bijection between the set of affine varieties in \mathbb{A}^n and radical ideals in $k[x_1, \dots, x_n]$ with Z and I . 

Proof It suffices to show that if J is an radical ideal, then $I(Z(J)) \subset J$. Let $g \in I(Z(J))$. It suffices to show that $g^n \in J$ for some J .

Let J' be the ideal in $k[x_1, \dots, x_n, x_{n+1}]$ generated by J and $gx_{n+1} - 1$. We claim that $Z(J') = \emptyset$, since if $(a_1, \dots, a_{n+1}) \in Z(J')$, then $(a_1, \dots, a_n) \in Z(J)$ and $g(a_1, \dots, a_n)x_{n+1} = 1$ which is not possible.

By Weak Nullstellensatz II, J' must be the entire $k[x_1, \dots, x_{n+1}]$. Thus, we can find $f_1, \dots, f_m \in J$ and $h_1, \dots, h_{m+1} \in k[x_1, \dots, x_{n+1}]$ such that $1 = h_1 f_1 + \dots + h_m f_m + h_{m+1} (gx_{n+1} - 1)$. Consider the homomorphism from $k[x_1, \dots, x_{n+1}]$ to $k(x_1, \dots, x_n)$ by sending x_{n+1} to g^{-1} . Then $1 = h_1(x_1, \dots, x_n, g^{-1}) f_1(x_1, \dots, x_n) + \dots + h_m(x_1, \dots, x_n, g^{-1}) f_m(x_1, \dots, x_n)$. By multiplying by g^N for sufficiently large N , we can show that $g^N \in J$, and we are done.

Chapter 6 Field Theory and Galois Theory

In this chapter, k, E, F are assumed to be fields.

6.1 Fields

Definition 6.1

F is called a field if it is a commutative ring where every nonzero element has a multiplicative inverse.

Example 6.1 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ are fields.

Example 6.2 If R is an integral domain, then $Q(R)$ is a field.

Example 6.3 The only ideals of a field are the zero ideal and the entire field.

Example 6.4 Every nonzero ring homomorphism of fields is injective.

Proof Note that the kernel cannot be the entire field, and we are done.

6.2 Polynomials over Fields

Example 6.5 $k[x]$ is a PID.

Definition 6.2

The field of rational functions over k , denoted by $k(x)$, is defined by $k(x) = Q(k[x])$.

$k(x)$ is always a field, since $k[x]$ is an integral domain.

Definition 6.3

The field of Laurent Series over k , denoted by $k((x))$, is defined by $k((x)) = \{a^n + a^{n+1} + \dots, n \in \mathbb{Z}\}$.

Proposition 6.1

$k((x)) \simeq k(x)$.

Proof Note that if $a_0 \neq 0$, then $1/f \in k[x]$, and if not, then take the smallest n such that $a_n \neq 0$. Thus, $k(x)$ can be embedded in $k((x))$. On the other hand, every Laurent series is clearly a quotient of a Taylor series and some x^n , and we are done.

6.3 Field Extensions

Definition 6.4

F/k is called a field extension, if k is subfield of F , i.e., $k < F$.

From now on, $E/k, F/k, K/F$ are assumed to be field extensions.

Example 6.6 F is a vector space over k .

Definition 6.5

The degree of the extension F/k is defined to be the dimension of F over k , denoted $[F : k]$.

Definition 6.6

F/k is called a finite degree, if $[F : k] < \infty$.

Proposition 6.2 (Tower Law)

If $L/K/F$ are two field extensions, then $[L : F] = [L : K][K : F]$.

Proof Consider the two bases a_i and b_j , and show that $a_i b_j$'s are linearly independent, and we are done.

6.4 Characteristics of Fields

Definition 6.7

The smallest n such that $n \cdot 1 = 0$ is called the characteristic of F , denoted $\text{char}(F)$, if exists. Otherwise, $\text{char}(F)$ is defined to be 0.

Example 6.7 The smallest subfield in F is the field generated by 1. There are only two cases. \mathbb{Q} or \mathbb{F}_p for some prime p .

Example 6.8 The order of every finite field is a power of a prime.

Definition 6.8

Note that every finite field is a vector space over some \mathbb{F}_p , and we are done.

Example 6.9 $\mathbb{F}_4 = \mathbb{F}_2/(x^2 + x + 1)$.

Proof Note that $x^2 + x + 1$ has no roots in \mathbb{F}_2 , and we are done.

6.5 Simple Extensions

Proposition 6.3

If $p(x) \in F[x]$ is irreducible, then

1. $K = F[x]/(p(x))$ is an extension of F such that $p(x)$ has a root in K .
2. $[K : F] = \deg p(x)$.
3. If K' is an extension containing a root α of $p(x)$, then K is isomorphic to $F(\alpha)$, the subfield generated by F and α .

Proof The key is that $[x]$ is a root of $p(x)$ in $F[x]/(p(x))$, and every element can be written as $[q(x)]$ where $\deg(q) < \deg(p)$.

Example 6.10 $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Example 6.11 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Example 6.12 $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$.

Proof Assume not, say $f(\sqrt{2}) = a + b\sqrt{3}$ where $b \neq 0$. Then $2 = a^2 + 3b^2 + 2ab\sqrt{3}$, so $a = 0$, and we are done.

Example 6.13 Let θ be a root of $p(x) = x^3 + 9x + 6$. Find $(1 + \theta)^{-1}$.

Proof By a long division, we can show $x^3 + 9x + 6 = (x^2 - x + 10)(x + 1) - 4$. Thus, $(1 + \theta)^{-1} = (x^2 - x + 10)/4$, and we are done.

Example 6.14 If $f(x)$ is an irreducible polynomial over F , and $h(x)$ is an irreducible factor of $f(g(x))$ for some $g(x) \in F[x]$, then $\deg(h) \mid \deg(f)$.

Proof Let α be a root of $h(x)$. Then $h(x)$ is the minimal polynomial of α and $f(x)$ is the minimal polynomial of $g(\alpha)$ over $F(x)$. Thus, $\deg(h) = [F(\alpha) : F] = [F(\alpha) : F(g(\alpha))][F(g(\alpha)) : F]$, and we are done.

6.6 Algebraic Extensions

Definition 6.9

$\alpha \in K$ is called algebraic over F if it vanishes over a polynomial in $F[x]$.

K/F is called algebraic, if every element in K is algebraic over F ; otherwise, K/F is called transcendental.

Proposition 6.4

If α is transcendental, then $F[\alpha] \simeq F[x]$ and $F(\alpha) \simeq F(x)$.

Proof The key is that $\alpha \mapsto x$ defined an isomorphism between $F[\alpha]$ and $F[x]$, and we are done.

Example 6.15 α is algebraic over F iff $[F(\alpha) : F] < \infty$.

Example 6.16 Every finite field extension is algebraic.

Proof Consider $1, \alpha, \dots$, and we are done.

Example 6.17 $k(x)$ is transcendental over k .

Example 6.18 Let D_1, D_2 be non-squares in F where $\text{char}(F) \neq 2$. Then $[F(\sqrt{D_1}, \sqrt{D_2}) : F]$ is 4 if $D_1 D_2$ is not a square, and 2 otherwise.

Proof The key is considering $x^2 - D_1$ in $F(\sqrt{D_2})[x]$. It is irreducible iff $D_1 D_2$ is not a square in F , and we are done.

Example 6.19 If $[F(\alpha) : F] = p$ is a prime, then for all $1 \leq k \leq p-1$, $F(\alpha^k) = F(\alpha)$.

Proof Use the Tower Law and the minimal polynomial, and we are done.

6.7 Splitting Fields

Definition 6.10

Let $p(x)$ be polynomial in $F[x]$. A splitting field for $p(x)$ is an extension field K where $p(x)$ splits into linear factors, and $p(x)$ does not split over any intermediate field.

Example 6.20 $\mathbb{Q}(\sqrt{2})$ is the splitting field of $p(x) = x^2 - 2$.

Example 6.21 $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of $p(x) = x^3 - 2$, since $\sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2$ are not in this field.

Example 6.22 Find the splitting field of $x^4 - 2$.

Proof Let $\alpha = \sqrt[4]{2}$. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $\mathbb{Q}(\alpha) \subset \mathbb{R}$. The splitting field is $\mathbb{Q}(\alpha, i)$ with degree 8.

Example 6.23 Find the splitting field of $x^4 - 4$.

Proof Let $\alpha = \sqrt{2}$. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ and $\mathbb{Q}(\alpha) \subset \mathbb{R}$. The splitting field is $\mathbb{Q}(\alpha, i)$ with degree 4.

Example 6.24 Find the splitting field of $x^5 - 7$.

Proof Let $\alpha = \sqrt[5]{7}$. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. The splitting field is $\mathbb{Q}(\alpha, \zeta_5)$ with degree 20, since the minimal polynomial of ζ_5 over $\mathbb{Q}(\alpha)$ is 4.

Definition 6.11

Find the splitting field of $x^4 + x^2 + 1$.

Proof It factors into a product of $x^2 + x + 1$ and $x^2 - x + 1$. Thus, the splitting field is $\mathbb{Q}(\sqrt{-3})$, and we are done.

Definition 6.12

Show $p(x) = x^{p-1} + \dots + x + 1$ is irreducible over \mathbb{Q} .

Proof Note that $p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}$, and we are done.

Example 6.25 If $p(x)$ is an irreducible quadratic in $F(x)$ and α is a root of $p(x)$, then $F(\alpha)$ is the splitting field of $p(x)$.

Example 6.26 Show $x^4 + 6x - 3$ is irreducible in $\mathbb{Q}(\sqrt[3]{5})$.

Proof First, it is irreducible in \mathbb{Q} . Clearly it cannot have quadratic divisors. If it has a linear factor, then there is a root θ of this irreducible polynomial in \mathbb{Q} which is also in $\mathbb{Q}(\sqrt[3]{5})$. However, it is a root of a cubic polynomial, and we are done.

Example 6.27 The degree of a splitting field of $p(x)$ with degree n is at most $n!$.

Proof Inductively take an irreducible factor and consider the quotient field, and we are done.

6.8 Constructible Numbers

Definition 6.13

$\alpha \in \mathbb{R}$ is called *constructible*, if it is possible to construct a segment of length α starting from the unit length segment, using only a straight-edge and compass.

It can be shown that α is constructible iff it is in a field F such that $\mathbb{Q} \subset F_1 \cdots \subset F_n = F$ where each extension has degree 2.

Example 6.28 $\cos(20^\circ)$ is not constructible.

Proof It is a root of $4x^3 - 3x - 1/2 = 0$, and we are done.

6.9 Cyclotomic Fields

Definition 6.14

$\zeta \in \mathbb{C}$ is called a *primitive n -th root of unity*, if it generates the cyclic group of n -th roots of unity. The set of all primitive n -th root of unity is denoted by p_n .

Proposition 6.5

The set of n -th roots of unity is the disjoint union of d -th roots of unity for $d|n$, i.e., $\sqcup_{d|n} p_d$.

Definition 6.15

The n -th cyclotomic polynomial is defined by $\Phi_n(x) = \prod_{\zeta \in p_n} (x - \zeta)$.

Example 6.29 If p is a prime, then $\Phi_p(x) = x^{p-1} + \cdots + x + 1$. We have shown that this polynomial is always irreducible over \mathbb{Q} .

Example 6.30 $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

6.10 Algebraic Closure

Definition 6.16

K is called an *algebraic closure* of F , if

1. Every polynomial in F splits over K .
2. Every element of K is algebraic over F .

Definition 6.17

F is called *algebraically closed*, if every polynomial in $F[x]$ splits.

Lemma 6.1

Every algebraic closure of F is algebraically closed.

Proof Let K be an algebraic closure of F . Let $f(x) \in K[x]$ be a polynomial. Let α be a root of $f(x)$. Then $K(\alpha)$ is algebraic over F . So $\alpha \in K$, and we are done.

Proposition 6.6

Every field has an algebraic closure, and any two algebraic closures are isomorphic.

Example 6.31 If $f : F \rightarrow F$ is a field automorphism and F is algebraic over \mathbb{Q} , then f is an isomorphism.

Proof We know that this has to be injective. Let $\alpha \in F$ and $p(x)$ be the minimal polynomial of α . Then $p(\psi(\alpha)) = \psi(p(\alpha)) = 0$. We can find some $m > n$ such that $\psi^m(\alpha) = \psi^n(\alpha)$, so $\psi^{m-n}(\alpha) = 1$, and we are done.

6.11 Separable Polynomials

Definition 6.18

$f(x) \in F[x]$ is called *separable*, if it has no multiple roots in its splitting field. Otherwise, it is called *inseparable*.

Definition 6.19

$f(x) \in F[x]$ is called *purely inseparable*, if it has exactly one root.

Definition 6.20

The formal derivative $D_x : F[x] \rightarrow F[x]$ is defined by $D_x(x^n) = nx^{n-1}$.

We can easily check that D_x is a derivation; i.e., it is linear and satisfies the Leibniz rule.

Lemma 6.2

Let α be a root of $f(x)$, then it is a multiple root iff it is also a root of $D_x(f) = f'$.

Example 6.32 $f(x)$ is separable iff $f(x)$ and $f'(x)$ are coprime.

Example 6.33 If $f(x)$ is irreducible and $f' \neq 0$, then $f(x)$ is separable.

Proof It suffices to show that if $f(x)$ has a multiple root α and $f(x)$ is irreducible, then $f'(x) = 0$. The key is that if $f(x)$ is irreducible and α is a root of both $f(x)$ and $f'(x)$, then $f(x) \mid f'(x)$. By the degree argument, we are done.

Example 6.34 If $\text{char}(F) = 0$, then irreducible polynomial is separable.

Proof By the previous example, separate two cases by whether $\deg(f) = 1$, and we are done.

6.12 Perfect Field

Definition 6.21

K is called a *perfect field*, if every irreducible polynomial is separable.

Proof Every field of characteristic 0 is perfect.

Proposition 6.7

If $\text{char}(F) = p$, then F is perfect iff the Frobenius endomorphism $\phi : a \mapsto a^p$ is surjective.

Proof If it is not surjective, then we may take $a \notin \text{im}(\phi)$, and $x^p - a$ is irreducible but not separable.

If it is surjective, then for each irreducible $f(x) \in p[x]$, we can write each coefficient as a power of p . Assume $f(x)$ is inseparable. Then $f'(x) = 0$, so $p \mid a_k$ for every non-multiples of p , and we are done.

Example 6.35 Every finite field is perfect.

6.13 Separable Extensions

Definition 6.22

K is called *separable over F* , if the minimal polynomial of every element in K is separable.

Example 6.36 Every extension of a field of characteristic 0 is separable, since every minimal polynomial over such a field is irreducible.

Example 6.37 If $\text{char}(K) = p$, L is an extension of K , and $p \nmid [L : K]$, then L is a separable extension.

Proof Let α be an algebraic element and f be its minimal polynomial. Then $[L : K] = [L : K(\alpha)] \deg(f)$. Suppose f is not separable, then $f' = 0$, so p divides the leading coefficient of f' , i.e., $\deg(f)$, and we are done.

Proposition 6.8

For every $n \in \mathbb{N}_1$, Φ_n has coefficients in \mathbb{Z} and is irreducible.

Proof Use $x^n - 1 = \prod_{d|n} \Phi_d(x)$ and Gauss's Lemma, we can inductively show that Φ_n must have integer coefficients.

Assume $\Phi_n(x) = f(x)g(x)$ where f is irreducible. Let ζ be a primitive n -th root and $p \nmid n$. Assume $g(\zeta^p) = 0$, so $f(x)$ is the minimal polynomial of ζ^p . Thus, $f(x)|g(x^p)$, and we have $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Reduce modulo p , we get $g(x)^p \equiv g(x^p) \equiv f(x)h(x)$. So f and g has a common root in an extension of \mathbb{F}_p . Thus, $x^n - 1$ is inseparable in \mathbb{F}_p , which leads to a contradiction. Therefore, $f(\zeta^p) = 0$ for all primes $p \nmid n$, and we are done.

6.14 Finite Fields

Proposition 6.9

The field of size p^n is unique up to isomorphism.

Proof Note that $x^{p^n} - x$ is a separable polynomial, and \mathbb{F}_{p^n} is the splitting field of this polynomial, and we are done.

Proposition 6.10

Let I_d be the set of irreducible polynomials of degree d . Then

$$x^{p^n} - x = \prod_{d|n} \prod_{f \in I_d} f(x).$$

Proof Let $f(x)$ be an irreducible polynomial of degree n , so $\mathbb{F}_p(\alpha)$ has size p^n and $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^n}$, so α is a root of $x^{p^n} - x$, and we are done.

6.15 Galois Groups

Definition 6.23

The *Galois group of the extension K/F* , denoted by $\text{Gal}(K/F)$, is defined by $\text{Gal}(K/F) = \{\sigma : K \rightarrow K : \sigma \text{ is an isomorphism}, \forall a \in F, \sigma(a) = a\}$.

Lemma 6.3

If $f(x) \in F[x]$ is a polynomial, $\alpha \in K$ is a root of $p(x)$ and $\sigma \in \text{Gal}(K/F)$, then $\sigma(\alpha)$ is also a root of $p(x)$.

Proof Note that $p(\sigma(\alpha)) = \sigma(p(\alpha)) = 0$, and we are done.

Example 6.38 $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathbb{Z}_2$, since $\sqrt{2}$ can only be mapped to $\pm\sqrt{2}$.

Example 6.39 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{e\}$, since $\sqrt[3]{2}$ can only be mapped to itself.

Definition 6.24

F/K is called *Galois* iff $|\text{Gal}(K/F)| = [K : F]$.

Example 6.40 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$, since $\sqrt{2}$ can only be mapped to $\pm\sqrt{2}$ and so is $\sqrt{3}$ and that they cannot be mapped to each other.

Example 6.41 The Frobenius endomorphism ϕ is in $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Note that ϕ has order n in the Galois group with order n . Hence, this Galois group is cyclic.

Proposition 6.11

If K/F is the splitting field of a separable polynomial, then K is Galois.

Proof By induction on $[K : F]$. If $g(x) \in F[x]$, K is the splitting field of $g(x)$ and α is a root of $g(x)$ that is not contained in F . Let $\alpha_1, \dots, \alpha_n$ be the set of roots of $g(x)$ in K since $g(x)$ is separable and splits in K . Thus, $\text{Gal}(K/F)$ acts on the roots by permuting elements. By the orbit-stabilizer theorem, $|Gx| = |G|/|\text{Stab}(x)|$. The action is transitive, since for each i , we can define σ_i by sending α to α_i since they have the same minimal polynomial. Also, the stabilizer is $\text{Gal}(K/F(\alpha))$. Therefore, $|\text{Gal}(K/F)| = n|\text{Gal}(K/F(\alpha))| = [F(\alpha), F][K : F(\alpha)] = [K : F]$, and we are done.

Example 6.42 Assume $f(x)$ is an irreducible cubic polynomial in $F[x]$, and K is its splitting field. Find all possibilities for the Galois group of K/F .

Proof The order is at most 6, so it is either a cyclic group of order 1 to 6, or the Klein four group V , or S_3 . Now that every element in the Galois group permute the roots, so any possibility of the Galois group must be embedded as a subgroup of S_3 , so $\mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6, V$ are not possible. Note that n must divide the order of the Galois group by the orbit-stabilizer theorem. Thus, the remaining possibilities are \mathbb{Z}_3, S_3 .

For \mathbb{Z}_3 , $x^3 - t$ is irreducible in $\mathbb{F}_3(t)$. The splitting field is $\mathbb{F}_3(t^{1/3})$ where $x^3 - t$ is purely inseparable and $3 = 0$ in \mathbb{F}_3 . We may also take $\mathbb{C}(t)$ and deduce that the Galois group is generated by $\sigma(t^{1/3}) = \zeta t^{1/3}$.

For S_3 , consider $x^3 - 2 \in \mathbb{Q}[x]$ which is a separable polynomial and we are done.

Example 6.43 The polynomial $x^p - t \in \mathbb{F}_p(t)$ generates a cyclic Galois group of order p .

Example 6.44 The polynomial $x^p - t \in \mathbb{C}_p(t)$ generates a cyclic Galois group of order p .

Proposition 6.12

Consider the field extension $F(t)/F$.

1. If $a, b, c, d \in F$ with $ad - bc \neq 0$, then the map

$$f(t) \mapsto f\left(\frac{at+b}{ct+d}\right)$$

is an automorphism of $F(t)$.

2. This is a surjective group homomorphism from $GL_2(F)$ to $\text{Gal}(F(t)/F)$.
3. The kernel exists the multiples of the identity matrix.
4. $\text{Gal}(F(t)/F)$ is isomorphic to $GL_2(F)/\{\lambda I : \lambda \in F^*\} \simeq PGL_2(F)$.

Proof The key is that every automorphism of $F(t)$ which fixes F is a linear fractional transformation. The point is that the image and preimage of t determines the automorphism.


6.16 Fixed Fields

Definition 6.25

If K be a field and $G < \text{Aut}(K)$, then the fixed field of G is $\text{Fix}(G) = \{a \in K : \forall \sigma \in G, \sigma(a) = a\}$.


The fixed field of G is always a field.

Lemma 6.4

If F is a field and G is a group, then the distinct homomorphisms χ_i 's from G to F^* are linearly independent. 

Proof Choose the minimal counterexample, say $a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0$ for all $g \in G$ where all $a_i \neq 0$. Take some $h \in G$ such that $\chi_1(h) \neq \chi_2(h)$. Then $0 = a_1\chi_1(h)\chi_1(g) + \cdots + a_n\chi_n(h)\chi_n(g)$, and we are done.

Proposition 6.13

If $G < \text{Aut}(K)$ and $F = \text{Fix}(G)$, then $[K : F] \geq |G|$. 

Proof Let $G = \{\sigma_1, \dots, \sigma_n\}$ and take a basis $\{y_1, \dots, y_m\}$ for K over F . Each y_i can be thought of a map by multiplication, representing an element of $\text{End}_F K$. $\{y_j\sigma_i\}$ has $mn > m^2$ elements, so we can find a linear dependence, say $\sum_{ij} a_{ij}y_j\sigma_i = 0$. Write $b_i = \sum_j a_{ij}y_j \in K$. Then $\sum b_i\sigma_i = 0$. Let H be the group of units in K , and we are done.


Proposition 6.14

If K/F is Galois, then $\text{Fix}(\text{Gal}(K/F)) = F$. 

Proof Let $L = \text{Fix}(\text{Gal}(K/F))$. Since $\text{Gal}(K/F)$ fixes all elements of F , we have $F < L < K$. By the previous proposition, we have that $[K : L] \geq |\text{Gal}(K/F)| = [K : F]$. By the tower law, $[K : L] \leq [K : F]$. Thus, $F = L$, and we are done.


6.17 Normal Extensions

Definition 6.26

K is called normal over F , if every irreducible polynomial splits in K . 

We can show that K is Galois iff it is normal and separable.

Proposition 6.15

If K/F is Galois, and $f(x) \in F[x]$ is irreducible, then it splits into distinct linear factors. 

Proof Let a_1, \dots, a_n be the distinct roots of $f(x)$ in K . If $\sigma \in \text{Gal}(K/F)$, then $\sigma(a_i) = a_j$ for some j . Let $g(x) = \prod_{i=1}^n (x - a_i)$. Thus, all coefficients of g is in the fixed field of the Galois group, i.e., F . So $g(x) \in F[x]$.

Proposition 6.16

If K is a field and $G < \text{Aut}(K)$, then $[K : F] = |G|$ where $F = \text{Fix}(G)$. 

Proof Assume $[K : F] > |G|$ and $G = \{\sigma_1, \dots, \sigma_n\}$. Assume $\sigma_1 = \text{id}$. Let $\{a_1, \dots, a_m\}$ be a basis of K over F and then $m > n$. Consider the system $\sigma_i(a_1) + \cdots + \sigma_i(a_m)x_m = 0$ for $1 \leq i \leq n$.

Let $x_1, \dots, x_m \in K$ be a non-trivial solution with the least number of non-zero entries. There must be some x_i such that $\sigma(x_i) \neq x_i$ since otherwise $x_i \in F$ for all i . Apply σ to get another solution $\sigma(x_1), \dots, \sigma(x_m)$. Hence, $x_1 - \sigma(x_1), \dots, x_m - \sigma(x_m)$ is another non-trivial solution with fewer non-zero entries, and we are done.

Proposition 6.17

K is Galois over F iff K is the splitting field of a separable polynomial. 

Proof Let K be a Galois extension over F and y_1, \dots, y_n be a basis of K over F . Let p_1, \dots, p_n be the minimal polynomials of y_1, \dots, y_n . Thus, each p_i splits completely in K . Hence, $f(x) = p_1(x) \cdots p_n(x)$ is separable and splits over K , and we are done.

6.18 The Fundamental Theorem of Galois Theory

Proposition 6.18 (The Fundamental Theorem of Galois Theory)

Let K/F be a Galois extension and $G = \text{Gal}(K/F)$. Then there is a bijection between the intermediate fields E such that $F \subset E \subset K$ and the subgroups $H < G$. More precisely, the bijection is given by $E \mapsto \{\sigma \in G : \forall x \in E, \sigma(x) = x\}$ and $H \mapsto \text{Fix}(H)$.

1. Containments are inclusion reversing.
2. $[K : E] = |H|$ and $[E : F] = [G : H]$.
3. K/E is always Galois with Galois group H .
4. E/F is Galois iff H is normal in G . In this case, $\text{Gal}(E/F) = G/H$.

Proof It suffices to prove the last statement.

On one hand, if E/F is Galois and $\sigma \in G$, then by roots argument, we can show that $\sigma(E) = E$. If $\tau \in H$, then $\sigma\tau\sigma^{-1}(a) \in E$, and we are done.

On the other hand, if $\text{Gal}(K/E)$ is normal, then for all $a \in E, \sigma \in G, \tau \in H$, we have $\sigma\tau\sigma^{-1}(a) = a$. It suffices to show it is normal. Let $a \in E$. Let $p(x)$ be its minimal polynomial. Since $\{\sigma(a) : \sigma \in G\} \subset K$ contains all roots of $p(x)$, so $\tau\sigma(a) = \sigma\tau^{-1}\tau\sigma(a) = \sigma(a)$. Hence, $\sigma(a) \in E$, and we are done.

Example 6.45 If $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of degree 5 containing exactly 3 real roots. Show that the Galois group of $f(x)$ is S_5 .

Proof Denote them by $r_1, r_2, r_3, s, \bar{s}$. 5 divides the order of the Galois group, and there is a transposition. Thus, the Galois group is isomorphic to S_5 .

6.19 Applications of the Fundamental Theorem of Galois Theory

Definition 6.27

K is called simple over F iff $K = F(\theta)$ for some $\theta \in K$.

Proposition 6.19

If K/F is a finite field extension, then K is simple over F iff there are finitely many intermediate fields $F \subset E \subset K$.

Proof Assume F has infinitely many elements and $\alpha, \beta \in K$. It suffices to show that $F(\alpha, \beta)$ is simple over F . Let $c \in F$ and consider $F \subset F(\alpha + c\beta) \subset F(\alpha, \beta)$. Choose some $c \neq c'$ such that $F(\alpha + c\beta) = F(\alpha + c'\beta)$. Thus, $(c - c')\beta \in F(\alpha + c\beta)$, so $\beta, \alpha \in F(\alpha + c\beta)$, and we are done.

Example 6.46 If K/F is finite and separable, then it is simple.

Proof Let L be the splitting field of the product of the minimal polynomials of a basis of K over F . Use the fundamental theorem, and we are done.

Example 6.47 Assume L is a finite Galois extension of K with characteristic 0. If L is not contained in \mathbb{R} , show that $|G|$ is even.

Proof Note that the complex conjugation is in the Galois group and that 2 divides $|G|$, and we are done.

Example 6.48 Assume L is a finite Galois extension of K with characteristic 0. If the minimal polynomial of α has at least a real root and at least a nonreal root, then G is nonabelian.

Proof Consider the conjugation and σ of order n in G . Consider $r \in \mathbb{R}$ such that $\sigma(r) \notin \mathbb{R}$, and we are done.

6.20 Cyclotomic Extensions

Example 6.49 $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$.

Definition 6.28

A Galois extension K/F is called *abelian*, if $\text{Gal}(K/F)$ is abelian.

**Proposition 6.20**

If G is a finite abelian group, then there is a Galois field extension F/\mathbb{Q} with the Galois group isomorphic to G .



Proof It suffices to show that there is some $n \in \mathbb{N}_1$ such that G is a quotient group of \mathbb{Z}_n^\times . Write G in the invariant factors form. It suffices to show the largest invariant factor n can divide some $p - 1$. But this is immediately by the special case of Dirichlet's theorem.