Graduate Algebra: 2021 - 2023

Compiled by J. Liu
University of California,
Los Angeles

Abstract

This book contains a compilation of lecture notes based on the graduate algebra courses at UCLA, taught by Dr. Merkurjev.
Current Version Number: 0.2025.5.29

Contents

List of Figures

1 Group Theory

1.1 Introduction

Definition 1.1.1 (Group). *A group G is a set G with a binary operation $\cdot : G \times G \to G$ that $(x, y) \mapsto xy = x \cdot y$ such that:*

1. *Associativity: $\forall x, y, z \in G$, $(xy)z = x(yz)$.*

2. *Existence of Unit: $\exists e \in G$ such that $ex = xe = x$ $\forall x \in G$.*

3. *Existence of Inverses: $\forall x \in G$, $\exists y \in G$ such that $xy = yx = e$.*

Remark 1.1.2.

1. *Element $e \in G$ given by 2) is unique. Indeed, suppose we also have $e' \in G$ as the unit, then $xe' = e'x = x$ and so $e' = e'e = e$.*

2. *Element $y \in G$ given in 3) is uniquely determined by $x \in G$. Consider $xy' = y'x = e$ for some other $y' \in G$, then $y' = e \cdot y' = (yx)y' = y(xy') = y \cdot e = y$. In particular, we write $y \in G$ as $y = x^{-1} \in G$.*

3. *Note that $xyz = (xy)z = x(yz)$ and $xyzt = ((xy)z)t = (x(yz))t = (yx)(zt) = x(y(zt)) = x((yz)t)$. This can be generalized by induction.*

Definition 1.1.3 (Abelian/Commutative Group). *If 4) commutativity: $xy = yx$ $\forall x, y \in G$ holds for a group G, then G is abelian (communitative).*

Remark 1.1.4. *If a group is abelian, we use $+$ to denote the binary operation. In particular, we can rewrite the group definition as:*

1. *$(x + y) + z = x + (y + z)$.*

2. *$\exists 0 \in G$ such that $0 + x = x + 0 = x$ for all $x \in G$.*

3. *$\forall x \in G$, $\exists y = -x \in G$ such that $x + (-x) = 0 \in G$.*

4. *We also denote $x - y = x + (-y)$.*

Remark 1.1.5. *Groups also have cancellation laws.*

1. *Left cancellation: $xy = xz$ indicates $y = z$ for all $x, y, z \in G$. Indeed, $x^{-1}(xy) = x^{-1}(xy)$, and therefore $y = z$.*

2. *Right cancellation: $yx = zx$ indicates $y = z$ for all $x, y, z \in G$.*

3. *Usually $xy = zx$ does not indicate $y = z$.*

4. *We also have $(xy)^{-1} = y^{-1}x^{-1}$ and $(x^{-1})^{-1} = x$.*

Example 1.1.6. 1. *Trivial Group: $G = \{e\}$.*

2. *Addition Group of Integers $\mathbb{Z}$.*

3. *For positive integer n, $\mathbb{Z}/n\mathbb{Z} = \{[a]_n\}$ for $a \in \mathbb{Z}$ where $[a]_n = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$. The operation is defined as $[a]_n + [b]_n = [a + b]_n$. The unit of the group is $[0]_n$. The inverse is $-[a]_n = [-a]_n$ for all $[a]_n \in \mathbb{Z}/n\mathbb{Z}$.*

4. *$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups with respect to addition. Notice that the operation is part of a group's definition. Moreover, these structures are not groups with respect to multiplication since there is the zero element.*

5. *Multiplication groups $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{R}^*\backslash\{0\}$, $\mathbb{C}^*\backslash\{0\}$.*

6. *Klein-4 Group $G = \{e, a, b, c\}$.*

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

7. *Symmetric Group $\Sigma(X)$ of set X. Define $\Sigma(X) = \{f : X \to X \text{ bijection}\}$. For $f, g \in \Sigma(X)$, we define $f \circ g = f(g(x))$. Similarly $(f \circ g) \circ h = f \circ (g \circ h)$ for all $f, g, h \in \Sigma(X)$.*

   - *Notice that if X is a finite set, then $card(\Sigma(X)) = card(X)!$.*
   - *$\Sigma(X)$ is not abelian if $card(X) > 2$.*

8. *Consider ring R, e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. For positive integer n, consider $GL_n(R) = \{n \times n$ invertible matrix with entries in $R\}$ as a group. This is called the general linear group of R.*
   - *We say A is invertible if there exists B such that $AB = BA = I_n$.*
9. *Let G and H be groups. Then $G \times H = \{(g, h) : g \in G, h \in H\}$ where $(g, h) \cdot (g', h') = (gg', hh')$ and $e_{G\times H} = (e_G, e_H)$.*
10. *We say a group G is finite if the order of the group $|G| = card(G) < \infty$.*

Algebra studies the relations between different algebraic structures in general. Relations between groups are given by homomorphisms.

1.2 Homomorphism

Definition 1.2.1 (Group Homomorphism)**.** *For groups G, H, a map $f : G \to H$ is called a homomorphism if $f(x \cdot_G y) = f(x) \cdot_H f(y)$ for all $x, y \in G$.*

Example 1.2.2. *1. Identity $id : G \to G$ that maps every element $g \in G$ to itself.*

2. Trivial homomorphism $f : G \to H$ that maps every element $g \in G$ to $e_H \in H$.

Property 1.2.3. *1. $f(e_G) = e_H$. Note that $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$, and therefore $e_H \cdot f(e_G) = f(e_G) \cdot f(e_G)$. By cancellation law, $f(e_G) = e_H$.*

2. $f(x^{-1}) = f(x)^{-1}$. Note that $e_H = f(e_G) = f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1})$, then $f(x^{-1}) = f(x)^{-1}$ by definition.

Remark 1.2.4. *Composition of homomorphisms is a homomorphism.*

Definition 1.2.5 (Isomorphism)**.** *A homomorphism $f : G \to H$ is an isomorphism if f is a bijection. Two groups G and H are isomorphic if there exists an isomorphism $f : G \to H$, denoted $G \cong H$.*

Remark 1.2.6. *1. $id : G \to G$ is an isomorphism.*

2. If there is an isomorphism $f : G \to H$, then $f^{-1} : H \to G$ is also an isomorphism.

3. Let $h = f(g)$, $h' = f(g')$ for some $g, g' \in G$. Then $hh' = f(g)f(g') = f(gg')$, and so $f'(hh') = gg' = f^{-1}(h)f^{-1}(h')$.

4. *If f, g are isomorphisms, then $g \circ f$ is an isomorphism.*

Claim 1.2.7. $\cong$ *is an equivalence relation.*

Proof. This is a direct result of remark 1.2.6, we can conclude reflexivity, symmetry and transitivity respectively. □

Example 1.2.8. 1. *If $|G| = |H| = 1$, then $G \cong H$.*

2. *Two finite groups are isomorphic if they have the same multiplication table.*

3. *Every two groups of order 2 are isomorphic. Moreover, they are all isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

4. *$\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$. (We can obviously construct it by $\mathbb{R}[x]/(x^2+1)$.) Furthermore, we have $f : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$ by mapping $f(a, b) = a + bi$ for arbitrary $a, b \in \mathbb{R}$.*

5. *$\mathbb{R}^+ \cong \mathbb{R}^{x,>0}$. Consider $f(x) = e^x$ with $f(x + y) = f(x) \cdot f(y)$.*

1.3 Cyclic Group

Definition 1.3.1 (Order, Generator, Cyclic Group)**.** *Consider arbitrary group G with $x \in G$ and some $n > 0$. We define x^n as the n-term multiplication of x, and $x^0 = e$ with $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.*

For $x \in G$, we say the smallest $n > 0$ such that $x^n = e$ is the order of x. If such n does not exist, we say the order is ∞.

For a group G, $x \in G$ is a generator of G if $\forall y \in G$, $y = x^n$ for some $n \in \mathbb{Z}$.

A group G is cyclic if G has a generator.

Remark 1.3.2. *For abelian groups, we write nx as the n-term summation of x, and $0 \cdot x = 0 \in G$, with $(-n)x = -(nx) = n \cdot (-x)$.*

Example 1.3.3. 1. *$\mathbb{Z}$ is a cyclic group with generators 1 and -1.*

2. *Take $0 < n \in \mathbb{Z}$, then $\mathbb{Z}/n\mathbb{Z}$ is cyclic. The generators are $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ with some $1 \le a \le n-1$ such that $\gcd(a, n) = 1$. Moreover, the number of generators is exactly $\varphi(n)$, where φ is the Euler Function.*

Theorem 1.3.4. *Every cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n > 0$.*

Proof. Case 1: suppose $|G| = \infty$. Let $g \in G$ be a generator. Define $f : \mathbb{Z} \to G$ with $f(m) = g^m$. Obviously f is onto because g is a generator. Now suppose $g^k = g^m$ for some $k > m$. Then $g^{k-m} = e$ with $k - m > 0$. Hence, the order of g has to be finite. Then G cannot have infinite cardinality, contradiction. Hence f is a bijection. Therefore, f is an isomorphism, $\mathbb{Z} \cong G$.

Case 2: suppose $|G| = n$ finite. Let $g \in G$ be a generator. Obviously $\text{ord}(g) < \infty$. We claim that $\text{ord}(g) = n$. Suppose $\text{ord}(g) = m$ for some $m > 0$. We can check that $g^0 = e, g, g^2, \cdots, g^{m-1}$ are all the elements in G. Indeed, $g^m = e$, and suppose $g^i = g^j$ for some $0 \leq j < i \leq m - 1$, then $g^{i-j} = e$ for $0 < i - j < m$. Since m is the order, we have a contradiction. Hence, $|G| = m = n$.

Now take $f : \mathbb{Z}/n\mathbb{Z} \to G$ with $f([a]_n) = g^a$. We check that $[a]_n = [b]_n$ indicates $g^a = g^b$. Indeed, $b \equiv a \pmod{n}$ indicates $b = a + nc$, which means $g^b = g^{a+nc} = g^a$. This concludes the proof. □

Remark 1.3.5.

1. *If G is cyclic with generator $g \in G$, then $|G| = ord(g)$.*
2. *Let G, H be cyclic. Then $G \cong H$ if and only if $|G| = |H|$.*
3. *The number of generators in a cyclic group of order n is $\begin{cases} 2 \text{ if } n = \infty \\ \varphi(n) \text{ if } n < \infty \end{cases}$.*
4. *Consider a finite group G with the isomorphism $f : \mathbb{Z}/n\mathbb{Z} \to G$ that maps $[1]_n \mapsto f([1]_n)$, with $[2]_n \mapsto f([1]_n)^2$. Note that such maps must preserve generators. i.e. $f([1]_n)$ is always a generator, and can be any generator of G. In particular, f is uniquely determined by $f([1]_n)$. There are $\varphi(n)$ isomorphisms between $\mathbb{Z}/n\mathbb{Z}$ and G (or any two cyclic groups of order n).*

1.4 Subgroup

Definition 1.4.1 (Subgroup)**.** *Consider group G with subset $H \subseteq G$. Assume $\forall h, h' \in H$ we have $h \cdot_G h' \in H$. Then H is a subgroup of G if H is a group with respect to $\cdot_G$.*

Proposition 1.4.2. *Let G be a group and $H \subseteq G$ is a subset. Then H is a subgroup if and only if the following holds:*

1. *$\forall h, h' \in H$, $hh' \in H$.*
2. *$e \in H$, i.e. H is not empty.*

3. *$\forall h \in H$, $h^{-1} \in H$.*

Proof. If the three properties hold, then H is a group, and so H is a subgroup of G.

Suppose H is a subgroup then it is obviously closed. Let $e' \in H$ be the unit, then $e' \cdot h = e \cdot h = h$ for all $h \in H$. Then $e' = e \in H$ by cancellation. Take $h \in H$, then there is $h' \in H$ such that $hh' = e$. Moreover, $h^{-1}hh' = h^{-1}e = h^{-1}$. Hence, $h' = h^{-1} \in H$. □

Example 1.4.3. 1. *$\{e\}, G \subseteq G$ are subgroups.*

2. *There exists a sequence of subgroups: $n\mathbb{Z} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.*

3. *There is also a list of subgroups $\mathbb{Q}^\times \subseteq \mathbb{R}^\times \subseteq \mathbb{C}^\times$. Note that $\mathbb{Q}^\times$ is not a subgroup of $\mathbb{Q}$ since they hold different operations.*

4. *Let $(H_i)_{i\in I}$ be a family of subgroups of G. Then $\bigcap\limits_{i\in I} H_i$ is a subgroup of G. In general, $\bigcup\limits_{i\in I} H_i$ is not a subgroup.*

Definition 1.4.4. *(Kernel, Image) Let $f : G \to H$ be a group homomorphism, with $f(gg') = f(g)f(g')$. Then $\ker(f) = \{g \in G : f(g) = e_H\}$ and im$(f) = \{h \in H : h = f(g)$ for some $g \in G\}$.*

Proposition 1.4.5. $\ker(f)$ *is a subgroup of G and im(f) is a subgroup of H.*

Proof. We prove the first claim.

Note that for all $g, g' \in \ker(f)$, we have $f(g) = f(g') = e$, which means $f(gg') = f(g)f(g') = e$. Hence, $gg' \in \ker(f)$.

Since $f(e_G) = e_H$, then $e_G \in \ker(f)$.

If $g \in \ker(f)$, then $f(g^{-1}) = f(g)^{-1} = e^{-1} = e$. □

Proposition 1.4.6. *Let $f : G \to H$ be a group homomorphism. Then:*

1. *f is surjective if and only if im$(f) = H$.*

2. *f is injective if and only if* $\ker(f) = \{e_G\}$.

3. *f is an isomorphism if im$(f) = H$ and* $\ker(f) = \{e_G\}$.

Proof. Part 1 and part 3 are obvious. We only have to prove part 2.

If f is injective, take $g \in \ker(f)$, then $f(g) = e_H$. Therefore, $f(g) = e_H = f(e_G)$, then $g = e_G$ by injection.

If $\ker(f) = \{e_G\}$, then consider $f(g) = f(g')$. Then $f(g^{-1}) \cdot f(g) = f(g^{-1}) \cdot f(g')$ and so $e_H = f(g^{-1}) \cdot f(g') = f(g^{-1}g')$. That means $g^{-1}g' = e_G$ and so $g' = g$. □

Example 1.4.7. 1. *Suppose $H \subseteq G$ is a subgroup. Then the inclusion map inc : $H \to G$ is injective defined as $inc(h) = h$ for all $h \in H$.*

2. *Consider an injective homomorphsim $f : H \to G$ for groups G, H, then $f' : H \to im(F)$ with $f'(h) = f(h)$ defined is an isomorphism. Then H is isomorphic to a subgroup of G, i.e. $H \cong im(f) \subseteq G$.*

3. *Let G be a group with $g \in G$. Then consider $f_g : G \to G$ with $f_g(x) = gx$. Note that $f_g \circ f_{g'} = f_{gg'}$ for all $g, g' \in G$. Moreover, $f_e = id_G$.*

   Note that f_g is a bijection because $f_g \circ f_{g^{-1}} = f_e = id_G = f_{g^{-1}} \circ f_g$ and so $f_{g^{-1}} = (f_g)^{-1}$. Therefore, $f_g \in \sum(G)$. Notice that f_g may not be a homomorphism.

   However, consider $f : G \to \sum(G)$ by $f(g) = f_g$, then f is a homomorphism. Furthermore, f is injective: if $g \in \ker(f)$, then $f_g = id_G$, hence $f_g(x) = x$ for all $x \in G$. Therefore, by definition $gx = x$ for all $x \in G$, which means $g = e_G$. Thus, f is injective. Following from the argument above, we know G is isomorphic to a subgroup of $\sum(G)$.

   Note that if $|G| = n$, then $\sum(G) = S_n$, the n-th symmetric group. Every finite group is contained in some symmetric group.

Definition 1.4.8. *(Coset) Suppose S, T to be subsets of a group G. Then define $S \cdot T = \{s \cdot t : s \in S, t \in T\} \subseteq G$.*

Note that if $S = \{s\}$, then $ST = sT$. Similarly if $T = \{t\}$ then $ST = St$.

Let $H \subseteq G$ be a subgroup, with $x \in G$. Then xH is the left coset of H in G, and Hx is the right coset of H in G.

Property 1.4.9. 1. *$(S \cdot T) \cdot V = S \cdot (T \cdot V)$.*

2. *If $H \subseteq G$ is a subgroup, then $H \cdot H = H$.*
   - *$\forall h, h' \in H$, $hh' \in H$, and so $H \cdot H \subseteq H$.*
   - *$\forall h \in H$, we have $h = h \cdot e \in H \cdot H$, therefore $H \subseteq H$.*

Lemma 1.4.10. *$xH = H \iff x \in H \iff Hx = H$.*

Proof. We prove the equivalence of the first two statements.

If $xH = H$, then $x = x \cdot e \in xH = H$. If $x \in H$, then $xH \subseteq H \cdot H = H$, and for all $h \in H$, $h = x \cdot (x^{-1} \cdot h) \in xH$. Hence, $xH = H$.

Note that $xH = yH$ if and only if $(y^{-1}x)H = H$ if and only if $y^{-1}x \in H$. Similarly $Hx = Hy$ if and only if $yx^{-1} \in H$. □

Remark 1.4.11. *Note that $xH = yH \iff (y^{-1}x)H = H \iff y^{-1}x \in H$. Similarly $Hx = Hy \iff yx^{-1} \in H$.*

Proposition 1.4.12. *Let $H \subseteq G$ be a subgroup, then xH and yH are either disjoint or equal.*

Proof. Consider xH and yH that are not disjoint. Then there is $z \in xH \cap yH$, which means $z \in xH$ and $z \in yH$. By definition, since $z \in xH$, then $zH = xH$, and similarly we have $zH = yH$, hence $xH = yH$. Therefore, they are equal. □

Remark 1.4.13. *Note that G is the disjoint union of left (right) cosets.*

Definition 1.4.14 (Index)**.** *Let G be a group with subgroup $H \subseteq G$. Index of H in G, denoted as $[G : H]$, is the number of left/right cosets of H in G.*

Theorem 1.4.15 (Lagrange)**.** *Let G be a finite group with subgroup $H \subseteq G$. Then $|G| = |H| \cdot [G : H]$. In particular, $|H|$ divides $|G|$.*

Proof. It suffices to show that $\text{card}(xH) = \text{card}(yH)$ for all $x, y \in G$. Notice that $H \to xH$ given by $h \mapsto xh$ is a bijection, therefore the cardinalities all equal to the cardinality of H. Hence, the cardinalities agree. □

Corollary 1.4.16. *Let G be a finite group with $x \in G$. Then 1) $\text{ord}(x) \mid G$ and 2) $x^{|G|} = e$.*

Proof.

1. Let $\text{ord}(x) = n$, then $\langle x \rangle = \{e, x, x^2, \cdots, x^{n-1}\}$ is a cyclic subgroup of G with order n. Therefore $|\langle x \rangle| \mid |G|$, hence the order of a divides the order of G.
2. We write $|G| = nk$ with $\text{ord}(x) = n$. Then $x^{|G|} = (x^n)^k = e^k = e$.

□

Example 1.4.17. *Let $n > 0$. Then $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n : \gcd(a, n) = 1\}$ is a group of order $\varphi(n)$. Since $\gcd(a, n) = 1$, then $[a]_n^{\varphi(n)} = [1]_n$ and so $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Corollary 1.4.18. *Every group of prime order is cyclic.*

Proof. Take $|G| = p$, then $\exists e \neq x \in G$. As $\text{ord}(x) \mid |G|$ then $\text{ord}(G)$ is either 1 or p. However, since $x \neq e$, then $\text{ord}(x) = p$. Therefore $G = \langle x \rangle$. □

Proposition 1.4.19. *Let G be a group of order $2n$; then G contains an element of order 2. If n is odd and G Abelian, there is only one element of order 2.*

Proof. Suppose not, then for every $e \neq g \in G$, we have $g \neq g^{-1}$, so we group pairs of elements by g and g^{-1}. Note that there is one element left. In particular, this element does not have a distinct inverse, which means it has order 2, contradiction.

We now show that this element is unique if n is odd and G is Abelian. Suppose not, then we have h_1, h_2 with order 2. But now $\{e, h_1, h_2, h_1h_2\}$ is a group of order 4. By Lagrange's Theorem, we have a contradiction. □

Definition 1.4.20 (Normal)**.** *Let $H \subseteq G$ be a subgroup. We say H is normal in G or $H \lhd G$ if $xH = Hx$ for all $x \in G$.*

Example 1.4.21. *1. If G is abelian, every subgroup H is normal.*

2. $\{e\}, G \lhd G$.

Proposition 1.4.22. *Let $H \subseteq G$ be a subgroup, then $H \lhd G$ if and only if $xHx^{-1} \subseteq H$ for all $x \in G$.*

Proof. If $H \lhd G$, then $xH = Hx$ and so $xHx^{-1} = Hxx^{-1} = H \subseteq H$.

Suppose $xHx^{-1} \subseteq H$, then $xHx^{-1}x \subseteq Hx$, hence $xH \subseteq Hx$. Similarly as $x^{-1}Hx \subseteq H$, then $Hx \subseteq xH$, and so $xH = Hx$, so H is normal in G. □

Example 1.4.23. *1. $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$, with $SL_n(\mathbb{R})$ as the set of $n \times n$ matrices with determinant 1. Indeed, take $A \in SL_n(\mathbb{R})$ and $B \in GL_n(\mathbb{R})$, we have $\det(BAB^{-1}) = \det(B)\det(A)\det(B)^{-1} = 1$.*

2. Note that if $H \lhd G$, then $(xH) \cdot (yH) = x(Hy)H = x(yH)H = (xy)H$. Let G/H be the set of all cosets $xH = Hx$. Operation $(xH) \cdot (yH) = (xy)H$ is well-defined if and only if $H \lhd G$.

Proposition 1.4.24. *Suppose G is a group and K and H are subgroups, satisfying $K \subseteq H \subseteq G$ and $H \lhd G$. Show that if H is cyclic, then $K \subseteq G$.*

Proof. Since H is cyclic, one can write $H = \langle h \rangle$ for some $h \in G$. In particular, since K is a subgroup of H, it must have the form $K = \left\langle h^k \right\rangle$ as a cyclic group as well.

Take arbitrary $g \in G$, and it suffices to show that $gKg^{-1} \subseteq K$. Since $H \lhd G$, there is $ghg^{-1} = h^n$ for some integer n. We then have $(ghg^{-1})^k = (h^n)^k$, which is just $gh^kg^{-1} = h^{nk}$. Now take arbitrary element $(h^k)^a \in K$, then for $g \in G$, we have $g(h^k)^a g^{-1} = (gh^kg^{-1})^a = h^{nka} = (h^n)^{ka} \in K$. By definition, $gKg^{-1} \subseteq K$ for all $g \in G$. Therefore, $K \subseteq G$. □

Example 1.4.25. *Consider $G = D_8$, and let a be of order 2 and b be of order 4, satisfying $abab = e$. Then $H = \left\langle a, b^2 \right\rangle$ has order 4, which is normal in G. Also, $K = \langle a \rangle$ has order 2 so it is normal in H. But one can show that K is not normal in G, otherwise $bab^{-1} \in \langle a \rangle$, which means $bab^{-1} = a$, so $ba = ab$, contradiction.*

This is an example of subgroups $K \lhd H \lhd G$, where K is not normal in G.

Claim 1.4.26. *If $H \lhd G$, G/H is a group.*

Proof.

1. $(xH \cdot yH) \cdot zH = (xyH) \cdot zH = (xy)zH = x(yz)H = xH \cdot (yH \cdot zH)$.
2. $e_{G/H} = H$, then $xH \cdot H = xH$, $H \cdot xH = e_H \cdot xH = xH$.
3. $(xH)(x^{-1}H) = eH = H = (x^{-1}H)(xH)$.

□

Remark 1.4.27. *The group G/H called the factor group of G by H.*

Property 1.4.28. *Consider $f : G \to G/H$ such that $x \mapsto xH$. Observe that $f(xy) = (xy)H = xH \cdot yH = f(x) \cdot f(y)$. Also note that f is surjective. Furthermore, $x \in \ker(f) \iff f(x) = e_{G/H} = H \iff xH = H \iff x \in H$. Therefore, $\ker(f) = H$.*

Remark 1.4.29. *The group homomorphism $f : G \to G/H$ defined in 1.4.28 is called the canonical homomorphism.*

Example 1.4.30.

1. *$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} = [a]_n\}$.*
2. *$\mathbb{C}/\mathbb{R}$. For $z \in \mathbb{C}$, $z + \mathbb{R}$ is the set of horizontal lines on $\mathbb{R}$-$\mathbb{C}$ plane.*
3. *$\mathbb{C}^\times/U$ for $U = \{z \in \mathbb{C}, |z| = 1\}$. For $z \in \mathbb{C}^\times$, $z \cdot U$ are the circles on the plane.*

Proposition 1.4.31 (Universal Property)**.** *Let $f : G \to H$ be a group homomorphism, and $N \lhd G$ such that $N \subseteq \ker(f)$. Then $\exists!$ group homomorphism $\bar{f} : G/N \to H$ such that $f = \bar{f} \circ \pi$, where $\pi : G \to G/N$ is the canonical homomorphism.*

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\pi"] & & H \\
& G/N \arrow[ur, dashed, "\exists!\bar{f}"] &
\end{tikzcd}$$

Figure 1.1: Universal Property of Group Homomorphism

Proof. Uniqueness: Suppose there exists $\bar{f}$ such that $f = \bar{f} \circ \pi$. For $x \in G$, $f(x) = \bar{f}(\pi(x)) = \bar{f}(xN)$. Therefore defining $\bar{f}(xN) = f(x)$ is unique.

Existence: We show $\bar{f}(xN) = f(x)$ is well-defined. For $xN = yN$ show $f(x) = f(y)$. $N = x^{-1}yN$ and so $x^{-1}y \in N \subseteq \ker(f)$. Hence, $f(x^{-1}y) = e_H$, so $f(x) = f(y)$.

We can also show that $\bar{f}$ is a group homomorphism. $\bar{f}(xN \cdot yN) = \bar{f}(xyN) = f(xy) = f(x)f(y) = \bar{f}(xN) \cdot \bar{f}(yN)$. Therefore, $\bar{f}$ is homomorphsim. □

1.5 Isomorphism Theorems

Lemma 1.5.1. *Let $f : G \to H$ be a group homomorphism. Then* $\ker(f) \lhd G$.

Proof. For $x \in \ker(f)$, $y \in G$, then $f(yxy^{-1}) = f(y)f(x)f(y)^{-1} = f(y)f(y)^{-1} = e$. So $yxy^{-1} \in \ker(f)$, hence $\ker(f) \lhd G$.

Note if $\pi : G \to G/H$ for group $H \subseteq G$ (not normal), with $\ker(f) = H$, then $H \lhd G$. □

Remark 1.5.2. *Let $f : G \to H$ be a homomorphism with $N = \ker(f) \lhd G$. By the universal property 1.4.31, $\exists! \bar{f} : G/N \to H$ such that the universal property holds with $\bar{f}(xH) = f(x)$. Then $\bar{f} : G/N \to im(f)$ is surjective.*

Theorem 1.5.3 (First Isomorphism Theorem)**.** *$\bar{f} : G/N \to im(f)$ is an isomorphism.*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"] & H \\ G/N \arrow[r, "\bar{f}"] & \mathrm{im}(f) \arrow[u, "inc"'] \end{tikzcd}$$

Figure 1.2: First Isomorphism Theorem

Proof. It suffices to show that $\ker(\bar{f}) = e_{G/N}$.

Take $xN \in \ker(\bar{f})$ for some $x \in G$. Note $f(x) = \bar{f}(xN) = e_H$, so $x \in \ker(f) = N$, hence $xN = N$. □

Remark 1.5.4. *Note that for $N \lhd G$, if homomorphism $f : G \to H$ is surjective, then $G/N \cong H$.*

Example 1.5.5.

1. *$\mathbb{C}/\mathbb{R} \cong \mathbb{R}$. $f : \mathbb{C} \to \mathbb{C}$ for $f(x + yi) = y$ is surjective with* $\ker(f) = \mathbb{R}$.

2. *$\mathbb{C}^\times/U$ where $U = \{z \in \mathbb{C} : |z| = 1\}$ has the property $\mathbb{C}^\times/U \cong \mathbb{R}^{\times,>0}$. Here $f : \mathbb{C}^\times \to \mathbb{R}^{\times,>0}$ with $f(z) = |z|$.*

Theorem 1.5.6 (Second Isomorphism Theorem)**.** *Let K, N be two subgroups of G with $N \lhd G$. Then:*

1. *KN is a subgroup of G.*

2. *$N \lhd KN$ and $K \cap N \lhd K$, and $KN/N \cong K/(K \cap N)$.*

Proof. 1. $e_G = e_K \cdot e_N \in KN$.

$(k_1 n_1)(k_2 n_2) = (k_1 k_2)[(k_2^{-1} n_1 k_2) n_2] \in KN$.

$(kn)^{-1} = n^{-1}k^{-1} = k^{-1}(kn^{-1}k^{-1}) \in KN$.

2. $n = e \cdot n \in KN$, $N \subseteq KN$, then since $N \lhd G$, we have $N \lhd KN$.

Consider $K \xhookrightarrow{f} KN \xrightarrow{\pi} KN/N$ defined by $f(k) = kN$ and π as the canonical homomorphism.

Note that f is surjective: $(k \cdot n) \cdot N = k \cdot N = f(k)$.

Now $k \in \ker(f) \iff f(k) = e_{k \cdot N/N} = N \iff k \cdot N = N \iff k \in K \cap N$. Then $\ker(f) = L \cap N \lhd K$.

By the first isomorphism theorem **1.5.3**, $K/(K \cap N) \cong KN/N$.

□

Theorem 1.5.7 (Third Isomorphism Theorem)**.** *Let K and H be two normal subgroups of a group G such that $K \subseteq H$. Then:*

1. *$H/K \lhd G/K$.*

2. *$(G/K)/(H/K) \cong G/H$.*

Proof. Consider $G \xrightarrow{\pi_1} G/K \xrightarrow{\pi_2} (G/K)/(H/K)$.

1. First note $h \in H, g \in G$, then $(gK) \cdot (hK) \cdot (gK)^{-1} = (ghg^{-1})K \in H/K$. Hence $H/K \lhd G/K$.

2. $x \in \ker(f) \iff \pi_1(x) \in \ker(\pi_2) = H/L \iff x \in H$. Therefore, $\ker(f) = H$. By the first isomorphism theorem, $(G/K)/(H/K) \cong G/H$.

□

Example 1.5.8. *Consider $n, m > 0$, $nm\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$, then $(\mathbb{Z}/nm\mathbb{Z})/(n\mathbb{Z}/nm\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.*

1.6 Group Actions

Definition 1.6.1 (Group Action). *Let G be a group and X be a set. A G-action on X is a map $G \times X \to X$ by $(g, x) \mapsto gx = g \cdot x$, called the action on x, such that:*

1. *$e \cdot x = x$ for all $x \in X$.*
2. *$g_1(g_2x) = (g_1g_2)x \; \forall g_1, g_2 \in G, x \in X$.*

Example 1.6.2.

1. *Trivial Action $g \cdot x = x$.*
2. *$\sum(X)$ acts on X, for $g \in \sum(X)$ we have $g : X \xrightarrow{\cong} X$, so for $x \in X$ we have $g \cdot x = g(x)$.*
3. *If H acts on X and $f : G \to H$ is a homomorphism, then G acts on X by $g \cdot x = f(g) \cdot x$. This is the pullback action with respect to f.*
4. *G acts on G as the left translation: $g \cdot x = gx$. Then $G \to \sum(G)$ is injective, so $G \cong A$ for some subgroup $A \subseteq \sum(G)$.*
5. *G acts on G by conjugation: $g * x = gxg^{-1}$.*
6. *If $H \subseteq G$ is a subgroup, take $X = G/H$ as the set of left cosets, then G acts on X with $g \cdot (aH) = g(aH) = gaH$.*

Remark 1.6.3. *For G acts on X, $g \in G$, consider $f_g : X \to X$ defined as $f_g(x) = gx$, $f_e = id$ as $f_e(x) = x$ and $f_{g_1} \circ f_{g_2} = f_{g_1g_2}$, and $f_g \circ f_{g^{-1}} = id = f_{g^{-1}} \circ f_g$. Then f_g is a bijection, which means $f_g \in \sum(X)$. Then $f : G \to \sum(X)$ defined by $g \mapsto f_g$ is a homomorphism.*

In particular, there exists a bijective correspondence between G-actions on X and $Hom(G, \sum(X))$, the set of homomorphisms from G to $\sum(X)$. This map takes $g \cdot x = f(g)(x)$, the pullback of the natural $\sum(X)$-action on X (universal action) with respect to f, to $f : G \to \sum(X)$. Moreover, there is a correspondence between the trivial action and the trivial homomorphism.

Example 1.6.4.

1. *An automorphism of G is an isomorphism $G \xrightarrow{\cong} G$. $Aut(G)$ is the automorphism group of G.*

   For arbitrary $x \in G$, consider $f_x : G \to G$ defined by $f_x(g) = xgx^{-1}$, then f_x is homomorphism. Furthermore, f_x is a bijection, then f_x is an isomorphism. Note $id_G = f_{x^{-1}} \circ f_x = f_x \circ f_{x^{-1}}$ and $f_x(gg') = xgg'g^{-1} = xgx^{-1}xg'x^{-1} = f_x(g)f_x(g')$.

Here, we say $f_x \in Aut(G)$ is an inner automorphism of G.

Consider G acts on $X = G$ by $x * g = xgx^{-1}$, defined by $G \to \sum(X)$, $x \mapsto f_x \in Aut(G)$, $G \xrightarrow{f} Aut(G) \hookrightarrow \sum(G)$. Image of f is the subgroup of all inner automorphisms of G. Note that $Inn(G) \subseteq Aut(G)$ is a subgroup in particular. On the other hand, $\ker(f) = \{x \in G : f_x = id\} = Z(G) \subseteq G$, is exactly the center of G. Indeed, $g = f_x(g) = xgx^{-1}$ for all $g \in G$, so $gx = xg$ for all $g \in G$. In particular, the center is a normal subgroup of G, i.e. $Z(G) \lhd G$.

By the first isomorphism theorem, $G/Z(G) \cong Inn(G)$. Note that the group $Inn(G)$ is trivial if and only if G is an Abelian group, and $Inn(G)$ is cyclic if and only if it is trivial.

2. *Consider $Aut(\mathbb{Z}/n\mathbb{Z})$. Note that an automorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is determined by image of the identity: $[1]_n \mapsto [a]_n$ where $\gcd(a, n) = 1$, then $[k]_n \mapsto [ka]_n$.*

   Note $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$: if $f([1]) = [a]$, $g([1]) = [b]$, then $(g \circ f)([1]) = [ab]$.

   In particular, $Aut(\mathbb{Z}) = \{\pm 1\}$.

3. *Let X be the set of all subsets of G. Consider G acts on X by conjugation $g * H = gHg^{-1} = f_g(H)$.*

Definition 1.6.5 (Orbit, Stabilizer, Transitive)**.** *Consider G acts on X. Define a relation on X: $\forall x, x' \in X$, $x \sim x'$ if $x' = gx$ for some $g \in G$. Note that $\sim$ is an equivalence relation. Now X is a disjoint union of equivalence classes, called orbits (G-orbits).*

More generally, for $x \in X$, $G \cdot x = \{g \cdot x \mid g \in G\}$ is the orbit of x. Note $Gx_1 = Gx_2$ if and only if x_1, x_2 belong to the same orbit.

The group action is transitive if there is exactly one orbit. Note that G acts transitively on X if $X \neq \varnothing$ and for all $x, x' \in X$, $\exists g \in X$ such that $x' = g \cdot x$. So $G \cdot x = X$ for all $x \in X$.

For G acts on X and $x \in X$, $Stab(x) = \{g \in G : g \cdot x = x\}$ is a subgroup of G, called the stabilizer of G.

Example 1.6.6.

1. *If G acts trivially on X, then orbit $G \cdot x = \{x\}$ and stabilizer is G.*

2. *Suppose G acts on itself by conjugation $*$. For $x \in G$, $G * x = \{gxg^{-1}, g \in G\}$, the orbit is the conjugacy classes of x in G.*

   Note that $x \in Z(G) \iff gxg^{-1} = x \; \forall g \in G \iff$ conjugacy class of x is $\{x\}$. The stabilizer is $\{g \in G : gxg^{-1} = x$ i.e. $gx = xg\}$, which is called the centralizer *of x. Moreover, a centralizer of a subgroup H of G, denoted $C_G(H)$, is the set of elements in G that acts as centralizers on all elements in H. In particular, $C_G(H) \cap H = Z(H)$.*

3. *Suppose subgroup $H \subseteq G$, then let $X = G/H$ be the set of left cosets xH. Consider G acts on X by left translation. This action is transitive, as $xH = (xy^{-1})yH$ for all $x, y \in G$. Note that $H = eH \in X$, then the stabilizer of H is Stab$(H) = \{g \in G : gH = H\} = H$.*

4. *Take subgroup $H \subseteq G$. Let X be the set of subgroups of G. Suppose G acts on X by conjugation: $g * H = gHg^{-1} = f_g(H)$. Now the orbit of H is the set of all subgroups gHg^{-1}. Stab$(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$, the normalizer of H in G. In particular, $H \lhd N_G(H)$. Hence, $H \lhd G \iff N_G(H) = G$.*

Theorem 1.6.7 (Orbit-Stabilizer Theorem)**.** *Let group G act on a set X. Take $x \in X$. Then card$(G \cdot x) = [G :$ Stab$(X)]$. In particular, if G is finite, then card$(G \cdot x) = \frac{|G|}{|Stab(x)|}$.*

Proof. Consider $f : G/\text{Stab}(x) \to G \cdot x$, $f(g\text{Stab}(x)) = gx$. We need to show that $g \cdot \text{Stab}(x) = g' \cdot \text{Stab}(x)$ then $gx = g'x$. In particular, if $g^{-1}g' \in \text{Stab}(x)$, $g^{-1}g'x = x$, hence $gx = g'x$. Therefore, the function is well-defined.

We claim that f is injective, note that if $gx = g'x$, then $g^{-1}g'x = x$, then $g^{-1}g' \in \text{Stab}(x)$. Therefore, $g \cdot \text{Stab}(x) = g' \cdot \text{Stab}(x)$ as desired. Note f is also surjective, hence it is a bijection. □

Example 1.6.8. *Let $H \subseteq G$ be a subgroup. The number of subgroups of G conjugate to H is $[G : N_G(H)]$.*

Theorem 1.6.9. *Let G be a finite group, and p is the smallest prime divisor of $|G|$. Then every subgroup $H \subseteq G$ with $[G : H] = p$ is normal.*

Proof. Take $X = G/H$ with card$(X) = p$. Consider G acts on X by left translation.

Define $f : G \to \sum(X) = S_p$, then $N = \ker(f) \lhd G$. We claim that $H = N$.

Note $f(g)(xH) = gxH$. When $g \in N$, $x = e$, $f(g)(H) = H$. Therefore, $N \subseteq H$.

Consider $\text{im}(f) \subseteq S_p$ as subgroup. Then $|\text{im}(f)| \mid p!$. Note $\text{im}(f) \cong G/N$. Then $|\text{im}(f)| = [G : N] \mid |G|$. Therefore, $|\text{im}(f)| = 1$ or p. However, $[G : N] \leq p$, so $[G : H] = p$, hence $H \subseteq N$.

Therefore, $[G : N] = p$, and so $H = N$. □

Proposition 1.6.10 (Class Equation of a Group Action). *Let G be a group and X be a finite set. Suppose we are given a group action of G on X.*

- *Let S_0 be the set of points in S that is fixed by the action of all elements of G.*
- *Let $O_1, \cdots, O_r$ be the orbits of size greater than 1 under this action. For each orbit O_i, take $s_i \in O_i$ and let $G_i = \mathbf{stab}(s_i)$.*

The class equation of this action is given by

$$|S| = |S_0| + \sum_{i=1}^{r} \frac{|G|}{|G_i|}.$$

Corollary 1.6.11 (Class Equation of a Group). *Suppose G is a finite group, $Z(G)$ is the center of G, and $C_1, C_2, \cdots, C_r$ are all the conjugacy classes in G comprising the elements outside the center. Let g_i be an element in C_i for each $1 \le i \le r$. Then, we have $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C(g_i)|$, where $C(g_i)$ is the centralizer of g_i.*

Remark 1.6.12. *This is a particular case of class equation of a group action, when we consider the action to be G acting on itself by conjugation.*

Lemma 1.6.13 (Burnside's Lemma). *Let G be a finite group that acts on a set X. For each g in G let X^g denote the set of elements in X that are fixed by g (also said to be left invariant by g), i.e. $X^g = \{x \in X | g \cdot x = x\}$. Then the number of orbits, denoted as $|X/G|$, satisfies $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$.*

Proof. First of all, observe that $\sum_{g \in G} |X^g| = \{(g,x) \in (G,X) : g \cdot x = x\} = \sum_{x \in X} \text{Stab}(x) = |G| \cdot \sum_{x \in X} \frac{1}{\text{Orb}(x)}$. Therefore, $\sum_{x \in X} \frac{1}{|\text{Orb}(x)|} = \frac{1}{|G|} \sum_{g \in G} |X^g|$. However, by splitting the elements into individual orbits, we may derive $\sum_{x \in X} \frac{1}{|\text{Orb}(x)|} = \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|\text{Orb}(x)|} = \sum_{A \in X/G} 1 = |X/G|$. Therefore, $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$. □

Remark 1.6.14. *The proof of class equations above should be very similar to the proof we provided for Burnside's Lemma, so we only listed this particular proof here.*

1.7 Sylow Theorems

Definition 1.7.1 (p-group, Fixed Set). *Let p be a prime integer. A group G is called a p-group if $|G| = p^n$ for some $n > 0$. A subgroup $H \subseteq G$ is a p-subgroup if H is a p-group.*

Suppose G acts on X, then we define $X^G = \{x \in X : gx = x \ \forall g \in G\} \subseteq X$.

Lemma 1.7.2. *Let a group H act on a set X. If H is a p-group and X is finite, then $|X^H| \equiv |X| \pmod{p}$.*

Proof. Suppose $X^H = \{x_1, \cdots, x_n\}$ with $|X^H| = n$.

Note that $\mathrm{Orb}(X_i) = H \cdot x_i = \{x_i\}$ with size 1.

Now consider $X = \coprod_{i=1}^{n+m} \mathrm{Orb}(x_i)$ as the disjoint union of orbits. For $i \leq n$, $|\mathrm{Orb}(x_i)| = 1$. For $i > n$, $\mathrm{Orb}(x_i) = \frac{|H|}{|\mathrm{Stab}(x_i)|}$ where $H = p^k$ for some k. In particular, $p \mid \mathrm{Orb}(x_i)$ since their orbit sizes are greater than 1.

Therefore, $|X| = n \times 1 + \sum_{i=n+1}^{n+m} |\mathrm{Orb}(x_i)|$, which means $|X| \equiv n \pmod{p}$. Therefore, $|X| \equiv |X^H| \pmod{p}$. □

Theorem 1.7.3 (Cauchy)**.** *Let G be a finite group and p be a prime divisor of $|G|$. Then G has an element of order p.*

Proof. Consider the set $X = \{(g_1, g_2, \cdots, g_p), g_i \in G, g_1 g_2 \cdots g_p = e\}$. Note that $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$. So $|X| = |G|^{p-1}$ and is divisible by p. Also note that $g_p g_1 g_2 \cdots g_{p-1} = e$ as well. Then if $(g_1, g_2, \cdots, g_p) \in X$, then $(g_p, g_1, \cdots, g_{p-1}) \in X$. By shifting p times, we are back to the start. Hence, there is a cyclic group H of order p with generator $\sigma \in H$, then H acts on X by $\sigma(g_1, \cdots, g_p) = (g_p, g_1, \cdots, g_{p-1})$.

Since H is a p-group, by lemma, $|X^H| \equiv |X| \pmod{p}$.

Observe that $(e, e, \cdots, e) \in X^H$, then $|X^H| > 0$, therefore $|X^H| \geq p > 1$, then there exists a non-trivial tuple $(g_1, g_2, \cdots, g_p) \in X^H$. By definition, this tuple must have the form $(g, g, \cdots, g)$ for some $e \neq g \in G$. Recall that $g^p = e$ by definition, then $\mathrm{ord}(g) = p$. □

Proposition 1.7.4. *Let G be a p-group, then $Z(G) \neq \{e\}$.*

Proof. Consider G acts on $X = G$ by conjugation. Then $X^G = \{x \in G : gxg^{-1} = x \ \forall x \in G\} = Z(G)$.

By lemma 1.7.2, $|X^G| \equiv |X| \pmod{p}$. Then $|Z(G)| \equiv |G| \pmod{p}$. Hence, $p \mid |Z(G)|$. In particular, $Z(G) \neq \{e\}$. □

Remark 1.7.5. *The center of a group is the set of fixed points on the group action of self-conjugation on G.*

Lemma 1.7.6. *Let H be a p-subgroup of a finite group G. Then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.*

Remark 1.7.7. *Note that the normalizer of H, $N_G(H)$, is the largest subgroup of G that satisfies $H \lhd N_G(H)$.*

Proof. Consider H acts on the set $X = G/H$ of left cosets by left translation. Note that $|X| = [G : H]$. We want to show that $|X^H| = [N_G(H) : H] = |N_G(H)/H|$. For $g \in G$, note that $gH \in X^H \iff hgH = gH \ \forall gH \iff g^{-1}hgH = H \ \forall h \in H \iff g^{-1}hg \in H \ \forall h \in H \iff g^{-1}Hg \subseteq H \iff g^{-1} \in N_G(H) \iff g \in N_G(H) \iff gH \in N_G(H)/H$. Therefore, $X^H = N_G(H)/H$. We conclude the proof by applying the lemma 1.7.2. □

Theorem 1.7.8 (First Sylow Theorem)**.** *Let G be a finite group of order $p^n \cdot m$ for prime p and $n > 0$, and $\gcd(p, m) = 1$. So p^n is the highest power of p dividing $|G|$.*

1. *For every $k = 0, 1, \cdots, n-1$, every subgroup of G of order p^k is a normal subgroup of a subgroup of order p^{k+1}.*
2. *G has subgroups of order $1, p, p^2, \cdots, p^n$.*

Remark 1.7.9. *It is not true that if $a \mid |G|$ then G has a subgroup of order a.*

Proof. It suffices to prove the first statement. If 1) is true, then $\{e\} \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n$ can be found where H_i has order p^i.

Consider $|H| = p^k$ for $k = 0, 1, \cdots, n-1$. As H is a p-subgroup, by lemma 1.7.6, $[N_G(H) : H] \equiv [G : H] \pmod p$. Therefore, $[N_G(H) : H] \equiv \frac{p^n \cdot m}{p^k} \pmod p$. Since $k < n$, then $p \mid [N_G(H) : H]$. Recall that $H \lhd N_G(H)$. Then $N_G(H)/H$ is a factor group of order divisible by p.

By Cauchy's Theorem, $\exists F \subseteq N_G(H)/H$ such that $|F| = p$. Then we have

$$\begin{tikzcd}
N_G(H) \arrow[r, two heads, "\pi"] & N_G(H)/H \\
\pi^{-1}(F) \arrow[u, hook, "inc"] \arrow[r, two heads, "\pi'"] & F \arrow[u, hook, "inc"]
\end{tikzcd}$$

Recall that $H = \pi^{-1}(e)$, then $H \subseteq N_G(H) \cap \pi^{-1}(F)$. In particular, $H \lhd \pi^{-1}(F)$. By the first isomorphism theorem, $\pi^{-1}(F)/H \cong F$, so $\frac{|\pi^{-1}(F)|}{|H|} = |\pi^{-1}(F)/H| = |F| = p$, which means $|\pi^{-1}(F)| = |H| \cdot p = p^k \cdot p = p^{k+1}$. This concludes the proof. □

Remark 1.7.10. *Consider $|G| = p^n \cdot m$ where $\gcd(m, p) = 1$ and $n > 0$. By the First Sylow theorem, there exists a subgroup $P \subseteq G$ of order p^n.*

Definition 1.7.11 (Sylow p-group)**.** *The group P defined in remark 1.7.10 is called a Sylow p-group of G.*

Remark 1.7.12. *For $g \in G$ and a Sylow p-group P, gPg^{-1} is also a Sylow p-group. In particular, $gPg^{-1} \cong P$.*

Take $|G| = p^n \cdot m$, $\gcd(m, p) = 1$ with $n > 0$. Let $P \subseteq G$ be a Sylow p-subgroup, i.e. $|P| = p^n$.

Theorem 1.7.13 (Second Sylow Theorem)**.** *Let G be a finite group, $|G|$ is divisible by prime p, let $P \subseteq G$ be a Sylow p-subgroup. Then*

1. *For every p-subgroup $H \subseteq G$ there is $g \in G$ such that $H \subseteq gPg^{-1}$, and*

2. *Every two Sylow p-subgroup of G are conjugate.*

Proof. 1. Consider H acts on $X = G/P$ by left translations. $|X| = [G : P] = \frac{|G|}{|P|} = \frac{p^n \cdot m}{p^n} = m$. By lemma 1.7.2, $|X^H| \equiv |X| = m \not\equiv 0 \pmod{p}$. Therefore, $X^H \neq \varnothing$, so $\exists gP \in X$ such that $hgP = gP$ for all $h \in H$. Then $g^{-1}hgP = P$, and so $g^{-1}hg \in P \in P$, then $h \in gPg^{-1}$ for all $h \in H$, hence $H \subseteq gPg^{-1}$.

2. Let Q be another Sylow p-subgroup of G. By 1), $Q \subseteq gPg^{-1}$ for some $g \in G$. Therefore, $p^n = |Q| = |P| = |gPg^{-1}|$, and so $Q = gPg^{-1}$.

□

Corollary 1.7.14. *A Sylow p-subgroup P in G is normal in G if and only if P is the only Sylow p-subgroup of G.*

Proof. $\Rightarrow$: If Q is Sylow p-subgroup, then $Q = gPg^{-1} = P$.

$\Leftarrow$: Suppose gPg^{-1} is a Sylow p-subgroup, then $gPg^{-1} = P$ for all $g \in G$, therefore $P \lhd G$. □

Theorem 1.7.15 (Third Sylow Theorem)**.** *Let G be a finite group, with $|G| = p^n \cdot m$, and suppose* $\gcd(m, p) = 1$ *and $n > 0$. Then the number of Sylow p-subgroup divides m and is congruent to* 1 *mod p.*

Proof. Note that the number of Sylow p-subgroup is the number of subgroups in the conjugacy class of a fixed Sylow p-subgroup $P \subseteq G$. Therefore, the number is equivalent to $[G : N_G(P)] = \frac{|G|}{|N_G(P)|}$ divides $\frac{|G|}{|P|} = m$.

Let X be the set of all Sylow p-subgroups of G, then P acts on X by conjugation. By lemma, $|X^P| \equiv |X| \pmod{p}$. Take $Q \in X^P$, then $pQp^{-1} = Q$ for all $p \in P$. Now P and Q are both subgroups of $N_G(Q)$. Also note that since P is Sylow in G, and $P \subseteq N_G(Q) \subseteq G$, then P is a Sylow p-subgroup in $N_G(Q)$. On the other hand, by definition Q is a Sylow p-subgroup of G as well, then similarly Q is a Sylow p-subgroup in $N_G(Q)$ since $Q \subseteq N_G(Q) \subseteq G$. Furthermore, recall that $Q \lhd N_G(Q)$, then by the previous corollary **1.7.14**, Q is the only Sylow p-subgroup of $N_G(Q)$. Therefore, $P = Q$, and so $X^P = \{P\}$, which means $|X^P| = 1$, then $|X| \equiv 1 \pmod{p}$. □

Proposition 1.7.16. *Let P denote a Sylow p-subgroup of a finite group G. Let $N_G(P)$ denote the normalizer of P in G.*

1. *Show that P is the unique Sylow-p subgroup of $N_G(P)$.*

2. *Let $\varphi \in \mathbf{Aut}(G)$, then $\varphi(P)$ is also a Sylow p-subgroup of G.*

3. *$N_G(N_G(P)) = N_G(P)$.*

Proof.

1. Since P is a Sylow p-subgroup of G, then it is also a Sylow p-subgroup in $N_G(P)$. By definition, $P \lhd N_G(P)$, so P is the unique Sylow p-subgroup in $N_G(P)$.

2. Since φ is an automorphism, the image of the map has the same order as P. In particular, the image is also a subgroup of G by definition, so $\varphi(P)$ is a Sylow p-subgroup of G.

3. Suppose $g \in N_G(N_G(P))$. We show that $g \in N_G(P)$. By definition, $gN_G(P)g^{-1} \subseteq N_G(P)$. Since P is the unique Sylow p-subgroup in $N_G(P)$, then any automorphism would preserve P. In particular, Therefore, g is a normalizer of P, i.e. $g \in N_G(P)$. We then conclude that $N_G(N_G(P)) = N_G(P)$.

□

Example 1.7.17. *Every group G of order $380 = 2^2 \cdot 5 \cdot 19$ is not simple.*

Suppose otherwise, that G does not have a non-trivial normal subgroup.

By Sylow Theorem, $n_{19} \equiv 1 \pmod 1)9$ and $n_{19} \mid 20$, so n_{19} has to be 20, otherwise we have a normal subgroup. Similarly, $n_5 \equiv 1 \pmod{5}$ and $n_5 \mid 76$, so n_5 has to be 1 or 76, and we must have 76 Sylow 5-subgroups. This gives us $20 \cdot (19 - 1) + 76 \cdot (5 - 1) = 664$ elements because the two types of Sylow subgroups would not intersect non-trivially. Therefore, contradiction, and G must have be non-simple.

Proposition 1.7.18. *If $p > q$ are primes, a group of order pq has at most one subgroup of order p.*

Proof. Suppose a subgroup H of order p in group G of order pq exists. Note that H must have index q, which is the smallest prime dividing $|G|$, then by **theorem 1.6.9**, H must be normal. In particular, H having order p means it is a Sylow p-subgroup of G. Therefore, H must be unique.

Therefore, if a subgroup of order p exists, it must be unique. That means G would have at most one subgroup of order p. □

1.8 Product

Definition 1.8.1 (External Product, Internal Product)**.** *For groups $G_1, G_2, \cdots, G_n$, $G = G_1 \times G_2 \times \cdots \times G_n$ is the external product.*

For group G and subgroups $H_1, \cdots, H_n \subseteq G$, we say that G is the internal product of $H_1, \cdots, H_N$, i.e. $G = H_1 \times H_2 \times \cdots \times H_n$ if:

1. *$H_i \lhd G$ for all i, and*

2. *Every $g \in G$ can be uniquely written as $g = h_1 \cdots h_n$ with $h_i \in H_i$.*

Remark 1.8.2.

1. *Both external product and internal product are groups.*

2. *For $G = H_1 \times \cdots \times H_n$, $H_i \cap H_j = \{e\}$ $\forall i \neq j$.*

   Indeed, take $g \in H_i \cap H_j$, then $g = e_1 \cdots e_{i-1} g e_{i+1} \cdots e_n = e_1 \cdots e_{j-1} g e_{j+1} \cdots e_n$. However, since g has to be uniquely expressed, then $g = e$.

3. *For $x \in H_i$ and $y \in H_j$ and $i \neq j$, we have $xy = yx$.*

   Let $[x, y] = xyx^{-1}y^{-1}$ be the commutator of x and y.

   We claim that $[x, y] = e$. Indeed, $H_i \ni x(yx^{-1}y^{-1}) = [x, y] = (xyx^{-1})y^{-1} \in H_j$. Therefore, $[x, y] \in H_i \cap H_j = \{e\}$. In particular, $xy = yx$.

Proposition 1.8.3.

1. *If G is the internal product of subgroups, then $G \cong H_1 \times H_2 \times \cdots \times H_n$ as an external product.*

2. *If G is the external product, then by definition we have $G = H_1 \times H_2 \times \cdots \times H_n$, then $H_i' = \{(e_1, e_2, \cdots, e_{i-1}, h_i, e_{i+1}, \cdots, e_n)\} \subseteq G$. Then $H_i' \lhd G$, $H_i' \cong H_i$, and $G = H_1' \times H_2' \times \cdots \times H_n'$ as the internal product.*

Proof. 1. Define $f : H_1 \times H_2 \times \cdots \times H_n \to G$ as the map from the defined external product to G, where $f(h_1, h_2, \cdots, h_n) = h_1 h_2 \cdots h_n \in G$. Observe that $f((h_1, \cdots, h_n) \cdot (h_1', h_2', \cdots, h_n')) = f(h_1 h_1', h_2 h_2', \cdots, h_n h_n') = h_1 h_1' h_2 h_2' \cdots h_n h_n' = h_1 h_2 \cdots h_n h_1' h_2' \cdots h_n' = f(h_1, \cdots, h_n) \cdot f(h_1', \cdots, h_n')$. Therefore f is a homomorphism. However, recall from the remark that f is bijective, then f is a group isomorphism.

2. Take $H_i' \to H_i$ by $(e_1, \cdots, e_{i-1}, h_i, e_{i+1}, \cdots, e_n) \mapsto h_i$. This is clearly an isomorphism. Then there is $(h_1, \cdots, h_n) = (h_1, e, \cdots, e) \cdot (e, h_2, e, \cdots, e) \cdot \cdots \cdot (e, \cdots, e, h_n)$, which is an isomorphism between G and $H_1' \times H_2' \times \cdots H_n'$.

□

Remark 1.8.4. *For finite group G as the internal product, 2) in definition is equivalent to $G = H_1 H_2 \cdots H_n$ and $|G| = |H_1| \cdot |H_2| \cdot \cdots \cdot |H_n|$.*

Indeed, ($\Rightarrow$) note that there is a bijection $H_1 \times \cdots \times H_n \to G$ and ($\Leftarrow$) since f is surjective and equalite, then f is a bijection, hence 2) holds.

Example 1.8.5. *Suppose* $\gcd(m, n) = 1$.

Note that $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with $[a]_{nm} \mapsto ([a]_n, [a]_m)$ because of Chinese Remainder Theorem. In particular, we can write $\mathbb{Z}/nm\mathbb{Z} = (m\mathbb{Z}/nm\mathbb{Z}) \times (n\mathbb{Z}/nm\mathbb{Z})$.

Proposition 1.8.6. *Let G be a finite group such that all Sylow subgroups of G are normal. Then G is the (internal) product of all Sylow subgroups.*

Proof. Denote $|G| = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ where p_i are distinct primes. Define P_i as Sylow p_i-subgroup for $i = 1, \cdots, s$. Note that $|G| = |P_1||P_2| \cdots |P_s|$, and every Sylow subgroup is normal in G. By remark 1.8.4, it suffices to show that $G = P_1 P_2 \cdots P_s$.

Take $g \in G$, define $q_i = \frac{|G|}{p_i^{k_2}}$, then $\gcd(q_1, q_2, \cdots, q_s) = 1$. Then by Bezout's Lemma, $\sum_{i=1}^{s} q_i m_i = 1$ for some $m_i \in \mathbb{Z}$.

Now, $g = g^1 = \prod_{i=1}^{s} (g^{q_i})^{m_i}$. Since $q_i \cdot p_i^{k_i} = |G|$, and $g^{|G|} = e$, we have $(g^{q_i})^{{p_i}^{k_i}} = e$. We know g^{q_i} generates a cyclic subgroup $H_i \subseteq G$ (p_i-subgroup) of order dividing $p_i^{k_i}$.

By the Second Sylow Theorem 1.7.13, $H_i \subseteq x P_i x^{-1} = P_i$ for some $x \in G$. Then $g^{q_i} \in H_i \subseteq P_i$, which means $(g^{q_i})^{m_i} \in P_i$. Therefore, $G = P_1 P_2 \cdots P_s$. This concludes the proof. □

Corollary 1.8.7. *Let G be a group of order pq for prime p and q. Suppose $p > q$. If $p \not\equiv 1 \pmod{q}$, then G is cyclic.*

Proof. Let P_p and P_q be Sylow subgroups of order p and q, respectively.

Note that $[G : P_p] = \frac{|G|}{|P_p|} = \frac{pq}{p} = q$ is the smallest prime divisor of $|G| = pq$. Therefore, by **1.6.9**, $P_p \lhd G$.

Take $H = N_G(P_q)$, then $P_q \subseteq H \subseteq G$. Note that $|H| = q$ or pq, then $[G : H] = 1$ or p. However, by the Third Sylow Theorem **1.7.15**, the number of Sylow q-subgroups is congruent to 1 modulo q. Therefore, $[G : H] = 1$, so $G = H$, which means $P_q \lhd G$.

By proposition **1.8.6**, corollary **1.4.18**, theorem **1.3.4** and example **1.8.5**, $G = P_p \times P_q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$, which means G is a cyclic group. This concludes the proof. □

Proposition 1.8.8. $|HK| = \frac{|H||K|}{|H \cap K|}$ *for* H, K *as subgroups of* G.

Proof. Consider the group homomorphism $f : H \times K \to HK$. This is clearly surjective. The equivalence class that sends elements in $H \times K$ to the same element in HK is exactly the set of elements $\{h_1k_1 = h_2k_2, h_i \in H, k_i \in K\}$. However, now $h_1^{-1}h_2 = k_1k_2^{-1} \in H \cap K$. Note that the number of pairs of (h_2, k_2) that makes the relation hold is exactly the number of elements in $h_1(H \cap K)$, which is just $|H \cap K|$. Therefore, $|HK| = \frac{|H||K|}{|H \cap K|}$. □

1.9 Nilpotent and Solvable Group

Definition 1.9.1 (Generated Subgroup)**.** *For any group G and subset $S \subseteq G$, $\langle S \rangle$ is the smallest subgroup of G containing S. This is the subgroup generated by S.*

Proposition 1.9.2. $\langle S \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}, x_i \in S, \varepsilon = \pm 1\}$.

Proof. Define $H = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}, x_i \in S, \varepsilon = \pm 1\}$. Note that $H \subseteq G$ is a subgroup. [1]

Now for $x \in S$, $x = x^1 \in H$, so $S \subseteq H$, which means $\langle S \rangle \subseteq H$.

On the other hand, for $x_i \in S$, $x_i^{\varepsilon_i} \in S \subseteq \langle S \rangle$. Therefore, an arbitrary element $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \in \langle S \rangle$. Therefore, $H \subseteq \langle S \rangle$. We conclude that $H = \langle S \rangle$. □

Remark 1.9.3. *If S satisfies $gSg^{-1} \subseteq S$ for all $g \in G$, then $\langle S \rangle \lhd G$.*

Example 1.9.4. *Let $S = \{g\}$, then $\langle S \rangle = \{g^k, k \in \mathbb{Z}\}$ is the cyclic group generated by g.*

[1] Note that even if S is empty, H still contains the empty product as an element, which is equivalent to the identity by definition. Therefore, H is not empty.

Definition 1.9.5 (Commutator). *Let G be a group and $x, y \in G$. The commutator of x and y is $[x, y] = xyx^{-1}y^{-1}$.*

Property 1.9.6.

1. $[x, y] = e \iff xy = yx$
2. $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$
3. $[x, y]^{-1} = [y, x]$

Definition 1.9.7 (Commutator Subgroup/Derived Subgroup). *The commutator subgroup (derived subgroup) is the subgroup generated by all commutators of G, denoted as $[G, G]$. In particular, an arbitrary element in $[G, G]$ has the form $[x_1, y_1] \cdot [x_2, y_2] \cdot \dots \cdot [x_n, y_n]$ where $[x_i, y_i]$ is a generator of $x_i, y_i \in G$.*

Remark 1.9.8.

1. *By example 1.9.6, $[G, G] \lhd G$.*
2. *G is Abelian if and only if $[G, G] = \{e\}$.*

Proposition 1.9.9. *Let $N \lhd G$. Then G/N is Abelian if and only if $[G, G] \subseteq N$.*

Proof.

$$\begin{aligned} G/N \text{ Abelian} &\iff xN \cdot yN = yN \cdot xN \ \forall x, y \in G \\ &\iff xyN = yxN \ \forall x, y \in G \\ &\iff x^{-1}y^{-1}xyN = N \ \forall x, y \in G \\ &\iff [x^{-1}, y^{-1}] \in N \ \forall x, y \in G \\ &\iff [G, G] \subseteq N \end{aligned}$$

□

Remark 1.9.10. *Observe that if $[G, G] \subseteq N \subseteq G$, then $N \lhd G$. Indeed, for arbitrary $g \in G$, $n \in N$, we have $gng^{-1}n^{-1} = h$ for some $h \in [G, G] \subseteq N$. Therefore, $gng^{-1} = hn \in N$. Hence, $N \lhd G$.*

Therefore, a better interpretation of proposition 1.9.9 is the following: let $N \subseteq G$ be a subgroup. Then $[G, G] \subseteq N$ if and only if $N \lhd G$ and G/N is Abelian.

Proposition 1.9.11. *If $f : G \to H$ is a homomorphism, H is Abelian, and N is a subgroup of G containing $\ker(f)$, then $N \lhd G$.*

Proof. By the first isomorphism theorem, we have $G/\ker(f) \cong \mathbf{im}(f) \subseteq H$. Since H is Abelian, we have $G/\ker(f)$ to be Abelian. By proposition, $[G,G] \subseteq \ker(f)$. Therefore, N has to contain $[G,G]$, which means $N \lhd G$. □

Remark 1.9.12 (Abelianization)**.** *Following remark* ***1.9.10****, take* $N = [G,G] \lhd G$*, it then follows that* $G/[G,G]$ *is Abelian. This group is called the Abelianization of group* G*.*

Proposition 1.9.13 (Universal Property of Abelian Groups)**.** *Let* $f : G \to H$ *be a group homomorphism where* H *is Abelian. Then the following diagram commutes:*

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/[G,G] \arrow[ur, dashed, "\exists!\bar{f}"] & \end{tikzcd}$$

Figure 1.3: Universal Property of Abelianization

Proof. By **remark 1.9.10**, $[G,G] \subseteq N$ if and only if $N \lhd G$ and G/N is Abelian. Take $N = \ker(f)$, then N is clearly normal, and $G/N \cong \text{im}(f) \subseteq H$ must be Abelian, which means $[G,G] \subseteq N$. By the universal property **proposition 1.4.31**, we have the diagram as desired. □

Definition 1.9.14 (Solvable Group)**.** *Let* G *be a group. Define* $G^{(0)} = G, G^{(1)} = [G,G], \cdots, G^{(i+1)} = [G^{(i)}, G^{(i)}]$*. Therefore,* $G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(n)} \rhd \cdots$*. Note that* $G^{(i)}/G^{(i+1)}$ *is Abelian. We say* G *is solvable if* $G^{(n)} = \{e\}$ *for some* n*.*

Property 1.9.15.

1. *G is solvable if and only if there is a sequence of subgroups $G = G_0 \supset G_1 \cdots$ such that $G_{i+1} \lhd G_i$ $\forall i$, G_i/G_{i+1} is Abelian, and $G_n = \{e\}$ for some n.*
2. *A subgroup of a solvable group is solvable.*
3. *If G is solvable and $N \lhd G$, then G/N is solvable.*
4. *Let $N \lhd G$, then G is solvable if and only if N and G/N are solvable.*

Proof.

1. Obviously if G is solvable, then $G_i = G^{(i)}$.

   Notice that G_i/G_{i+1} Abelian if and only if $[G_i, G_i] \subseteq G_{i+1}$. We show $G^{(i)} \subseteq G_i$ by induction on i. Suppose this is true, then $G^{(n)} \subseteq G_n = \{e\}$, which means $G^{(n)} = \{e\}$ is solvable.

The case $i = 0$ is clear. Suppose the case is true at i, consider the case with $i + 1$. By definition, $G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}$. This concludes the proof.

2. Let G be solvable. Then $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$, $G_{i+1} \supseteq [G_i, G_i]$.

   Let $H \subseteq G$ and define $H_i = H \cap G_i$.

   Since $G_{i+1} \triangleleft G_i$, then by the Second Isomorphism Theorem **1.5.6**, $H_{i+1} \triangleleft H_i$. Now, $H_i \cap G_{i+1} = H_{i+1} \subseteq H_i$, and so $[H_i, H_i] \subseteq [G_i, G_i] \cap H_i \subseteq G_{i+1} \cap H_i = H_{i+1}$.

   Hence, H_i/H_{i+1} is Abelian. Then by property 1, H is solvable.

3. Take $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$. Note that $G_{i+1} \supseteq [G_i, G_i]$.

   Now $G/N = GN/N = G_0/N \triangleright G_1N/N \triangleright \cdots \triangleright G_nN/N = N/N = \{e\}$ where $G_{i+1}N/N \supseteq [G_iN/N, G_iN/N]$. Indeed, for $g, g' \in G$ and $n, n' \in N$, we then have $[gnN, g'n'N] = [gN, g'N] = [g, g']N \in G_{i+1}N$. Therefore, G/N is solvable.

4. The $\Longrightarrow$ direction has been proven. We prove the $\Longleftarrow$ direction.

   Observe that $N = N_0 \triangleright N_1 \triangleright \cdots \triangleright N - n = \{e\}$ where N_i/N_{i+1} is Abelian.

   Now $G/N = F_0 \triangleright F_1 \triangleright \cdots \triangleright F_m = \{e\}$ is a sequence where F_i/F_{i+1} is Abelian. However, let $\pi : G \to G/N$ be the canonical homomorphism, and consider the preimage $G_i = \pi^{-1}(F_i)$, we have a corresponding sequence $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m$. The nested subgroups are normal by the correspondence of preimage of the surjective homomorphism. Observe that $G_m = \pi^{-1}(F_m) = \ker(\pi) = N$.

   Collecting the properties from above, we have $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = N = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_n = \{e\}$.

   There is $\ker(G_i = \pi^{-1}(F_i) \twoheadrightarrow F_i) = N$, so by the First Isomorphism Theorem **1.5.3**, $F_i \cong G_i/N$. In particular, by the Third Isomorphism Theorem **1.5.7**, $F_i/F_{i+1} \cong (G_i/N)/(G_{i+1}/N) \cong G_i/G_{i+1}$. Therefore, G is solvable by property 1.

□

Example 1.9.16. *1. p-groups are solvable.*

This can be proven by induction on $|G|$. Since G is a p-group, then by proposition 1.7.4, $Z(G) \neq \{e\}$, and by definition $Z(G)$ is an Abelian group. Notice that the commutator subgroup of an Abelian group has to be trivial, then by definition $Z(G)$ is solvable. On the other hand, $G/Z(G)$ is another p-group, but by induction hypothesis it is also solvable. Therefore, by the previous properties, G is solvable.

2. *Let G be a finite group with $|G| = p \cdot q$ where p, q are prime. Then G is solvable.*

   If $p = q$, use the previous example. Suppose $p \neq q$, without loss of generality, assume $p > q$. Now let N be a Sylow p-subgroup, then $N \cong \mathbb{Z}/p\mathbb{Z}$ is Abelian. Then $[G : N] = q$, which is the smallest prime divisor of $|G|$. Therefore, $N \lhd G$. By the corollary, N is the only Sylow p-subgroup of G. In particular, N is Solvable by the previous remark.

   On the other hand, G/N is a factor group of order q since $N \lhd G$. Therefore, G/N is also solvable. By the property above, G is solvable.

3. *All groups of order less than 60 are solvable. A_5, with order 60, is not solvable.*

The following text on nilpotent groups were not officially covered in lectures. The notes are collected through other sources and through homework problems.

Definition 1.9.17 (Nilpotent Group). *A group G is called nilpotent if there is a sequence of subgroups*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\},$$

such that each G_i is normal in G and G_i/G_{i+1} is contained in the center of G/G_{i+1}.

Property 1.9.18. 1. *If $H, K < G$ and $[H, K] < H$, then $K < N_G(H)$.*

2. *If $H < G$, then $[G, H] = 1$ if and only if $H < Z(G)$.*

3. *If $H, K < G$ and $N \lhd G$ with $N < H, K$, then $[H/N, K/N] = [H, K]/(N \cap [H, K])$.*

Proposition 1.9.19. *A sequence of subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ with $G_i \lhd G$ for each i satisfies $[G, G_i] < G_{i+1}$ for each i if and only if $G_i/G_{i+1} \subset Z(G/G_{i+1})$ for each i.*

Proof. By properties in 1.9.18, then $[G, G_i] < G_{i+1}$ if and only if $[G/G_{i+1}, G_i/G_{i+1}] = \{e\}$, which happens if and only if $G_i/G_{i+1} < Z(G/G_i)$. □

Remark 1.9.20. *An equivalent definition of a nilpotent group G is that there exists a sequence of subgroups*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\},$$

such that such that each $G_i \lhd G$ and $[G, G_i] < G_{i+1}$ for each i.

Proposition 1.9.21.

1. *Finite products of nilpotent groups are nilpotent.*
2. *If $G/Z(G)$ is nilpotent, so is G.*
3. *Every abelian group is nilpotent.*
4. *Every p-group is nilpotent.*
5. *Every nilpotent group is solvable.*
6. *Let G be a nilpotent group and $H \subset G$ a subgroup different from G. Prove that $N_G(H) \neq H$.*
7. *Prove that a finite group is nilpotent if and only if it is isomorphic to the direct product of p-groups.*
8. *Any subgroup or quotient of a nilpotent group is nilpotent.*

Proof. See Homework 4. □

1.10 Symmetric and Alternating Group

Definition 1.10.1 (Symmetric Group, Cycle)**.** *Let $n \geq 1$, $X = \{1, 2, \cdots, n\}$. $S_n = \sum(X)$ is the Symmetric group of n symbols, with order $n!$.*

Recall that for a group G of order n, $G \hookrightarrow S_n$ is an embedding.

Take $\sigma \in S_n$, then $\sigma : X \overset{\cong}{\rightarrow} X$. Suppose there are distinct $a_1, \cdots, a_k \in X$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, ..., $\sigma(a_k) = a_1$, and $\sigma(b) = b$ $\forall b \neq a_i$ $\forall i$.

We say $\sigma = (a_1\ a_2\ \cdots a_k)$ is a k-cycle. Note $\sigma^k = e$, and $ord(\sigma) = k$. Also note that $(a_1\ \cdots a_k) = (a_2\ a_3\ \cdots a_k\ a_1)$. The length of cycle is k, when $k = 0$, $\sigma = (\ ) = id$, k can be $0, 2, 3, \cdots, n$.

$\sigma = (i\ j)$ is called a transposition.

Example 1.10.2.

1. $S_1 = \{e\}$.
2. $S_2 = \{e, (1\ 2)\}$.
3. $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

   Let $\sigma = (1\ 2\ 3)$ and $\tau = (1\ 2)$, note $\sigma^3 = e$ and $\tau^2 = e$. Then $\sigma\tau = (1\ 2\ 3)(1\ 2) = (1\ 3)$, and $\tau\sigma = (1\ 2)(1\ 2\ 3) = (2\ 3)$.

   The subgroups of S_3 are exactly the following:

$\langle\sigma\rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \lhd S_3$.

$\langle\tau\rangle = \{e, (1\ 2)\}$, $\langle(1\ 3)\rangle = \{e, (1\ 3)\}$ and $\langle(2\ 3)\rangle = \{e, (2\ 3)\}$ are not normal subgroups are S_3.

4. *In S_4, $(1\ 2)(3\ 4)$ is a product of 2-cycles, but not a cycle itself. Observe that $(1\ 2)(3\ 4) = (3\ 4)(1\ 2)$.*

   In fact, an element in S_n is always a product of these cycles.

Theorem 1.10.3. *Every element in S_n is a product of disjoint cycles, i.e. $\tau_1\tau_2\cdots\tau_s$. Moreover, τ_i's are unique (up to permutation).*

Proof. Take $\sigma \in S_n$, a bijection on X. Consider S_n acts on X with $H = \langle\sigma\rangle \subseteq S_n$, H acts on X. Now X is a disjoint union of H-orbits. i.e. $X = X_1 \coprod X_2 \coprod \cdots \coprod X_s$.

Consider $X_1 = \{a_1, \cdots, a_k\}$, and WLOG take $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, ..., $\sigma(a_k) = a_1$. Then $\tau_1 = (a_1\ a_2\ \cdots a_k)$. In a similar fashion, $X_i \mapsto \tau_i$ cycle. Therefore, $\sigma = \tau_1\tau_2\cdots\tau_s$ as product of disjoint cycles.

On the other hand, if $\sigma = \tau_1\tau_2\cdots\tau_n$ is a product of disjoint cycles, then τ_i msut permute $X_i \subseteq X$, and $X = X_1 \coprod X_2 \coprod \cdots \coprod X_s$ as disjoint union. Therefore, σ acts transitively in each X_i, so X_i are the orbits of $H = \langle\sigma\rangle$, which shows that such τ_i is unique. □

Definition 1.10.4 (Length, Type). *Consider $\sigma = \tau_1\tau_2\cdots\tau_s$ with corresponding $X = X_1 \coprod X_2 \coprod \cdots \coprod X_s$, then $k_i = |X_i|$ is defined as the length of σ_i. If we also count the 1-cycles (which we don't write down in the representations), then $\sum\limits_{i=1}^{s} k_i = n$. Therefore, $(k_1, \cdots, k_s)$ are uniquely determined up to permutation. We call this the type of σ.*

Example 1.10.5. *Suppose $\sigma \in S_n$ denoted as the cycle $(a_1\ a_2\ \cdots\ a_k)$. Let $\tau \in S_n$. What is $\tau\sigma\tau^{-1}$?*

If $b_i = \tau(a_i)$, then $(\tau\sigma\tau^{-1})(b_i) = \tau(\sigma(\tau^{-1}(b_i))) = \tau(\sigma(a_i)) = \tau(a_{i+1}) = b_{i+1}$;For $c \neq b_i\ \forall i$, $(\tau\sigma\tau^{-1})(c) = c$.

Therefore, $\tau\sigma\tau^{-1} = (b_1\ b_2\ \cdots\ b_k)$ is a k-cycle as well.

Remark 1.10.6. *If $\sigma \in S_n$ is a product of disjoint cycles, i.e. $\sigma = \sigma_1\cdots\sigma_s$, where σ_i is a k_i-cycle, then type$(\sigma) = (k_1, \cdots, k_s)$.*

Take $\tau \in S_n$, then $\tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1}\cdots\tau\sigma_s\tau^{-1}$, then $\tau\sigma_i\tau^{-1}$ is a k_i-cycle, hence type$(\tau\sigma\tau^{-1}) =$ type(σ).

If $\sigma, \sigma' \in S_n$, type(σ) = type(σ'), let $\sigma = \sigma_1 \cdots \sigma_s$ and $\sigma' = \sigma'_1 \cdots \sigma'_s$ where σ_i and σ'_i are k_i-cycles. Therefore we can write $\sigma_i = (a_1 \ \cdots \ a_n)$, $\sigma'_i = (a'_1 \ \cdots \ a'_n)$. If $\tau \in S_n$ is such that $\tau(a_j) = a'_j$ for all $j = 1, \cdots, k_i$, then $\sigma'_i = \tau\sigma_i\tau^{-1}$.

In particular, there exists $\tau \in S_n$ such that $\sigma' = \tau\sigma\tau^{-1}$.

Proposition 1.10.7. *$\sigma, \sigma' \in S_n$ are conjugate if and only if type(σ) = type(σ').*

Proof. See remark 1.10.6. □

Remark 1.10.8. *Note that the number of conjugacy classes in S_n equals to the number of types and is equal to the number of partitions of n.*

Example 1.10.9.

1. *Consider S_3. Note that 3 can be represented by $1+1+1$, $1+2$ or 3 (up to permutation). Therefore, there are 3 conjugacy classes. They are identity e, transposition $(1\ 2)$ and 3-cycle $(1\ 2\ 3)$, respectively.*

2. *Consider S_4. Note that 4 can be represented by $1+1+1+1$, $1+3$, $1+1+2$, $2+2$ or 4 (up to permutation). Therefore, there are 5 conjugacy classes.*

Remark 1.10.10. *Suppose $\sigma = \sigma_1 \cdots \sigma_s$ as the product of disjoint cycles, where σ_i is a k_i-cycle, i.e. ord$(\sigma_i) = k_i$.*

Therefore, we know ord(σ) = lcm$(k_1, \cdots, k_s)$.

Example 1.10.11. *Note that $N = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq S_4$ is a subgroup. Note that the subgroup is Abeliand and normal.*

We have $|S_4/N| = 6$ and is isomorphic to S_3.

In particular, S_4/N is solvable, but N is also solvable, which means S_4 is solvable.

Remark 1.10.12. *S_n is solvable for $n \leq 4$.*

Definition 1.10.13 (Monomial Matrix, Representation)**.** *Let $\sigma \in S_n$, $A^\sigma = (a^\sigma_{i,j})$ be an $n \times n$ matrix, where $a^\sigma_{i,j} = \begin{cases} 1 \text{ if } \sigma(j) = i \\ 0 \text{ otherwise} \end{cases}$. Then A^σ is called a monomial matrix.*

Note that $(A^\sigma A^\tau)_{i,j} = \sum\limits_{k=1}^{n} (A^\sigma)_{i,k} \cdot (A^\tau)_{k,j} = a^\sigma_{i,j}\tau = (A^{\sigma\tau})_{i,j}$.

Observe that $A^\sigma \cdot A^\tau = A^{\sigma\tau}$, and $A^e = I_n$, and $A^\sigma \cdot A^{\sigma^{-1}} = I_n = A^{\sigma^{-1}} \cdot A^\sigma$. Therefore, the monomial matrices form a group in S_n.

In particular, $s : S_n \to GL_n(\mathbb{R})$ where $s(\sigma) = A^\sigma$ is a homomorphism, called the representation of σ.

Remark 1.10.14. *$GL_n(\mathbb{R})$ can be replaced by $GL_n(\mathbb{Z})$ or $GL_n(\mathbb{Q})$.*

Remark 1.10.15. *We have the composition $\varepsilon : S_n \xrightarrow{s} GL_n(\mathbb{Z}) \xrightarrow{\det} \mathbb{Z}^\times = \{\pm 1\}$.*

Note $\det(A^\sigma) = 1\ \forall \sigma \in S_n$.

Definition 1.10.16 (Even, Odd)**.** *$\sigma \in S_n$ is even if $\varepsilon(\sigma) = 1$, and $\sigma \in S_n$ is odd if $\varepsilon(\sigma) = -1$.*

Remark 1.10.17.

1. *Transpositions are always odd. This can be viewed from a matrix's perspective.*
2. *ε is surjective if $n \geq 2$.*
3. *The alternating group $A_n = \ker(\varepsilon)$ is the subgroup of all even elements in S_n.*

   In particular, $A_n \lhd S_n$, $S_n/A_n \cong \{\pm 1\}$, therefore $|A_n| = \frac{n!}{2}$ for $n \geq 2$.

Example 1.10.18.

1. *$A_1 = S_1 = \{e\}$.*
2. *$S_2 \cong \mathbb{Z}/2\mathbb{Z}$, $A_2 = \{e\}$.*
3. *$A_3 \cong \mathbb{Z}/3\mathbb{Z}$.*
4. *$|A_4| = 12$ is non-Abelian.*
5. *$A_n \subseteq S_n$ is solvable if $n \leq 4$.*

Remark 1.10.19. *For $n \geq 3$, we have $Z(S_n) = \{e\}$; for $n \geq 4$, we have $Z(A_n) = \{e\}$.*

Proposition 1.10.20. *Every element in S_n is a product of transpositions.*

Proof. We perform induction on n.

It is clear when $n = 1, 2$, since $S_2 = \{e, (1\ 2)\}$.

Suppose the case is true for $n - 1$, we consider the case of n.

Take $\sigma \in S_n$, let $i = \sigma(n)$.

Case 1: $i = n$. Then $\sigma \in S_{n-1} = \{\tau \in S_n : \tau(n) = n\} \subseteq S_n$. By the induction hypothesis, σ is a product of transpositions.

Case 2: $i \neq n$. Consider $\tau = (i\ n)$, let $\sigma' = \tau \cdot \sigma$.

Then $\sigma'(n) = \tau(\sigma(n) = \tau(i) = n$. By case 1, $\sigma' = \tau_1 \cdots \tau_s$ is the product of transpositions. Then $\sigma = \tau^{-1} \cdot \sigma' = \tau_1 \cdots \tau_s$. □

Remark 1.10.21. *Consider $\sigma \in S_n$, then $\sigma = \tau_1 \cdots \tau_s$ where τ_i is a transposition.*

Note that σ is even if s is even, and σ is odd if s is odd.

Suppose $\sigma \in A_n$ then s is even, so $\sigma = (\tau_1\ \tau_2) \cdots (\tau_{s-1}\ \tau_s)$.

Corollary 1.10.22. *A_n is generated by products of two transpositions.*

Proof. See remark 1.10.21 above. □

Example 1.10.23.

$$\begin{aligned}\sigma &= (a_1 \ \cdots \ a_k)\\ &= (a_1 \ a_k)(a_1 \ \cdots \ a_{k-1})\\ &= \cdots\\ &= (a_1 \ a_k)(a_1 \ a_{k-1})\cdots(a_1 \ a_2)\end{aligned}$$

k-cycle is even when k is odd. k-cycle is odd when k is even.

Lemma 1.10.24. *A_n is generated by 3-cycles.*

Proof. It suffices to write $\tau_1\tau_2$ into a product of 3-cycles, where τ_i is a transposition. WLOG let $\tau_1 = (i \ j), \tau_2 = (k \ l)$.

Case 1: τ_1, τ_2 have two common symbols. Then $\tau_1 = \tau_2$, $\tau_1\tau_2 = e$.

Case 2: τ_1, τ_2 have one common symbol. i.e. $\tau_1 = (i \ j), \tau_2 = (j \ k)$. Then $\tau_1\tau_2 = (i \ j \ k)$, which is a 3-cycle.

Case 3: τ_1, τ_2 have no common symbols. Then $\tau_1\tau_2 = (i \ j)(k \ l) = (i \ j)(j \ k)(j \ k)(k \ l) = (i \ j \ k)(j \ k \ l)$. □

Lemma 1.10.25. *If $n \geq 5$, then every two 3-cycles in A_n are conjugate.*

Proof. Let $\sigma = (i \ j \ k)$ and $\tau = (l \ m \ n)$. Take $\rho \in S_n$ such that $\rho(i) = l$, $\rho(j) = m$ and $\rho(k) = n$. Therefore $\rho\sigma\rho^{-1} = \tau$.

If $\rho \in A_n$ we are done. Suppose not, then ρ has to be odd. Consider s, t different from i, j, k. Let $\varepsilon = (s, t)$, then $\sigma\varepsilon = \varepsilon\sigma$. In particular, $(\rho\varepsilon)\sigma(\rho\varepsilon)^{-1} = \rho(\varepsilon\sigma\varepsilon)\rho^{-1} = \rho\sigma\rho^{-1} = \tau$.

Therefore, $\rho\varepsilon \in A_n$. This concludes the proof. □

Definition 1.10.26 (Simple)**.** *A group $G \neq \{e\}$ is called simple if G has no non-trivial normal subgroup.*

Example 1.10.27.

1. *$\mathbb{Z}/p\mathbb{Z}$ for prime p is simple.*
2. *An Abelian group is simple if and only if it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Indeed, suppose a group G is Abelian and non-trivial. Let $e \neq a \in G$. If a generates an infinite cyclic group, then a^2 generates a proper subgroup and G cannot be simple. If $\langle a \rangle$ is finite, and G is simple, then $G = \langle a \rangle$. Let n be the order and suppose it is not prime. Then $n = rs$ for some $r, s \neq 1$, and $a^r \neq e$, so a^r generates a proper subgroup of G, contradiction, which means $G = \langle a \rangle$ must have order p. Hence, $G \cong \mathbb{Z}/p\mathbb{Z}$.

3. *Every non-Abelian simple group is not solvable.*

   Note that $\{e\} \neq [G, G] \lhd G$, then $[G, G] = G$. In particular, $G = G_1 = G_2 = \cdots = G_n = \cdots$ where G_i must all be $G = [G, G]$. Therefore, G is not solvable.

4. *S_n, A_n are solvable if $n \leq 4$. S_3, S_4, A_4 are not simple.*

   Indeed, note that $A_n \lhd S_n$, then S_n is not simple for $n \geq 3$.

Theorem 1.10.28. *A_n is simple for $n \geq 5$.*

Proof. Consider $\{e\} \neq N \lhd A_n$. We show that $N = A_n$.

It suffices to prove that N contains a 3-cycle σ. Suppose this is true, then $\forall \tau \in A_n$, $\tau\sigma\tau^{-1} \in N$ since $N \lhd A_n$. But from the previous lemma **1.10.25**, all 3-cycles in A_n are conjugates for $n \geq 5$. Therefore, N contains all 3-cycles. However, recall from lemma **1.10.24** that A_n is generated by 3-cycles, so $A_n = N$.

Let $e \neq \sigma \in N$ be an element that fixes the largest number of symbols. We show that σ is a 3-cycle. Let $\sigma = \sigma_1\sigma_2 \cdots \sigma_s$ be the disjoint cycles.

Suppose all σ_i's are transpositions, then $\text{type}(\sigma) = (2, 2, \cdots, 2)$. Therefore, $\sigma \in N \subseteq A_n$ has to be even, which means s is even, so $s \geq 2$. Therefore, we can write $\sigma = (i\ j)(k\ l) \cdots$. Since $n \geq 5$, then there exists a symbol $r \neq i, j, k, l$. Take $\gamma = (k\ l\ r) \in A_n$. Let $\sigma' = [\gamma, \sigma] = (\gamma\sigma\gamma^{-1})\sigma^{-1} \in N$. Notice that $\gamma(i\ j)\gamma^{-1} = (\gamma(i)\ \gamma(j)) = (i\ j)$, and $\gamma(k\ l)\gamma^{-1} = (\gamma(k)\ \gamma(l)) = (l\ r)$

Claim 1.10.29. *$\sigma' \neq e$.*

Subproof. Observe that $\gamma\sigma\gamma^{-1} = (\gamma\sigma\gamma^{-1})(\gamma\sigma\gamma^{-1}) \cdots = (i\ j)(l\ r) \cdots \neq (i\ j)(k\ l) \cdots = \sigma$. Therefore, $\gamma\sigma\gamma^{-1} \neq \sigma$, which means $\sigma' \neq \{e\}$. ■

Now $\sigma'(i) = \gamma\sigma\gamma^{-1}\sigma^{-1}(i) = \gamma\sigma\gamma^{-1}(j) = \gamma\sigma(j) = \gamma(i) = i$.

Therefore, σ' fixes i and j, but σ does not fix i and j.

Suppose σ fixes $p \neq r$, so $\sigma(p) = p$. Then $p \neq k, l$. Moreover, $\gamma(p) = p$, $\gamma^{-1}(p) = p$ and $\sigma^{-1}(p) = p$.

Hence, $\sigma' = \gamma\sigma\gamma^{-1}\sigma^{-1}$ fixes p.

Therefore, σ' fixes more symbols than σ, which is a contradiction.

Now suppose not all σ_i are transpositions. Without loss of generality, let σ_1 be length with at least 3. Therefore, we can write $\sigma_1 = (i\ j\ k\ \cdots)$. We want to show that $\sigma_1 = (i\ j\ k)$.

Claim 1.10.30. *There exists distinct symbols l and r such that $l, r \neq i, j, k$ and σ does not fix l, r.*

Subproof. Let $\sigma = \sigma_1 \cdots \sigma_s$. If $s \geq 2$, then $\sigma_2 = (l\ r\ \cdots)$, and we are done. If $s = 1$, $\sigma = \sigma_1 = (i\ j\ k\ \cdots)$, but $\sigma \neq (i\ j\ k\ l)$ is odd, then σ is at least a 5-cycle, i.e. $\sigma = (i\ j\ k\ l\ r\ \cdots)$. ■

Take $\gamma = (k\ l\ r)$ and $\sigma' = [\gamma, \sigma] = \gamma\sigma\gamma^{-1}\sigma^{-1} \in N$.

Claim 1.10.31. *$\sigma' \neq e$.*

Subproof. Note that $\gamma\sigma\gamma^{-1} = \gamma(i\ j\ k)\sigma_2 \cdots \sigma_s\gamma^{-1} = (i\ j\ l\ \cdots) \cdots \neq (i\ j\ k\ \cdots) \cdots$. Therefore, $\gamma\sigma\gamma^{-1} \neq \gamma$, and so $\sigma' \neq e$. ■

Since $\sigma(j) = k$, then σ does not fix j. On the other hand, $\sigma'(j) = \gamma\sigma\gamma^{-1}\sigma^{-1}(j) = \gamma\sigma\gamma^{-1}(i) = \gamma\sigma(i) = \gamma(j) = j$. Therefore, σ' fixes j.

Let $\sigma(p) = p$, then $p \neq k, l, r$ since σ does not fix these elements. Then $\gamma(p) = p$, $\gamma^{-1}(p) = p$, $\sigma^{-1} = p$. In particular, $\sigma'(p) = p$. Again, σ' fixes more elements than σ, contradiction. This concludes the proof. □

Corollary 1.10.32. *A_n, S_n are not solvable if $n \geq 5$.*

Proof. A_n is simple but not Abelian, so not solvable.

S_n is not solvable because $A_n \lhd S_n$. □

Proposition 1.10.33. *A_n is the only non-trivial normal subgroup of S_n if $n \geq 5$.*

Proof. Consider $N \lhd S_n$. We want to show that N is either $\{e\}$, A_n or S_n.

Consider $f : A_n \hookrightarrow S_n \to S_n/N$. Then $\ker(f) = N \cap A_n \lhd A_n$. Therefore, $N \cap A_n = \{e\}$ or A_n. Suppose $N \cap A_n = A_n$, then $A_n \subseteq N \subseteq S_n$, which means $N = A_n$ or S_n. Suppose $N \cap A_n = \{e\}$, then f is injective, which means $A_n \hookrightarrow S_n/N$. In particular, $\frac{n!}{2} = |A_n| \leq |S_n/N| = \frac{n!}{|N|}$, so $|N| \leq 2$. Suppose $|N| = 2$, i.e. $N = \{e, \sigma\} \lhd S_n$. For all $\tau \in S_N$, $\tau N \tau^{-1} = N$, which means $\{e, \tau\sigma\tau^{-1}\} = \{e, \tau\}$, then $\tau\sigma\tau^{-1} = \sigma$ for all $\tau \in S_n$. In particular, $\sigma \in Z(S_n) = \{e\}$, contradiction. Therefore, $|N| = 1$, which means N is trivial. □

1.11 Semidirect Product

Definition 1.11.1 (Internal Direct Product)**.** *Recall the definition: consider $K, H \lhd G$, then $G = H \times K$ is considered to be the internal direct product if*

1. *every $g \in G$ can be written uniquely as $g = hk$ for some $h \in H, k \in K$.*

   Equivalently,

2. *$H \times K \to G$ defined by $(h, k) \mapsto hk$ is a bijection.*
3. *$G = H \cdot K$ and $H \cap K = \{e\}$.*
4. *for finite G, $G = HK$ and $|G| = |H| \cdot |K|$.*
5. *for finite G, $H \cap K = \{e\}$ and $|G| = |H| \cdot |K|$.*

Analogously, we define internal semidirect products.

Definition 1.11.2 (Internal Semidirect Product)**.** *Consider $K, H \subseteq G$ where $H \lhd G$. Then G is the internal semidirect product of H and K, denoted by $G = H \rtimes K$, if all the equivalent conditions hold in the previous definition **1.11.1**.*

Remark 1.11.3. *For $h_1, h_2 \in H$ and $k_1, k_2 \in K$, $(h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})k_1k_2 = h_1(f_{k_1}(h_2))(k_1k_2) \in HK$, where $f_k : H \to H$ is defined as $f_k(h) = khk^{-1}$ for $k \in K, h \in H$.*

Note that $f_e = \mathbf{id}_H$, $f_k \circ f_{k'} = f_{kk'}$, and $(f_k)^{-1} = f_{k^{-1}}$. Therefore, this is a homomorphism.

Furthermore, $f_k \in Aut(H)$. Therefore, $f : K \to Aut(H)$ is a homomorphism where $f(k) = f_k$.

In particular, $f : K \to Aut(H) \hookrightarrow \sum(H)$, K acts on H by automorphisms.

Definition 1.11.4 (External Semidirect Product)**.** *Consider K, H as groups. $f : K \to Aut(H)$ is a homomorphism. Let $G = H \times K = \{hk : h \in H, k \in K\}$ be a set, with the product defined by $(h_1, k_1) \cdot (h_2, k_2) = (h_1f(k_1)h_2, k_1k_2)$.*

G is a group based on this operation, called the external semidirect product of H and K with respect to f, denoted $G = H \rtimes_f K$.

Remark 1.11.5. *Let $G = H \rtimes_f K$ be the external semidirect product.*

Denote $H' = \{(h, e_K), h \in H\} \lhd G$, then $H' \cong H$.

Denote $K' = \{(e_H, k), k \in K\} \subseteq G$, then $K' \cong K$.

In particular, $(h, k) = (h, e_K) \cdot (e_H, K) \in H' \rtimes K'$. Therefore, $G = H' \rtimes K'$ as an internal semidirect product.

Remark 1.11.6. *Let $G = H \rtimes K$ be the internal semidirect product. Consider the bijection $H \times K \to G$ where $(h, k) \mapsto hk$. We can use f to define $H \rtimes K$ on the set $H \times K$. In particular, the map $H \rtimes_f K \xrightarrow{\cong} G$ is an isomorphism.*

Remark 1.11.7. *Both semidirect products are the usual product if and only if $f : K \to Aut(H)$ is trivial if and only if K acts on H trivially.*

Example 1.11.8.

1. *Consider $S_3 \supseteq H, K$ where $H = \langle(1\ 2\ 3)\rangle$ and $K = \langle(1\ 2)\rangle$. In particular, $H \lhd S_3$ and $H \cap K = \{e\}$, and $|H| \cdot |K| = 3 \cdot 2 = 6 = |S_3|$. Hence, S_3 is a semidirect product of $H \rtimes K$.*

2. *$S_4 \supseteq N = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, and let $S_3 = K \subseteq S_4$. Note that $N \cap K = \{e\}$, and $|N| \cdot |K| = 4 \times 6 = 24 = |S_4|$. Therefore, $S_4 = N \rtimes K$. Observe that there is $f : S_3 \xrightarrow{\cong} Aut(N)$.*

3. *Consider $|G| = pq$ where $q < p$ are prime numbers. Moreover, let $p \equiv 1 \pmod q$. Note that $G_p \lhd G, G_q \subseteq G$, $G_p \cap G_q = \{e\}$, $|G_p| \times |G_q| = |G|$. Therefore, $G = G_p \rtimes G_q$.*

   Now consider $f : \mathbb{Z}/q\mathbb{Z} = G_q \to Aut(G_p) = Aut(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Note that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p - 1$.

   Since $p \equiv 1 \pmod q$, so $q \mid p-1$, then there is a nontrivial map $f([1]) = h \neq 1 \in H$, as $h^q = [1]$. Hence, $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ is a non-Abelian group of order pq. Even though there are $q-1$ maps, they are all isomorphic. Therefore, it is the unique non-trivial construction.

4. *Let C be a cyclic group of order n, where $\sigma \in C$ is a generator. Let $K = \{e, \tau\}$ be cyclic of order 2.*

   Consider $f : K \to Aut(C)$ where $f(e) = \mathbf{id}$ and $f(\tau) = (x \mapsto x^{-1})$.

   Now, D_{2n} is defined as the group $C \rtimes_f K$, the dihedral group, with generators σ, τ as $\sigma^n = e$ and $\tau^2 = e$.

   Note that $\tau\sigma\tau^{-1} = \sigma^{-1}$, which means $\tau\sigma\sigma^{-1}\tau$.

   In particular, with $f : K \to Aut(\mathbb{Z})$ defined by $\tau \mapsto (x \mapsto -x)$ and $e \mapsto e$, we have $\mathbb{Z} \rtimes_f K = D_\infty$.

Remark 1.11.9 (Classification of Small Order Groups).

1. *Order 1:* $\{e\}$
2. *Order 2:* $\mathbb{Z}/2\mathbb{Z}$
3. *Order 3:* $\mathbb{Z}/3\mathbb{Z}$
4. *Order 4:* $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Since* $|G| = p^2$, *then* G *is Abelian. If there exists* $\sigma \in G$ *with order* p^2, *then* G *is cyclic, and is isomorphic to* $\mathbb{Z}/4\mathbb{Z}$. *If* $\forall \sigma \in G$ *we have* $\sigma^p = 1$, *then* $p \cdot \sigma = 0$, *which means* G *is a vector space over* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. *In particular,* $G \cong \mathbb{F}_p \times \mathbb{F}_p$.
5. *Order 5:* $\mathbb{Z}/5\mathbb{Z}$
6. *Order 6: Note that* $6 = 2 \times 3$ *as product of two primes and* $3 \equiv 1 \pmod 2$. *In general, we can write* $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Then we have* $\mathbb{Z}/2\mathbb{Z} \to Aut(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^\times$. *Therefore for* $[x]^2 = [1]$, *we have* $x \equiv \pm 1 \pmod p$. *When* $x = [1]$, *we have* $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}$; *when* $x = [-1]$, *we have* $G = D_{2p}$.

   In particular, when $p = 3$, *we have two groups* $\mathbb{Z}/6\mathbb{Z}$ *and* D_6.
7. *Order 7:* $\mathbb{Z}/7\mathbb{Z}$
8. *Order 8:*

   a) *Suppose* $\exists x \in G$ *of order* 8, *then* $G \cong \mathbb{Z}/8\mathbb{Z}$.

   b) *Suppose* $\forall x \in G$, $x^2 = e$, *then* G *is a vector space over* $\mathbb{Z}/2\mathbb{Z}$. *In particular,* $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   c) *Suppose* $\exists x \in G$ *with order* 4. *Denote* $H = \langle x \rangle$, *then* H *has order* 4 *and is a normal subgroup of* G.

      i. *Suppose* $\exists y \in G \backslash H$ *such that* $y^2 = e$, *then denote* $K = \langle y \rangle = \{e, y\}$. *Note that* $K \cap H. = \{e\}$, *and* $|K| \times |H| = |G|$, *then* $G = H \rtimes K$. *There is* $K = \mathbb{Z}/2\mathbb{Z} \xrightarrow{f} Aut(H) = (\mathbb{Z}/2\mathbb{Z})^\times$, *which is cyclic of order 2.*

      If f *is trivial, then* $G = H \times K = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *If not, then* $G = D_8$.

      ii. *Suppose* $\forall y \in G \backslash H$, y *has order* 4. *Therefore,* G/H *is cyclic of order* 2. *Hence,* $y^2 H = (yH)^2 = H$ *with* $e \neq y^2 \in H$. *Then* $G = \{e, x, x^2, x^3, y, xy, x^2y, x^3y\}$.

      Observe that $y^2 \in H$ *has order* 2, *then* $y^2 = x^2$. *However,* $xy \neq yx$ *otherwise* $xyxy = x^2y^2 = x^4 = e$, *but* $xy \notin H$, *contradiction. Furthermore,*

$H \ni yxy^{-1} \neq x$, but the order of yxy^{-1} is the same as the order of x, which is 4. Therefore, $yxy^{-1} = x^3$, so $yx = x^3y$. In particular, $G \cong Q_8$. Note that $c = x^2 = y^2$ commutes with x and y, so c is in the center. Then $Q_8 = \{e, x, y, xy, c, cx, cy, cxy\}$ and $cx = xc$, $cy = yc$, $x^4 = e = y^4$, $yx = cxy$.

Finally, notice that $Q_8 = \mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ where $i^2 = j^2 = -1$ and $k = ij = -ji$.

Note that D_8 has 5 elements of order 2, and Q_8 has 1 element of order 2, with other 3 groups are Abelian.

9. *Note $9 = 3^2$, then the groups are $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

10. *Since $2 \times 5 = 10$, then the possible groups are $\mathbb{Z}/10\mathbb{Z}$ and D_{10}.*

11. $\mathbb{Z}/11\mathbb{Z}$

12. *By Sylow's Theorem, there exists a subgroup $H \subseteq G$ of order 4 and a subgroup $K \subseteq G$ of order 3. We claim that at least one of H and K is normal in G.*

    Note that the number of Sylow 3-subgroups divides 4 and is equivalent to 1 modulo 3. Suppose K is not normal in G, then K is not the unique Sylow 3-subgroup, which means there are four Sylow 3-subgroups. In particular, there are $(3-1) * 4 = 8$ non-identity elements. On the other hand, this means the Sylow 2-subgroup H has to be unique. Therefore, $H \lhd K$. Therefore, either $G = H \rtimes K$ or $G = K \rtimes H$.

    Suppose $G \cong H \rtimes K$. In particular, there is $f : K \to Aut(H)$. If H is cyclic, then $Aut(H) = (\mathbb{Z}/4\mathbb{Z})^\times$ of order 2, which means f is trivial, so $G = H \times K = \mathbb{Z}/12\mathbb{Z}$; If $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then $Aut(H) = S_3$. In particular, $f : \mathbb{Z}/3\mathbb{Z} \to S_3$. If f is trivial, $G = H \times K = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. If f is not trivial, $G = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z} \cong A_4$. (Note that $S_4 \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes S_3$.)

    Suppose $K \lhd G$, then $G = K \rtimes H$. There is $f : H \to Aut(K) = (\mathbb{Z}/3\mathbb{Z})^\times$ cyclic of order 2. If $H = \mathbb{Z}/4\mathbb{Z}$, f is either trivial with $G = K \times H = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/12\mathbb{Z}$, or f is the only non-trivial homomorphism $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $[1]_4 \mapsto [1]_2$, $G = K \rtimes H = Dic_{12}$ dicyclic group. If $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, f is non-trivial, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, with $f' = f \circ g$ for $g \in Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Therefore, $G = D_{12}$.

We have two Abelian groups $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (also known as the direct product of $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$). The non-Abelian groups can be characterized by the following:

	A_4	D_{12}	Dic_{12}
$H \lhd G$	✓		
$K \lhd G$		✓	✓
$H \cong \mathbb{Z}/4\mathbb{Z}$			✓
$H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	✓	✓	

13. $\mathbb{Z}/13\mathbb{Z}$

14. *Since $14 = 2 \times 7$, we have $\mathbb{Z}/14\mathbb{Z}$ and D_{14}.*

15. *Recall from corollary **1.8.7** that this is cyclic, which means it is $\mathbb{Z}/15\mathbb{Z}$.*

16. *Groups start to be more complicated: there are 14 groups of order 16.*

Remark 1.11.10. *All groups above are either cyclic or semidirect product of two cyclic groups, except Q_8.*

Definition 1.11.11 (Short Exact Sequence)**.** *Consider a sequence $H \xrightarrow{s} G \xrightarrow{t} F$. Note that $t \circ s = 1$ if and only if $\ker(t) \supseteq im(s)$.*

We say this sequence is exact if $\ker(t) = im(s)$.

In particular, the sequence $1 \to G \xrightarrow{t} F$ is exact if and only if t is injective; the sequence $H \xrightarrow{s} G \to 1$ is exact if and only if s is surjective.

The sequence $\cdots \to G_1 \xrightarrow{s_1} G_2 \xrightarrow{s_2} G_3 \xrightarrow{s_3} G_4 \to \cdots$ is exact if every sequence $G_{i-1} \xrightarrow{s_{i-1}} G_i \xrightarrow{s_i} G_{i+1}$ is exact $\forall i$.

Note that $1 \to H \xrightarrow{s} G \xrightarrow{t} F \to 1$ is exact if and only if t is surjective and $im(s) = \ker(t)$. This is called a short exact sequence.

Example 1.11.12. *Suppose $H \lhd G$. Consider the short exact sequence*

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, hook, "s"] & G \arrow[r, two heads, "t"] & G/H \arrow[r] & 1 \end{tikzcd}$$

Figure 1.4: Standard Short Exact Sequence

We claim that every short exact sequence is isomorphic to this one.

Consider an arbitrary short exact sequence $1 \to H \xrightarrow{s} G \xrightarrow{t} F \to 1$. Note that $H = \ker(t) \lhd G$. Then by the First Isomorphism Theorem, $F = im(t) \cong G/\ker(t) = G/im(s) = G/H$. Therefore, we have

$$\begin{tikzcd}
1 \arrow[r] & H \arrow[r, "s"] \arrow[d, equal] & G \arrow[r, "t"] \arrow[d, equal] & F \arrow[r] \arrow[d, "\cong"] & 1 \\
1 \arrow[r] & H \arrow[r, hook, "s"] & G \arrow[r, two heads, "t"] & G/H \arrow[r] & 1
\end{tikzcd}$$

Figure 1.5: Isomorphism between the Sequences

Definition 1.11.13 (Split). *A short exact sequence is split if $\exists K \subseteq G$ such that $t|_K : K \to F$ is an isomorphism.*

Equivalently, the short exact sequence is split if and only if there exists a group homomorphism $v : F \to G$ such that $t \circ v = id_F$. v is called a splitting of the short exact sequence. Note that the splitting may not be unique.

$$\begin{tikzcd}
1 \arrow[r] & H \arrow[r, hook, "s"] & G \arrow[r, two heads, "t"] & G/H \arrow[r] \arrow[l, bend right, dashed, "v"'] & 1 \\
 & & K \arrow[u, hook] \arrow[ur, "t|_K"', "\cong"] & &
\end{tikzcd}$$

Figure 1.6: Split Short Exact Sequence

Remark 1.11.14. *Indeed, we can take $v = i \circ (t|_K)^{-1}$ where i is the inclusion map from K to G, for $x \in F$ we have $(t \circ v)(x) = t(v(x)) = x$, which means $t \circ v = id_F$.*

On the other hand, let $K = im(v) \subseteq G$. Then consider $id : F \overset{v}{\twoheadrightarrow} K \xrightarrow{t|_K} F$. Note that v has to be an isomorphism. Then since id is another isomorphism, then $t|_K$ has to be an isomorphism.

Example 1.11.15. *1. Consider the following short exact sequence:*

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "s"] & \mathbb{Z}/4\mathbb{Z} \arrow[r, "t"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

where $s([1]_2) = s([1]_4)$ and $t([a]_4) = ([a]_2)$. However, this is not a split short exact sequence. Suppose such $K \subseteq \mathbb{Z}/4\mathbb{Z}$ exists, then $K \cong \mathbb{Z}/2\mathbb{Z}$, so $K = \ker(t)$, which means $t|_K : K \to \mathbb{Z}/2\mathbb{Z}$ has to be the zero map.

2. Let $G = H \rtimes K$ where $H \lhd G$. Consider the following sequence:

$$\begin{tikzcd}
1 \arrow[r] & H \arrow[r, hook, "s"] & G \arrow[r, two heads, "t"] & K \arrow[r] & 1 \\
 & & K \arrow[u, hook] & &
\end{tikzcd}$$

Figure 1.7: Standard Split Short Exact Sequence

For arbitrary $g \in G$, there is unique $h \in H, k \in K$ such that $g = hk$. We now define $t : G \to K$ with $t(g) = k$ for any g, k defined above. In particular, the map has $\ker(t) = H$. Therefore, this is a short exact sequence. This sequence is also split. For $k = e \cdot k$, we have $t(k) = k$, so $t|_K = id_K$.

We claim that every split short exact sequence is isomorphic the sequence above.

Consider the arbitrary split short exact sequence below.

$$\begin{tikzcd}
1 \arrow[r] & H \arrow[r, hook, "s"] & G \arrow[r, two heads, "t"] & G/H \arrow[r] & 1 \\
 & & K \arrow[u, hook] \arrow[ur, "\cong", "t|_K"'] & &
\end{tikzcd}$$

We claim that $G = H \rtimes K$. In particular, we show that $G = H \cdot K$ and $H \cap K = \{e\}$.

For $x \in G$, $y = t(x)$, there exists $k \in K$ such that $t(k) = y$. Therefore, $t(xk^{-1}) = t(x) \cdot t(k)^{-1} = y \cdot y^{-1} = e$. Therefore, let $h = xk^{-1}$, and we have $h = xk^{-1} \in \ker(t) = H$. Hence, $x = h \cdot k$.

Take $x \in H \cap K$, then $t(x) = e$ since $x \in H$, and $t|_K(x) = e$ since $x \in K$. However, $t|_K$ is an isomorphism, so $x = e$.

Hence, $G = H \rtimes K$ by definition.

Therefore, we have the following correspondence:

$$\begin{tikzcd}
1 \arrow[r] & H \arrow[r] & G \arrow[r] & F \arrow[r] & 1 \\
1 \arrow[r] & H \arrow[u, equal] \arrow[r, hook] & H \rtimes K \arrow[u, equal] \arrow[r] & K \arrow[u, "\cong", "t|_K"'] \arrow[r] & 1
\end{tikzcd}$$

Figure 1.8: Isomorphism between the Sequences

Example 1.11.16. *Let $|G| = 8$ and take $H \subseteq G$ as a subgroup of order 4. Note that $H \lhd G$. Now, the short exact sequence*

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, hook] & G \arrow[r, two heads] & G/H \arrow[r] & 1 \end{tikzcd}$$

is split if $G = D_8 = \left\langle \sigma, \tau | \sigma^4 = \tau^2 = 1 \right\rangle$ *and* $H = \langle \sigma \rangle$ *and* $K = \langle \tau \rangle$*; it is not split if* $G = D_8$.

1.12 Free Group

Definition 1.12.1 (Letter, Alphabet, Word)**.** *Let X be a set. Then $x \in X$ is called a letter x in the alphabet X. We call $x_1 x_2 \cdots x_n$ a word where $x_i \in X$ are letters.*

Remark 1.12.2. *Let S be the set of all words. For $v = x_1 \cdots x_n$ and $w = y_1 \cdots y_m$, define $v \cdot w = x_1 \cdots x_n y_1 \cdots y_m$. Note that S is still not a group.*

Consider $\bar{X}$ as "a copy" of X: using different notation for the exact same set. There is clearly a bijection between $\bar{x} \in \bar{X}$ and $x \in X$, with $\bar{\bar{x}} = x$.

For $X \cup \bar{X}$, let T be the set of all words in $X \cup \bar{X}$. We hope to let $\bar{X} = X^{-1}$ since we don't have inverses in the set yet.

We define the operation of a reduction $\mapsto$. Let $u = vx\bar{x}w$ where v, w are words and $x \in X \cup \bar{X}$. Then a reduction is $u = vx\bar{x}w \mapsto vw$.

We define an equivalence relation based on the reduction operation. We say two words $u, u' \in T$ are equivalent with $u \sim u'$ if $\exists u_0 = u,\ u_1, \cdots, u_n = u'$ in T such that for all i we have $u_i \mapsto u_{i+1}$ or $u_{i+1} \mapsto u_i$.

For example, we know $xy\bar{y}\bar{z}zt \mapsto x\bar{z}zt \mapsto xt$, and $xy\bar{y}\bar{z}zt \mapsto x\bar{z}zt \mapsto xt$, then $xy\bar{y}\bar{z}zt \sim x\bar{z}r\bar{r}zt$.

The set of equivalence classes $T/\sim$ should be a free group. Let $F(x)$ be the set of equivalence class of words (in $X \cup \bar{X}$). In particular, if v is a word, then $[v] \in F(X)$.

The equivalence class is well-defined as $[v] \cdot [w] = [vw]$, and if $v_1 \sim v_2$ and $w_1 \sim w_2$, by definition there is $[v_1 w_1] = [v_2 w_2]$ by reduction.

Claim 1.12.3. *$F(X)$ is a group on set X, namely the free group.*

Proof.

1. For arbitrary $[u], [v] \in F(X)$, there is $([u] \cdot [v]) \cdot [w] = [uv] \cdot [w] = [uvw] = [u] \cdot [vw] = [u] \cdot ([v] \cdot [w])$.
2. $e = [\_] = [\varnothing]$
3. For $u = x_1 \cdots x_n$ where $x_i \in X \cup \bar{X}$, define $v = \bar{x_n} \bar{x_{n-1}} \cdots \bar{x_1}$, then uv is reduced to $\varnothing$ and vu is also reduced to $\varnothing$. Therefore, we have found an inverse for u.

□

For abbreviation, we write u for $[u]$, and u^{-1} for such v above. Every element in $F(X)$ can be written as $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ for some $x_i \in X$ and some $\varepsilon_i = \pm 1$.

Note that every equivalence class in $F(X)$ contains an irreducible word (a word of the minimal length i.e. cannot be further reduced). Indeed, this can be done by picking the word of smallest length, since a reduction operation at least reduces the length of 2.

Proposition 1.12.4. *Every equivalence class in $F(X)$ contains exactly one irreducible word.*

Proof. Suppose $u \sim v$ are irreducible words in the same equivalence class. Therefore, there is a sequence $w_1, w_2, \cdots, w_n$ where $w_1 = u$ and $w_n = v$, and $\forall i = 1, \cdots, n-1$, one of u_i, u_{i+1} is a reduction of the other, i.e. $w_i \mapsto w_{i+1}$ or $w_{i+1} \mapsto w_i$.

Let n be the length of the shortest possible sequence from u to v. We want to show that $n = 1$ and $u = w_1 = v$.

Assume $n \geq 2$, then $u = w_1 \mapsfrom w_2, \cdots, w_{n-1} \mapsto w_n = v$. Let w_i be the longest word among $w_2, \cdots, w_{n-1}$. Therefore, there must be a reduction $w_{i-1} \mapsfrom w_i \mapsto w_{i+1}$. Suppose the first reduction reduces $x\bar{x}$ and the second reduction reduces $y\bar{y}$. We split into cases.

Case 1: suppose $x\bar{x} = y\bar{y}$. Then we can write $w_{i-1} = ab$, $w_i = ax\bar{x}b$ and $w_{i+1} = ab$. Hence, $w_{i-1} = w_{i+1}$. However, that means we can delete w_{i-1} and w_i from the sequence, a contradiction since n is the smallest.

Case 2: suppose $x\bar{x}$ and $y\bar{y}$ overlaps, i,e, $y = \bar{x}$. Therefore, we have $w_{i-1} = axb$, $w_i = ax\bar{x}xb$ and $w_{i+1} = axb$. Similar to case 1, since $w_{i-1} = w_{i+1}$, we know this is a contradiction.

Case 3: suppose $x\bar{x}$ and $y\bar{y}$ don't overlap. Therefore, we have the following diagram:

$$\begin{tikzcd}
aby\bar{y}c \arrow[dr] & ax\bar{x}by\bar{y}c \arrow[l] \arrow[r] & ax\bar{x}bc \arrow[dl] \\
& abc &
\end{tikzcd}$$

Denote $w_i = abc$. Therefore, we can replace the sequence $w_1, \cdots, w_i, \cdots, w_n$ with $w_1, \cdots, w_i', \cdots, w_n$. However, the length of w_i' must be shorter than w_i, which is a contradiction.

Therefore, the irreducible word has to be unique in the equivalence class. □

Remark 1.12.5. *For a set X, there is a bijection between $F(X)$ and the set of irreducible words.*

Example 1.12.6. *1. For $X = \varnothing$, $F(X) = \{e\}$.*

2. For $X = \{x\}$, $F(X)$ consists of n-term words $xx \cdots x$ or $\bar{x}\bar{x} \cdots \bar{x}$. These words are irreducible.

In particular, $F(X) \cong \mathbb{Z}$ is an infinite cyclic group generated by $x \in X$.

3. If $|X| \geq 2$, for $x \neq y \in X$, $xy \neq yx \in F(X)$. Therefore, $F(X)$ is not Abelian.

Theorem 1.12.7 (Universal Property of Free Groups)**.** *Let X be a set and G be a group. Then every map $f : X \to G$ of sets extends uniquely to a group homomorphism $\tilde{f} : F(X) \to G$, i.e. $\tilde{f}(x) = f(x)\ \forall x \in X$.*

Proof. Take arbitrary $u \in F(X)$, then we can write $u = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ for some $x_i \in X$.

Note that $\tilde{f}(x_i) = f(x_i)$ and $\tilde{f}(x_i^{-1}) = \tilde{f}(x_i)^{-1} = f(x_i)^{-1}$, and therefore $\tilde{f}(x_i^{\varepsilon_i}) = f(x_i^{\varepsilon_i})$. Therefore, $\tilde{f}(u) = f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n}$. Note that if such a homomorphism exists, then it must be unique given by f.

Note that a desired group homomorphism exists by using the definition above. The definition is well-defined. Suppose $v \mapsto u$ for $v = a \cdot x\bar{x} \cdot b$ and $u = ab$. Then $\tilde{f}(ax\bar{x}b) = \tilde{f}(a) \cdot f(x) \cdot f(x)^{-1} \cdot \tilde{f}(b) = \tilde{f}(a) \cdot \tilde{f}(b) = \tilde{f}(u)$. Hence, $\tilde{f}(uv) = \tilde{f}(u)\tilde{f}(v)$, hence f is a well-defined homomorphism indeed. This concludes the proof. □

Remark 1.12.8. *Note that we don't have any relations between the generators at this point, which is why the group is called a "free group".*

Let H be a group and $R \subseteq H$ be a subset. We denote $\langle\langle R \rangle\rangle$ as the normal subgroup generated by R, which is the smallest subgroup containing R, and the intersections of all subgroups containing R.

Proposition 1.12.9. $\langle\langle R \rangle\rangle = \{(g_1 \tau_1 g_1^{-1})^{\varepsilon_1} \cdots (g_n \tau_n g_n^{-1})^{\varepsilon_n}, \tau_i \in R, g_i \in H, \varepsilon_i = \pm 1\} = \left\langle\left\langle \bigcup_{g \in G} gRg^{-1} \right\rangle\right\rangle$.

Proof. See Homework 6 problem 6. □

Let X be a set and $F(X)$ be a free group. Suppose $R \subseteq F(X)$ is the subset of irreducible words, then let $G = F(X)/\langle\langle R \rangle\rangle$. Consider the map $X \hookrightarrow F(X) \xrightarrow{\pi} G$, which sends $x \in X$ to $x \in G$. Note that the set of $\{x \in G\}$ would generate G, then define the relation in G as $r = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in F(X)$, so $r \in \langle\langle R \rangle\rangle$ by definition. In particular, $r = e \in G$ by the mapping above, and we say R is the set of defining relations, with $r \in R$ is a relation in G.

We say that $G = F(X)/\langle\langle R\rangle\rangle = \langle X \mid R\rangle$ is the group defined by generators X and relations R.

Remark 1.12.10. *For a free group $F(X)$ over a set X, the group has no relations, i.e. $R = \varnothing$.*

Proposition 1.12.11. *Let $G = \langle X \mid R\rangle$ and H be a group. Define $f : X \to H$ as a map of sets such that $f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n} = e_H$ for all $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in R$. Then there is a unique homomorphism $\tilde{f} : G \to H$ such that $\tilde{f}(x) = f(x)\ \forall x \in X$.*

Proof. Note that by extension of f, there is a homomorphism $\hat{f} : F(X) \to H$ such that $\hat{f}(x) = f(x)\ \forall x \in X$. Let $N = \ker(\hat{f}) \lhd F(X)$.

Consider $\tau = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in R$, $\hat{f}(\tau) = \hat{f}(x_1)^{\varepsilon_1} \cdots \hat{f}(x_n)^{\varepsilon_n} = f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n} = e_H$.

Since $R \subseteq \ker(\tilde{f}) = N$, then $\langle\langle R\rangle\rangle \subseteq N$.

Now $\bar{f}$ factors through the map as the following:

$$\begin{tikzcd}
F(X)/\langle\langle R\rangle\rangle \arrow[rr, "\tilde{f}"] & & H \\
& F(X) \arrow[ul, "\pi"] \arrow[ur, "\hat{f}"] &
\end{tikzcd}$$

Figure 1.9: Factoring Property between Group and Corresponding Presentation

In particular, $xN \in G$ if and only if $x \in X$, then $\tilde{f}(x) = \tilde{f}(Nx) = \hat{f}(x) = f(x)$.

□

We now consider the relationship backwards.

Let G be a group with a generating set $X \subseteq G$. The inclusion map $X \hookrightarrow G$ extends $\hat{f} : F(X) \twoheadrightarrow G$ by $x \mapsto x$. Let $N = \ker(\hat{f}) \lhd F(X)$. Let $R \subseteq N$ be a subset such that $\langle\langle R\rangle\rangle = N$. By the First Isomorphism Theorem, $G = \operatorname{im}(\hat{f}) \cong F(X)/N = F(X)/\langle\langle R\rangle\rangle = \langle X \mid R\rangle$. Therefore, $G \cong \langle X \mid R\rangle$.

Definition 1.12.12 (Presentation)**.** *$\langle X \mid R\rangle$ defined above is called the presentation of the group G.*

Proposition 1.12.13. *Every group G has a presentation.*

Proof. An explicit presentation is $G \cong \langle G \mid \{abc \mid a, b, c \in G \text{ with } abc = 1 \text{ in } G\}\rangle$. □

Example 1.12.14. *1. Consider $\mathbb{Z}/n\mathbb{Z}$. Note that $\mathbb{Z} = F(\{\sigma\}) = \langle \sigma \mid \varnothing \rangle$ for some arbitrary σ, with $\langle\langle \sigma^n \rangle\rangle = n\mathbb{Z}$. Therefore, $\mathbb{Z}/n\mathbb{Z} = \langle \sigma \mid \sigma^n \rangle$.*

2. Consider the group D_{2n}. Note that the group is generated by σ and τ where $\sigma^n = e = \tau^2$ and $\tau\sigma\tau\sigma = e$.

We claim that $D_{2n} = \left\langle \sigma, \tau \mid \sigma^n, \tau^2, \tau\sigma\tau\sigma \right\rangle$, defined as a set named S. Now pick $\bar{\sigma}, \bar{\tau} \in S$. We have $\bar{\sigma}^n = e$, $\bar{\tau}^2 = e$, and therefore note that $\bar{\tau}^{-1} = \tau$. Notice that there is a defined surjective homomorphism from S to D_{2n} because S at least has $2n$ elements.

For $v \in F(\sigma, \tau)$, we have $\bar{v} = \bar{\sigma}^{a_1}\bar{\tau}^{b_1}\bar{\sigma}^{a_2}\bar{\tau}^{b_2}\cdots = \bar{\sigma}^i\bar{\tau}^j$. In particular, $2n = |D_{2n}| \leq |S| \leq 2n$. Therefore, the two groups must have the same order, and we can then conclude that there is an isomorphism.

3. $\left\langle \sigma, \tau \mid \sigma^2, \tau^2, (\sigma\tau)^2 \right\rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4. $H = \left\langle x, y \mid x^2, y^2 \right\rangle \cong D_\infty = \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Take $\sigma \in \mathbb{Z}$ and $\tau \in \mathbb{Z}/2\mathbb{Z}$. Note that $\tau\sigma\tau^{-1} = \sigma^{-1}$, and $\tau^2 = e$, so $(\tau\sigma)^2 = e$. In particular, take the map $x \mapsto \tau\sigma$ and $y \mapsto \tau$.

Furthermore, we can construct the inverse with $\tau \mapsto y$ and $\sigma \mapsto yx$. In particular, as $yx \in H$, we have $\langle yx \rangle \lhd H$ and $H = \langle yx \rangle \rtimes \langle \tau \rangle$.

5. Consider $G \cong \left\langle x, y \mid x^2, y^3 \right\rangle$. Define the special linear group $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \det = 1 \right\}$. Then $G = SL_2(\mathbb{Z}) / \left\{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$.

Define $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. Note that $\sigma^2 = \tau^3 = e$. We may now obtain an isomorphism by mapping $x \mapsto \sigma$ and $y \mapsto \tau$.

Definition 1.12.15 (Free Product). *Let $(G_i)_{i \in I}$ be a family of groups, then the free product is defined as $\coprod\limits_{i \in I} G_i = F(\coprod\limits_{i \in I} G_i) / \langle\langle R \rangle\rangle$, where $R = \coprod\limits_{i \in I}(\{1_{G_i}\} \cup \{abc \mid a, b, c \in G_i, abc = 1_{G_i} \in G_i\}$.*

Remark 1.12.16. *The free product is the coproduct in the category of groups, sometimes denoted as $G * H$ instead of $G \coprod H$.*

Proposition 1.12.17. *Let $G_i = \langle A_i \mid R_i \rangle$, then $\coprod\limits_{i \in I} G_i = \left\langle \coprod\limits_{i \in I} A_i \mid \bigcup\limits_{i \in I} R_i \right\rangle$. Moreover, $\coprod\limits_{i \in I} G_i = \left\langle \bigcup\limits_{i \in I} S_i \mid \bigcup\limits_{i \in I} R_i \right\rangle$ where $G_i = \langle S_i \mid R_i \rangle$.*

Remark 1.12.18. *Analogously, if there are two disjoint sets S_1, S_2, then $\langle S_1 \mid R_1 \rangle * \langle S_2 \mid R_2 \rangle = \langle S_1 \cup S_2 \mid R_1 \cup R_2 \rangle$.*

Theorem 1.12.19 (Universal property of free products)**.** *Let $G = \coprod\limits_{i \in I} G_i$ for groups $(G_i \mid i \in I)$. Then for any group H and homomorphisms $f_i : G_i \to H$, there is a unique $f : G \to H$ such that $f_i = f \circ \iota_i$ for each $i \in I$.*

$$\begin{tikzcd}
 & H & \\
G_1 \arrow[ur, "f_1"] \arrow[r, "\iota_1"'] & G \arrow[u, dashed, "f"] & G_2 \arrow[ul, "f_2"'] \arrow[l, "\iota_2"]
\end{tikzcd}$$

Figure 1.10: Universal Property of Free Products

2 Category Theory in Group Context

2.1 Introduction to Categories

Definition 2.1.1 (Category)**.** *A category $\mathscr{C}$ consists of a class of objects ("dots") $\mathbf{Ob}(\mathscr{C})$ and a class of morphisms ("arrows") $\mathbf{Mor}(\mathscr{C})$ between the objects of $\mathscr{C}$.*

For objects $A, B \in \mathscr{C}$, a morphism $f : A \to B$ has A as the source and B as the target. For $f : A \to B$ and $g : B \to C$ as morphisms in $\mathscr{C}$, the composition $g \circ f$ is defined by $A \xrightarrow{g\circ f} C$, such that:

1. *Associativity holds: for $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, we have $h \circ (g \circ f) = (h \circ g) \circ f$.*
2. *$\forall A \in \mathbf{Ob}(\mathscr{C})$, there is a morphism $\mathbf{id}_A : A \to A$ such that $\forall f : X \to A$ morphism, $\mathbf{id}_A \circ f = f$, and $\forall g : A \to Y$ morphism, $g \circ \mathbf{id}_A = g$.*

Definition 2.1.2 (Small, Locally Small)**.** *For objects $A, B \in \mathscr{C}$, $\mathbf{Mor}_{\mathscr{C}}(A, B)$ is the class of morphisms from A to B.*

A category $\mathscr{C}$ is locally small if $\mathbf{Mor}_{\mathscr{C}}(A, B)$ is a set for all objects $A, B \in \mathscr{C}$.

A category $\mathscr{C}$ is small if it is locally small and $\mathbf{Ob}(\mathscr{C})$ is a set.

Definition 2.1.3 (Isomorphism)**.** *A morphism $f : A \to B$ in a category $\mathscr{C}$ is an isomorphism if $\exists g : B \to A$ such that $f \circ g = \mathbf{id}_B$ and $g \circ f = \mathbf{id}_A$. Such g is unique if exists, called the inverse of f, so $g = f^{-1}$, and $(f^{-1})^{-1} = f$.*

We denote $A \cong B$ if there exists an isomorphism $f : A \to B$.

Example 2.1.4.

1. *Denote* **Set** *as the category of sets. The objects of this category are sets and the morphisms are maps between sets.*

   Note $\mathbf{Mor}_{\mathbf{Set}}(X, Y) \subseteq X \times Y$ must be a set for $X, Y \in$ **Set**. *Therefore,* **Set** *is locally small. Isomorphisms in* **Set** *are just bijections.*

2. *Denote* **Grp** *as the category of groups. The objects of this category are groups and morphisms are the homomorphisms between groups.*

*Again, **Grp** is locally small, and isomorphisms between elements in **Grp** are just group isomorphisms.*

3. *Denote **Ab** as the category of Abelian groups. This is a subcategory of **Grp**.*

4. *Consider arbitrary set X, we can view the set as a category.*

   Here $\mathbf{Ob}(X) = X$ and $\mathbf{Mor}_X(x, x') = \begin{cases} \varnothing \textit{ if } x \neq x' \\ \{(x, x')\} \textit{ as identity if } x = x' \end{cases}$. This is a small category, and the only isomorphism is the identity.

5. *Let G be a group, then we can view the group as a category. Here $\mathbf{Ob}(G) = *$ and $\mathbf{Mor}(*, *) = G$ as a set, and the composition of morphisms is the group operation in G. Here, the identity morphisms is just the identity element of G.*

   This is a small category, and every morphisms in G is an isomorphism. Such G is called a groupoid.

6. *We can construct a group using the set $X = \{1, 2, \cdots, n\}$. Let the objects be the set X and let $\mathbf{Mor}_X(i, j) = \begin{cases} \varnothing \textit{ if } i > j \\ \{(i, j)\} \textit{ if } i \leq j \end{cases}$. The only isomorphisms in this category are the identities.*

   *This can be generalized to a category **Pos** of posets. One can also view the set of natural numbers $\mathbb{N}$ as a poset category.*

7. *Let $\mathscr{C}$ be a category, then we can define a category out of the morphisms of $\mathscr{C}$, denoted as $\mathbf{Ar}(\mathscr{C})$.*

   The objects of the category are morphisms $A \xrightarrow{f} B$ in $\mathscr{C}$, and the morphisms of any $A \xrightarrow{f} B$ and $A' \xrightarrow{f'} B'$ are a pair of morphisms $A \xrightarrow{g} A'$ and $B \xrightarrow{h} B'$ such that the diagram is commutative as follows:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "g"] & B \arrow[d, "h"] \\
A' \arrow[r, "f'"] & B
\end{tikzcd}$$

Figure 2.1: Morphisms in an Arrow Category

   i.e. $h \circ f = f' \circ g$.

8. *Let $\mathscr{C}$ be a category. The dual (opposite) category $\mathscr{C}^\circ$ has objects $\mathbf{Ob}(\mathscr{C}^\circ) = \mathbf{Ob}(\mathscr{C})$ (a copy $A^\circ \in \mathscr{C}^\circ$ for $A \in \mathscr{C}$) and morphisms $\mathbf{Mor}_{\mathscr{C}^\circ}(A^\circ, B^\circ) = \mathbf{Mor}_{\mathscr{C}}(B, A)$, i.e. a dual morphism $f^\circ : B \to A$ in $\mathscr{C}^\circ$ for $f : A \to B$ in $\mathscr{C}$.*

9. *Let $\mathscr{C}_1, \mathscr{C}_2$ be categories. Then we can define a product category $\mathscr{C}_1 \times \mathscr{C}_2$ from the two categories. The objects of $\mathscr{C}_1 \times \mathscr{C}_2$ are $\mathbf{Ob}(\mathscr{C}_1 \times \mathscr{C}_2) = \{(A_1, A_2) : A_1 \in \mathbf{Ob}(\mathscr{C}_1), A_2 \in \mathbf{Ob}(\mathscr{C}_2)\}$, and the morphisms for objects $(A_1, A_2), (B_1, B_2)$ in category $\mathscr{C}_1 \times \mathscr{C}_2$ are $\mathbf{Mor}_{\mathscr{C}_1 \times \mathscr{C}_2}((A_1, A_2), (B_1, B_2)) = \mathbf{Mor}_{\mathscr{C}_1}(A_1, B_1) \times \mathbf{Mor}_{\mathscr{C}_2}(A_2, B_2)$.*

10. *Let $\mathscr{C}$ be a category. Consider a subclass of objects $M \subseteq \mathbf{Ob}(\mathscr{C})$. We can derive a new category $\mathscr{C}'$ where the objects of the category are $\mathbf{Ob}(\mathscr{C}') = \mathbf{Ob}(\mathscr{C}) \backslash M$ and the morphisms are $\mathbf{Mor}_{\mathscr{C}'}(A, B) = \mathbf{Mor}_{\mathscr{C}}(A, B)$ if $A, B \notin M$.*

Definition 2.1.5 (Initial/Final Object)**.** *Let $\mathscr{C}$ be a category. An object $A \in \mathscr{C}$ is initial if $\forall B \in \mathbf{Ob}(\mathscr{C})$, $\exists!$ morphism $A \to B$.*

An object $A \in \mathscr{C}$ is final (terminal) if $\forall B \in \mathbf{Ob}(\mathscr{C})$, $\exists!$ morphism $B \to A$.

Remark 2.1.6. *Note that the initial objects in $\mathscr{C}$ are exactly the final objects in $\mathscr{C}^\circ$.*

Proposition 2.1.7. *Every two initial objects are canonically isomorphic.*

Proof. Let A, A' be initial in category $\mathscr{C}$. Then there exists a unique morphism $f : A \to A'$ and a unique morphism $g : A' \to A$. In particular, $g \circ f : A \to A$ must be the identity morphism since A is an initial object, and $f \circ g : A' \to A'$ must also be the identity morphism.

Hence, f, g are isomorphic, then this induces a unique isomorphism. Hence, $A \cong A'$. □

Remark 2.1.8. *Similarly, two final objects are canonically isomorphic.*

Example 2.1.9.

1. *Consider* **Set**. *The initial object of this category is $\varnothing$, and the final objects of this category are the singleton sets.*

   In particular, the set of maps from any set X to $\varnothing$ is $\varnothing$ if $X \neq \varnothing$ and is $\{\mathbf{id}_\varnothing\}$ if $X = \varnothing$.

2. *Consider* **Grp**. *The initial object and the final object of this category are both the identity group $\{e\}$.*

3. *For a group G defined as a category, recall that $\mathbf{Ob}(G) = \{*\}$ and $\mathbf{Mor}(*, *) = G$. Now, if $|G| > 1$, then there are no initial/final objects.*

4. *Consider the set* $X = \{1, 2, \cdots, n\}$ *as a category. Then* 1 *is the initial object and* n *is the final object.*

Notice that for a category $\mathscr{C}$ and $X, Y, X', Y' \in \mathbf{Ob}(\mathscr{C})$, with $f \in \mathbf{Mor}(Y, Y'), g \in \mathbf{Mor}(X, Y)$, then $f \circ g \in \mathbf{Mor}(X, Y')$. In particular, there is a map $f_* : \mathbf{Mor}(X, Y) \to \mathbf{Mor}(X, Y')$ such that $g \mapsto f \circ g$.

In a similar sense, consider $h \in \mathbf{Mor}(X, X')$, then $g \circ h \in \mathbf{Mor}(X, Y)$, and there is a map $h^* : \mathbf{Mor}(X', Y) \to \mathbf{Mor}(X, Y)$ with $g \mapsto g \circ h$.

Definition 2.1.10 (Product)**.** *For* $X, Y \in \mathscr{C}$ *as objects in a category, define the product of* X *and* Y *as* $X \times Y \in \mathscr{C}$ *with* $p : X \times Y \to X$ *and* $q : X \times Y \to Y$ *such that for all morphisms* $f : Z \to X$ *and* $g : Z \to Y$*, there is a unique* $h : Z \to X \times Y$ *with the property* $p \circ h = f$ *and* $q \circ h = g$*, i.e. the following diagram commutes:*

$$\begin{tikzcd}
Z \arrow[dr, dashed, "\exists ! h"] \arrow[drr, bend left, "f"] \arrow[ddr, bend right, "g"'] & & \\
& X \times Y \arrow[r, "p"] \arrow[d, "q"] & X \\
& Y &
\end{tikzcd}$$

Figure 2.2: Universal Property of Product

In particular, this induces a bijection $\mathbf{Mor}(Z, X \times Y) \xrightarrow{p_*, q_*} \mathbf{Mor}(Z, X) \times \mathbf{Mor}(Z, Y)$.

Example 2.1.11.

1. *Consider the category* **Set**. *The category has a usual product of sets.*

2. *Consider the category* **Grp**. *The category has a usual product of groups.*

3. *Consider the category* **Ab**. *The category has a usual product of Abelian groups.*

4. *Consider the category from the set* $X = \{1, 2, \cdots, n\}$ *where morphisms are the relations* $i \leq j$*. The product of this category is the minimal of* i *and* j*.*

For $f : X \to X'$ and $g : Y \to Y'$, they induce a morphism $f \times g : X \times Y \to X' \times Y'$ as follows:

$$\begin{tikzcd}
X \times Y \arrow[r] \arrow[d] \arrow[dr, dashed, "\exists! f\times g"] & X \arrow[dr, "f"] & \\
Y \arrow[dr, "g"'] & X' \times Y' \arrow[r] \arrow[d] & X' \\
& Y' &
\end{tikzcd}$$

Figure 2.3: Morphism Product

Moreover, the universal property can be induced by canonical isomorphism:

$$\begin{tikzcd}
Z \arrow[dr, dashed, "\exists!"'] \arrow[drr, dashed, "\exists!"] \arrow[drrr, bend left=50] \arrow[ddrr, bend right=50] & & & \\
& V \arrow[r, "\sim"] & X \times Y \arrow[r] \arrow[d] & X \\
& & Y &
\end{tikzcd}$$

Figure 2.4: Product Unique Up to Canonical Isomorphism

Proposition 2.1.12. *Let $X \times Y$ and $\widetilde{X \times Y}$ be two products of X and Y, then there is a unique isomorphism $X \times Y \underset{h}{\xrightarrow{\sim}} \widetilde{X \times Y}$ such that the diagram*

$$\begin{tikzcd}
X \times Y \arrow[r] \arrow[d] \arrow[dr, "h", "\sim"'] & X \\
Y & \widetilde{X \times Y} \arrow[l] \arrow[u]
\end{tikzcd}$$

commutes.

Proof. Consider the category of pairs of morphisms with objects $(Z \xrightarrow{f} X, Z \xrightarrow{g} Y)$ and morphisms $(Z \xrightarrow{f} X, Z \xrightarrow{g} Y) \to (Z' \xrightarrow{f'} X', Z' \xrightarrow{g'} Y')$, which is a morphism from Z to Z' such that the diagram

$$\begin{tikzcd}
Z \arrow[r, "g"] \arrow[d, "f"] \arrow[dr, "h"] & Y \\
X & Z' \arrow[l, "f'"] \arrow[u, "g'"']
\end{tikzcd}$$

commutes.

In particular, $(X \times Y \xrightarrow{p} X, X \times Y \xrightarrow{q} Y)$ is a final object. □

Remark 2.1.13. *We can define product of a family of objects in $\mathscr{C}$ by $\prod\limits_{i\in I} X_i$ and morphisms $\prod\limits_{i\in I} X_i \xrightarrow{p_j} X_j$.*

In particular, $\mathbf{Mor}(Z, \prod\limits_{i\in I} X_i) \xrightarrow[\sim]{p_{i*}} \prod\limits_{i\in I} \mathbf{Mor}(Z, X_i)$ is a bijection.

Definition 2.1.14 (Coproduct)**.** *Let $X, Y \in \mathscr{C}$. The coproduct $X * Y$ is an object together with two morphisms $X \to X * Y \leftarrow Y$ such that $\forall X \to Z, Y \to Z$, there exists a unique $X * Y \to Z$ such that the diagram*

$$\begin{tikzcd}
 & Y \arrow[d] \arrow[ddr, bend left] & \\
X \arrow[r] \arrow[drr, bend right] & X * Y \arrow[dr, dashed, "\exists!"] & \\
 & & Z
\end{tikzcd}$$

Figure 2.5: Universal Property of Coproduct

commutes.

Remark 2.1.15. *Note there is a bijection $\mathbf{Mor}(X * Y, Z) \to \mathbf{Mor}(X, Z) \times \mathbf{Mor}(Y, Z)$, sometimes also written as $\mathbf{Mor}(\coprod\limits_{i\in I} X_i, Z) \to \prod\limits_{i\in I} \mathbf{Mor}(X_i, Z)$.*

In particular, this tells us that $(X * Y)^\circ = X^\circ \times Y^\circ$, so the coproduct is a dual notion of the product.

Example 2.1.16. *1. Consider the category* **Set***. The coproduct is exact the disjoint union, i.e. $X * Y = X \coprod Y$.*

2. Consider the category **Grp***. Consider the product $G \times H$ in the usual sense. However, one may notice that the product is not equivalent to the coproduct. Indeed,* *consider $i : G \to G \times H$ by $g \mapsto (g, e_H)$ and $j : H \to G \times H$ by $h \mapsto (e_G, h)$. We would have the following diagram:*

$$\begin{tikzcd}
& H \arrow[d, "j"] \arrow[ddr, bend left, "t"] & \\
G \arrow[r, "i"] \arrow[drr, bend right, "s"'] & G \times H \arrow[dr, dashed, "\exists ! k"] & \\
& & Z
\end{tikzcd}$$

Figure 2.6: Universal Property of Product/Coproduct in Abelian Groups

Here, $(g, h) = (g, e) \cdot (e, h) = i(g) \cdot j(h)$. Furthermore, we have $k(g, h) = k(i(g)) \cdot k(j(h)) = s(g) \cdot t(h)$. Let this be the definition for our unique homomorphism k. Then we have $k((g, h) \cdot (g', h')) = k(gg', hh') = s(gg') \cdot t(hh')$. On the other hand, since k is a homomorphism, this is equivalent to $k(g, h) \cdot k(g', h') = s(g) \cdot t(h) \cdot s(g') \cdot t(h')$. This is true if and only if our choices of G, H are Abelian.

3. *For the category of Abelian groups* **Ab***, the coproduct is exactly the product, defined by the universal property in* ***Figure 2.6*** *above.*

4. *Reconsider the coproduct of groups. Let $G = \langle X \mid R \rangle$ and $H = \langle Y \mid S \rangle$. Define the coproduct by $G * H = \langle X \coprod Y \mid R \cup S \rangle$, where the unique homomorphism $k : G * H \to Z$ is generated by $k(x) = s(x)$ and $k(y) = t(y)$ for all $x \in x \in G, y \in H$, as shown in the figure below.*

$$\begin{tikzcd}
& H \arrow[d] \arrow[ddr, bend left, "t"] & \\
G \arrow[r] \arrow[drr, bend right, "s"'] & G \times H \arrow[dr, dashed, "\exists ! k"] & \\
& & Z
\end{tikzcd}$$

Example 2.1.17. 1. *Note that $\mathbb{Z}/2\mathbb{Z} \cong \left\langle \sigma \mid \sigma^2 \right\rangle$ as a presentation. Then $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} = \left\langle \sigma, \tau \mid \sigma^2, \tau^2 \right\rangle = D_\infty$, which is exactly the infinite dihedral group.*

2. *$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} = \left\langle \sigma, \tau \mid \sigma^2, \tau^3 \right\rangle = \mathbf{PSL}_2(\mathbb{Z})$, the projective special linear group over $\mathbb{Z}$.*

Definition 2.1.18 (Subcategory, Full)**.** *Let $\mathscr{C}$ be a category, and let $\mathscr{C}'$ be a category such that*

- $\mathbf{Ob}(\mathscr{C}') \subseteq \mathbf{Ob}(\mathscr{C})$, *and*
- $\mathbf{Mor}_{\mathscr{C}'}(X, Y) \subseteq \mathbf{Mor}_{\mathscr{C}}(X, Y)$ *for all* $X, Y \in \mathbf{Ob}(\mathscr{C}')$.

Then $\mathscr{C}'$ is a subcategory of $\mathscr{C}$.

If $\mathbf{Mor}_{\mathscr{C}'}(X, Y) = \mathbf{Mor}_{\mathscr{C}}(X, Y)$ for all $X, Y \in \mathbf{Ob}(\mathscr{C}')$, then we say $\mathscr{C}'$ is a full subcategory of $\mathscr{C}$.

Example 2.1.19. *1.* **Ab** *is a full subcategory of* **Grp**.

2. **Grp** *is a subcategory of* **Set**, *but not full.*

3. Let $M \subseteq \mathbf{Ob}(\mathscr{C})$ be a subclass of objects, then $\mathscr{C} \backslash M$ is a full subcategory of $\mathscr{C}$.

2.2 Functor

Definition 2.2.1 (Functor)**.** *Let $\mathscr{C}, \mathscr{D}$ be categories. A (covariant) functor $F : \mathscr{C} \to \mathscr{D}$ assigns to every object $C \in \mathscr{C}$ an object $FC \in \mathscr{D}$ and to every morphism $f : C \to D$ in $\mathscr{C}$ a morphism $Ff : FC \to FD$ in $\mathscr{D}$ such that*

- $F(f \circ g) = Ff \circ Fg$, *and*
- $F(\mathbf{id}_A) = \mathbf{id}_{FA}$.

On the other hand, a (contravariant) functor would be $F : \mathscr{C}^\circ \to \mathscr{D}$ that sends objects $C^\circ \in \mathscr{C}^\circ$ to $FC \in \mathscr{D}$ and morphisms $f : C \to C'$ in $\mathcal{C}$ to $Ff : FC' \to FC$ in $\mathscr{D}$.

Remark 2.2.2. *A functor takes isomorphisms to isomorphisms. If there is $f : X \to Y$ and $g : Y \to X$ such that $f \circ g = \mathbf{id}_Y$ and $g \circ f = \mathbf{id}_X$, then correspondingly there is $Ff : FX \to FY$ and $Fg : FY \to FX$ such that $Ff \circ Fg = \mathbf{id}_{FY}$ and $Fg \circ Ff = \mathbf{id}_{FX}$.*

Example 2.2.3. *1. For arbitrary category $\mathscr{C}$, there is an identity functor $\mathbf{Id} : \mathscr{C} \to \mathscr{C}$.*

2. For arbitrary categories $\mathscr{C}, \mathscr{D}$, there is a constant functor $F : \mathscr{C} \to \mathscr{D}$ such that for arbitrary $Y \in \mathbf{Ob}(D)$, there is $FX = Y$ for all $X \in \mathbf{Ob}(\mathscr{C})$ and $Ff = \mathbf{id}_Y$ for all $f \in \mathbf{Mor}_{\mathscr{C}}$.

3. *For some categories $\mathscr{C}$ that are set-based (e.g.* **Grp**, **Ring**, *etc), there is a forgetful functor $F : \mathscr{C} \to$* **Set** *that "forgets" the structure and transform it back to a set.*

4. *Let $\mathscr{C}'$ be a subcategory of $\mathscr{C}$, then there is an inclusion functor $\mathbf{i} : \mathscr{C}' \to \mathscr{C}$.*

5. *Let I be a category of the form*

$$\begin{tikzcd}
\cdot_1 \arrow[loop above] \arrow[r, "\alpha"] & \cdot_2 \arrow[loop above]
\end{tikzcd}$$

Then a functor $F : I \to \mathscr{C}$ would map $\cdot_1$ to some object X in $\mathscr{C}$ and map $\cdot_2$ to some object Y in $\mathscr{C}$, and map α to some morphism $f : X \to Y$ in $\mathscr{C}$.

Therefore, a functor from I to $\mathscr{C}$ induces a morphism in $\mathscr{C}$.

Moreover, for a small category I, a functor $F : I \to \mathscr{C}$ is equivalent to a commutative diagram of shape I in shape I in $\mathscr{C}$.

For example, there is the following correspondence given by a functor from I to $\mathscr{C}$:

$$\begin{tikzcd}
\cdot \arrow[r] \arrow[d] \arrow[dr] & \cdot \arrow[d] & \Longrightarrow & A \arrow[r] \arrow[d] \arrow[dr] & B \arrow[d] \\
\cdot \arrow[r] & \cdot & \Longrightarrow & C \arrow[r] & D
\end{tikzcd}$$

6. *Let G be a group with an induced category $\underline{G}$. Then $\mathbf{Ob}(\underline{G}) = \{*\}$ and $\mathbf{Mor}(*, *) = G$.*

A functor $F : \underline{G} \to$ **Set** *is just an G-action on a set.*

Definition 2.2.4 (Functor Representation)**.** *Let $\mathscr{C}$ be a locally small category. Take some $X \in \mathbf{Ob}(\mathscr{C})$.*

Define a functor $R^X : \mathscr{C} \to$ **Set** *that sends objects Y to $\mathbf{Mor}_{\mathscr{C}}(X, Y)$ and morphisms $f : Y \to Y'$ to $f_* : \mathbf{Mor}(X, Y) \to \mathbf{Mor}(X, Y')$, i.e. sends $R^X(Y)$ to $R^X(Y')$.*

If this is the case, then we say R^X is a functor represented by X.

Similarly, define $R_X : \mathscr{C}^\circ \to$ **Set** *by sending objects Y° to $\mathbf{Mor}_{\mathscr{C}}(Y, X)$ and morphisms $f^\circ : Y \to Y'$ to $f^* : \mathbf{Mor}(Y, X) \to \mathbf{Mor}(Y', X)$. If this is the case, then we say R_X is a functor corepresented by X.*

Remark 2.2.5. *Observe that the functor R^X is actually just the covariant Hom functor $\mathbf{Hom}(X, -)$ and the functor R_X is just the contravariant Hom functor $\mathbf{Hom}(-, X)$. They are called "representation" because of their relation with the notion of representable functors we introduce later.*

Definition 2.2.6 (Full, Faithful)**.** *A functor $F : \mathscr{C} \to \mathscr{D}$ is faithful if $\mathbf{Mor}_{\mathscr{C}}(X, Y) \to \mathbf{Mor}_{\mathscr{D}}(FX, FY)$ is injective $\forall X, Y \in \mathscr{C}$.*

A functor $F : \mathscr{C} \to \mathscr{D}$ is full if $\mathbf{Mor}_{\mathscr{C}}(X, Y) \to \mathbf{Mor}_{\mathscr{D}}(FX, FY)$ is surjective $\forall X, Y \in \mathscr{C}$.

We say a functor is fully faithful if it is both faithful and full.

Example 2.2.7. *Let $\mathscr{C}' \subseteq \mathscr{C}$ be a subcategory, then $\mathscr{C}' \hookrightarrow \mathscr{C}$ is fully faithful if and only if $\mathscr{C}'$ is a full subcategory of $\mathscr{C}$.*

Definition 2.2.8 (Equivalence)**.** *A fully faithful functor $F : \mathscr{C} \to \mathscr{D}$ is called an equivalence if $\forall Y \in \mathbf{Ob}(\mathscr{D})$, there exists $X \in \mathbf{Ob}(\mathscr{C})$ such that $Y \cong FX$.*

In particular, one can say that there is a bijection between isomorphism classes in $\mathscr{C}$ and isomorphism classes in $\mathscr{D}$.

Example 2.2.9.

1. *Let $\mathscr{C}' \subseteq \mathscr{C}$ be a full subcategory. Therefore, $\forall X \in \mathbf{Ob}(\mathscr{C})$, there exists some $X' \in \mathbf{Ob}(\mathscr{C}')$ such that $X' \cong X$. Therefore, $\mathscr{C}' \hookrightarrow \mathscr{C}$ is an equivalence.*

   Notice that suppose $\mathscr{C}' = \mathscr{C} \backslash \{Z\}$ for some object Z. By the argument above, there is some $Y \in \mathbf{Ob}(\mathscr{C}')$ such that $Y \cong Z$. Moreover, for all objects $U \in \mathscr{C}'$, we have the following diagram:

$$\begin{tikzcd}
Y \arrow[rr, bend left, "f"] \arrow[dr] & & Z \arrow[ll, bend left, "g"] \arrow[dl] \\
& U &
\end{tikzcd}$$

   In particular, there is an isomorphism $\mathbf{Mor}(Y, U) \cong \mathbf{Mor}(Z, U)$.

   The idea is that one may delete extra copies of objects by using equivalences.

2. *Denote $\mathbf{Vect}(K)$ as the category of finite-dimensional vector spaces over K and linear maps between these vector spaces. This is equivalent to the category $\mathscr{C}_K$ with objects as non-negative numbers and morphisms $\mathbf{Mor}_{\mathscr{C}_K}(n, m)$ is the set of $m \times n$ matrices with K entries.*

   In particular, a functor $F : \mathscr{C}_K \to \mathbf{Vect}(K)$ would send objects n to K^n and send morphisms A ($m \times n$ matrices) to a linear transformation $A : K^n \to K^m$.

3. *Let $F : \mathscr{C} \to \mathscr{D}$ be a fully faithful functor. Let $D' \subseteq D$ be a subcategory consists of Y in D such that $Y \cong FX$ for some object $X \in \mathscr{C}$.*

   One can induce an equivalence $F'\mathscr{C} \xrightarrow{\sim} \mathscr{D}'$, then $\mathscr{C}$ is equivalent to the full subcategory $\mathscr{D}' \subseteq \mathscr{D}$.

Definition 2.2.10 (Functor Category, Natural Transformation, Natural Isomorphism). *We define a category of functors (between categories $\mathscr{C}$ and $\mathscr{D}$), denoted by* $\mathbf{Func}(\mathscr{C}, \mathscr{D})$, *with functors $F : \mathscr{C} \to \mathscr{D}$ as objects. The morphisms of this category can be defined as follows.*

Let $F, G : \mathscr{C} \to \mathscr{D}$ by functors. A morphism $\alpha : F \to G$ in the functor category is the class of morphisms $FX \xrightarrow{\alpha_X} GX$ in $\mathscr{D}$ for every object X in $\mathscr{C}$ such that for every morphism $f : X \to Y$ in $\mathscr{C}$, the diagram

$$\begin{tikzcd}
FX \arrow[r, "\alpha_X"] \arrow[d, "Ff"] & GX \arrow[d, "Gf"] \\
FY \arrow[r, "\alpha_Y"] & GY
\end{tikzcd}$$

Figure 2.7: Natural Transformation

commutes. Moreover, a morphism $\alpha : F \Rightarrow G$ in the functor category is called a natural transformation.

We say the natural transformation $\alpha : F \to G$ is an isomorphism (or just natural isomorphism) if $\alpha_X : FX \to GX$ is an isomorphism for all objects $X \in \mathscr{C}$.

Remark 2.2.11. *We also denote the functor category* $\mathbf{Func}(\mathscr{C}, \mathscr{D})$ *by $\mathscr{D}^{\mathscr{C}}$.*

Lemma 2.2.12 (Yoneda Lemma). *Consider functor $F : \mathscr{C} \to$* **Set** *and some object $X \in \mathscr{C}$ for $\mathscr{C}$ locally small. Let $R^X : \mathscr{C} \to$* **Set** *maps object Y to $\mathbf{Mor}_{\mathscr{C}}(X, Y)$, and let $\alpha : R^X \to F$ be a natural transformation, where $\alpha_X : R^X X \to FX$. In particular, a map $\varphi : \mathbf{Mor}_{\mathbf{Func}}(R^X, F) \to FX$ is given by $\alpha_X(\mathbf{id}_X) = \varphi(\alpha) \in FX$. The lemma says that φ is a bijection. Moreover, the bijection is natural in both X and F.*

For clarity, we can write bijection $\varphi : \mathbf{Hom}(\mathbf{Hom}(X, -), F) \to FX$.

Proof. See **?**, theorem 2.2.4. □

Remark 2.2.13. *Let $\alpha, \beta : R^X \to F$, if $\alpha_X(\mathbf{id}_X) = \beta_X(\mathbf{id}_X)$, then $\alpha = \beta$.*

For all $f : X \to Y$, there is $\alpha_Y(f) = Ff(\alpha_X(\mathbf{id}_X))$, but $\beta_Y(f) = Ff(\beta_X(\mathbf{id}_X))$, so $\alpha_Y = \beta_Y$ for all objects Y, then $\alpha = \beta$.

$$\begin{tikzcd}
R^X X \arrow[r, "\alpha_X"] \arrow[d, "R^X f"'] & FX \arrow[d, "Ff"] \\
R^X Y \arrow[r, "\alpha_Y"] & FY
\end{tikzcd}$$

Corollary 2.2.14 (Yoneda Embedding).
- *The covariant version of the embedding states that $\mathbf{Mor}_{\mathbf{Func}}(R^X, R^{X'}) \cong R^{X'}(X) = \mathbf{Mor}_{\mathscr{C}}(X', X)$. In particular, $A \xrightarrow{\cong} B$ if and only if $R^B \cong R^A$.*

- *Considering the dual notion, the contravariant version of the embedding states that $\mathbf{Mor}_{\mathbf{Func}}(R_X, R_{X'}) \cong R_{X'}(X) = \mathbf{Mor}_{\mathscr{C}}(X, X')$. In particular, $A \xrightarrow{\cong} B$ if and only if $R_A \cong R_B$.*

Remark 2.2.15. *There is a functor $F : \mathscr{C}^\circ \to \mathbf{Func}(\mathscr{C}, \mathbf{Set})$ that takes $X \mapsto R^X$, where $R^X Y = \mathbf{Mor}(X, Y)$ and $(X' \to X) \mapsto (R^X \to R^{X'})$. Note that F is fully faithful. In particular, $\mathscr{C}^\circ$ is equivalent of a full subcategory of $\mathbf{Func}(\mathscr{C}, \mathbf{Set})$.*

We can also define a functor $G : \mathscr{C} \to \mathbf{Func}(\mathscr{C}^\circ, \mathbf{Set})$ in the dull notion by mapping X to R_X. The functor category $\mathbf{Func}(\mathscr{C}^\circ, \mathbf{Set})$ is called the presheaves on $\mathscr{C}$ in $\mathbf{Set}$.

Remark 2.2.16. *Every morphism between R^X, R^Y is of the form R^f for a unique $f : Y \to X$, defined as $R^f : R^X \to R^Y$ that maps $Z \mapsto R^f(Z) : R^X(Z) \to R^Y(Z)$ and $g \mapsto g \circ f$.*

Every isomorphism $R^X \xrightarrow{\sim} R^Y$ is given by a unique isomorphism $Y \xrightarrow{\sim} X$ up to canonical isomorphism.

Definition 2.2.17 (Representable). *A functor $F : \mathscr{C} \to \mathbf{Set}$ is representable if $F \cong R^X$ for some $X \in \mathscr{C}$. X is uniquely determined by the functor F (if exists) up to isomorphism. (Equivalently, $R^X \xrightarrow{\sim} R^Y$ is given by unique $Y \xrightarrow{\sim} X$, and F is represented by X.)*

Analogously, $G : \mathscr{C}^\circ \to \mathbf{Set}$ is corepresentable if $G \cong R_X$ for some $X \in \mathscr{C}$.

Remark 2.2.18. *In particular, $F : \mathscr{C} \to \mathbf{Set}$ is represented (by $X \in \mathscr{C}$) if there exists an isomorphism $\alpha : F \xrightarrow{\sim} R^X$ such that*

$$\begin{tikzcd}
FY \arrow[r, "\alpha_Y", "\sim"'] \arrow[d, "Fg"] & R^X Y \arrow[r, "\cong"] \arrow[d, "R^X g"] & \mathbf{Mor}_{\mathscr{C}}(X, Y) \arrow[d, "g_*"] \\
FY' \arrow[r, "\alpha_Y", "\sim"'] & R^X Y' \arrow[r, "\cong"] & \mathbf{Mor}_{\mathscr{C}}(X, Y')
\end{tikzcd}$$

commutes.

Example 2.2.19.
1. *Consider a functor $F : \mathscr{C} \to \mathbf{Set}$ defined by $Y \mapsto \{*\}$ and $g \mapsto \mathbf{id}_*$ for all objects Y and morphisms g in $\mathscr{C}$.*

   We want to show that F is representable, so it suffices to find a representation object $X \in \mathscr{C}$. Therefore, for arbitrary object $Y \in \mathscr{C}$, there is an isomorphism

$FY = \{*\} \cong \mathbf{Mor}_{\mathscr{C}}(X, Y)$. However, this means this set of morphism has to be a singleton for arbitrary object Y. In particular, X should be the initial object of $\mathscr{C}$ by definition.

2. *Let X be a set, and consider the group G along with the set of G-actions on X.*

   *Note that if there is a homomorphism $f : G \to G'$, then having G' acts on X would induce an action of G acting on X by the pullback action. (This is induced from **example 1.6.2**.)*

   Define a functor $F : \mathbf{Grp}^\circ \to \mathbf{Set}$ defined by mapping group G to the set of G-actions on X. We want to show that F is representable, so it suffices to check that there is some object O such that $F(G) = \{G\text{– actions on } X\} \xrightarrow{\cong} \mathbf{Hom}(G, O)$. This object O is exactly the symmetric group $\sum(X)$ by interpretation.

   We now check that the diagram commutes.

$$\begin{tikzcd}
F(G) = \{G - \text{actions on } X\} \arrow[r, "\sim"] & \mathbf{Hom}(G, \sum(X)) \\
F(G') = \{G' - \text{actions on } X\} \arrow[r, "\sim"] \arrow[u, "Ff"] & \mathbf{Hom}(G', \sum(X)) \arrow[u, "pullback"']
\end{tikzcd}$$

   Here each action $g \cdot X$ in FG is defined as $f(g) \cdot x$ via the pullback action. For arbitrary $g \in G$, the morphism Ff maps the action $f(g) \cdot x$ to $g \cdot x$ defined as $f(g) \cdot x$. Therefore, there is $\varphi \in \mathbf{Hom}(G, \sum(X))$ given by $\varphi(g)(x) = g \cdot x = f(g) \cdot x$ as defined by the upper routine.

   Taking the bottom routine, there is $\psi \in \mathbf{Hom}(G', \sum(X))$ defined by $\psi(f(g))(x) = f(g) \cdot x$. However, the pullback gives $(\psi \circ f)(g)(x) = \psi(f(g))(x) = f(g) \cdot x = g \cdot x = \varphi(g)(x)$. Therefore, the diagram above commutes by definition.

3. *Consider arbitrary $X, Y \in \mathbf{Ob}(\mathscr{C})$. Define a functor $F : \mathscr{C} \to \mathbf{Set}$ by $Z \mapsto R^X(Z) \times R^Y(Z)$.*

   One can check that this functor is represented by the coproduct object $X * Y \in \mathscr{C}$. In particular, $\mathbf{Mor}(X, Z) \times \mathbf{Mor}(Y, Z) \cong \mathbf{Mor}(X * Y, Z)$, so $R^X \times R^Y \cong R^{X*Y}$.

   Similarly, defining functor $G : \mathscr{C} \to \mathbf{Set}$ by the mapping $Z \mapsto R_X(Z) \times R_Y(Z)$, then the functor is represented by the product object $X \times Y \in \mathscr{C}$. In particular, $\mathbf{Mor}(Z, X) \times \mathbf{Mor}(Z, Y) \cong \mathbf{Mor}(Z, X \times Y)$, so $R_X \times R_Y \cong R_{X \times Y}$.

4. *Take $X \in \mathbf{Ob}(\mathscr{C})$. Define a functor $F : \mathbf{Set}^{\mathscr{C}} \to \mathbf{Set}$ that maps G to GX.*

We want to show that F is a representable functor. Therefore, $F(G) = GX = \mathbf{Mor}_{\mathbf{Functors}}(O, G)$ for some functor $O : \mathscr{C} \to \mathbf{Set}$.

Observe that by Yoneda Lemma, this is exactly the covariant hom functor R^X.

5. *Let X be a set. Define a functor $F : \mathbf{Grp} \to \mathbf{Set}$ by mapping G to the set of maps from X to G (as the underlying set).*

   We want to show that F is a representable functor, then it suffices to show that $\mathbf{Maps}(X, G) = \mathbf{Hom}(O, G)$ for some group O for all groups G. By the universal property of free groups, this group O is exactly the free group of X.

6. *Consider the forgetful functor $F : \mathbf{Grp} \to \mathbf{Set}$ by mapping each group G to its underlying set. We claim that this functor is representable. Indeed, take an object $\mathbb{Z}$, then for all groups G, there is $\underline{G} \cong \mathbf{Hom}(\mathbb{Z}, G)$ by corresponding $g \in G$ to a homomorphism generated by $1 \mapsto g$.*

7. *Take some integer $n > 0$. Define a functor $F : \mathbf{Grp} \to \mathbf{Set}$ by mapping a group G to a set $\{g \in G : g^n = e\}$. To show this functor is representable, it suffices to find an object O such that $\mathbf{Hom}(O, G) \cong \{g \in G : g^n = e\}$. One can take the object as $\mathbb{Z}/n\mathbb{Z}$, then there is a group homomorphism generated by $[1] \to g$ to element g.*

Definition 2.2.20 (Adjoint). *Let $F : \mathscr{C} \to \mathscr{D}$ and $G : \mathscr{D} \to \mathscr{C}$ be functors. Recall that the functor $\mathbf{Mor}(-,-) : \mathscr{C}^\circ \times \mathscr{C} \to \mathbf{Set}$ that maps $(X^\circ, Y) \mapsto \mathbf{Mor}(X, Y)$. We can construct two functors $\mathscr{C}^\circ \times \mathscr{D} \to \mathbf{Set}$:*

- $(X^\circ, Y) \mapsto \mathbf{Mor}_{\mathscr{D}}(FX, Y)$
- $(X^\circ, Y) \mapsto \mathbf{Mor}_{\mathscr{C}}(X, GY)$

We say F is a left adjoint of G (and G is a right adjoint of F) if the two functors above from $\mathscr{C}^\circ \times \mathscr{D} \to \mathbf{Set}$ are isomorphic.

In particular, that means $\mathbf{Mor}_{\mathscr{D}}(FX, Y) \cong \mathbf{Mor}_{\mathscr{C}}(X, GY)$. Moreover, this is natural in both X and Y.

Remark 2.2.21. *Note that if we fix $X \in \mathscr{C}$, then the functor $\mathscr{D} \to \mathbf{Set}$ defined as $Y \mapsto \mathbf{Mor}_{\mathscr{C}}(X, GY)$ is represented by FX.*

Remark 2.2.22. *Adjoint functors (for a given functor) are unique.*

Example 2.2.23. *1. Consider the forgetful functor $K : \mathbf{Grp} \to \mathbf{Set}$ that takes a group G to the underlying set $\underline{G}$. Fix a set $X \in \mathbf{Set}$. We hope to construct a left adjoint functor $F : \mathbf{Set} \to \mathbf{Grp}$. By definition, it suffices to find F such that $\mathbf{Mor}_{\mathbf{Grp}}(FX, G) \cong \mathbf{Mor}_{\mathbf{Set}}(X, K(G) = \underline{G})$. Such F is exactly the free operation that takes a set X to a free group $F(X)$.*

2. *Consider the inclusion functor $K : \mathbf{Ab} \to \mathbf{Grp}$ with some $A \in \mathbf{Ab}$ and some $G \in \mathbf{Grp}$. We hope to find a left adjoint $F : \mathbf{Grp} \to \mathbf{Set}$, so that $\mathbf{Hom}(G, KA = A) = \mathbf{Hom}(FG, A)$. Note that the most convenient construction of functor F is the Abelianization that maps a group G to the Abelian group $G/[G, G]$.*

3. *Consider a functor $G : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ by mapping (X, Y) to $X \times Y$. We hope to construct a left functor $F : \mathscr{C} \to \mathscr{C} \times \mathscr{C}$. Note that we would have $\mathbf{Mor}_{\mathscr{C}}(Z, G(X, Y)) = \mathbf{Mor}_{\mathscr{C}\times\mathscr{C}}(FZ, X \times Y)$. Denote $FZ = (Z_1, Z_2)$, then $\mathbf{Mor}_{\mathscr{C}\times\mathscr{C}}(FZ, X \times Y) = \mathbf{Mor}_{\mathscr{C}}(Z_1, X) \times \mathbf{Mor}_{\mathscr{C}}(Z_2, Y)$, and note that $\mathbf{Mor}_{\mathscr{C}}(Z, G(X, Y)) = \mathbf{Mor}_{\mathscr{C}}(Z, X \times Y) = \mathbf{Mor}_{\mathscr{C}}(Z, X) \times \mathbf{Mor}_{\mathscr{C}}(Z, Y)$. However, this is the case if and only if $Z_1 = Z = Z_2$, which means $F(Z) = (Z_1, Z_2) = (Z, Z)$. This gives us a construction of diagonal functor F.*

Remark 2.2.24. *Let $F : \mathscr{C} \to \mathscr{D}$ be a functor and $(X_i)_{i\in I}$ be a family of objects in $\mathscr{C}$. Let $p_j : \prod_{i\in I} X_i \to x_j$ be the projections for all $j \in I$. Therefore, there is $Fp_j : F(\prod_{i\in I} X_i) \to F(X_j)$. This induces a morphism $\alpha : F(\prod_{i\in I}(X_i) \to \prod_{i\in I} F(X_i)$.*

Definition 2.2.25 (Commutes with products)**.** *We say F commutes with products if α is an isomorphism for all families of objects $(X_i)_{i\in I}$.*

Proposition 2.2.26. *If $F : \mathscr{C} \to \mathscr{D}$ has a left adjoint, then F commutes with products.*

Proof. Take arbitrary $Z \in \mathscr{D}$, and let $G : \mathscr{D} \to \mathscr{C}$ be the left adjoint of F. Therefore,

$$\begin{aligned}
\mathbf{Mor}_{\mathscr{D}}(Z, F(\prod_{i\in I} X_i)) &\cong \mathbf{Mor}_{\mathscr{C}}(GZ, \prod_{i\in I} X_i) \\
&\cong \prod_{i\in I} \mathbf{Mor}_{\mathscr{C}}(GZ, X_i) \\
&\cong \prod_{i\in I} \mathbf{Mor}_{\mathscr{D}}(Z, FX_i) \\
&\cong \mathbf{Mor}_{\mathscr{D}}(Z, \prod_{i\in I} FX_i)
\end{aligned}$$

By the Yoneda Embedding, $F(\prod\limits_{i\in I} X_i) \cong \prod\limits_{i\in I} FX_i$. □

Example 2.2.27. *This proposition gives us a loose criteria to check if a functor has adjoint or not.*

1. *Consider the forgetful functor $F : \mathbf{Grp} \to \mathbf{Set}$. Since this functor has a left adjoint, then F commutes with product, i.e. $F(\prod\limits_{i\in I} G_i) \cong \prod\limits_{i\in I} FG_i$, which means the set product structure is preserved from the group product structure.*

   However, F does not commute with coproduct, which means F does not have a right adjoint.

2. *Consider the inclusion functor $F : \mathbf{Ab} \hookrightarrow \mathbf{Grp}$. Since this functor has a left adjoint, then F commutes with the product. Again, the functor does not commute with coproduct, which means F has no right adjoint.*

Definition 2.2.28 (Inverse Limit)**.** *Consider a family of objects*

$$\begin{tikzcd} A_1 & A_2 \arrow[l, "f_2"'] & A_3 \arrow[l, "f_3"'] & \cdots \arrow[l, "f_4"'] & A_n \arrow[l, "f_n"'] & \cdots \arrow[l, "f_{n+1}"'] \end{tikzcd}$$

We define the inverse limit $\varprojlim(A_i)_{i\in I} = \{(a_i)_{i\in I} \mid f_i(a_i) = a_{i-1}\ \forall i\}$.

Remark 2.2.29. *Note that there is an I-shaped functor $F : I \to \mathscr{C}$ where I is a small category given by*

$$\begin{tikzcd} \cdot_1 & \cdot_2 \arrow[l] & \cdot_3 \cdots \arrow[l] \end{tikzcd}$$

This functor corresponds the diagram above to the family of objects given above.

Since there are morphisms $\varprojlim(A_i)_{i\in I} \to A_j$ for all index j, for arbitrary object $X \in \mathscr{C}$, this induces a family of morphisms $\mathbf{Mor}_{\mathscr{C}}(X, \varprojlim(A_i)_{i\in I}) \to \mathbf{Mor}_{\mathscr{C}}(X, A_j)$ by applying the hom functor.

Therefore, there is a diagram

$$\begin{tikzcd} & & X \arrow[dll] \arrow[dl] \arrow[dr] & & \\ A_1 & A_2 \arrow[l] & \cdots \arrow[l] & A_n \arrow[l] & \cdots \arrow[l] \end{tikzcd}$$

This induces a bijection $\mathbf{Mor}_{\mathscr{C}}(X, \varprojlim(A_i)_{i\in I}) \xrightarrow{\sim} \mathbf{Mor}_{\mathbf{Func}}(\mathbf{id}_X, F)$ from the diagram of I above.

Furthermore, there is

$$\begin{tikzcd}
X \arrow[rr] \arrow[dr] & & \prod\limits_{i\in I} A_i \arrow[dl] \\
& \varprojlim(A_i)_{i\in I} &
\end{tikzcd}$$

In particular, the inverse limit is an object in $\mathscr{C}$.

Definition 2.2.30 (Constant Functor, Constant Natural Transformation)**.** *For any object $c \in \mathscr{C}$ and any category J, the constant functor $c : J \to \mathscr{C}$ sends every object of J to c and every morphism in J to the identity morphism $\mathbf{id}_c$. The constant functors define an embedding $\Delta : \mathscr{C} \to \mathbf{Func}(J, \mathscr{C})$ that sends an object c to the constant functor at c and a morphism $f : c \to c'$ to the constant natural transformation, in which each component is defined to be the morphism f.*

Definition 2.2.31 (Cone)**.** *A cone over a diagram $F : J \to \mathscr{C}$ with summit $c \in \mathscr{C}$ is a natural transformation $\lambda : c \to F$ whose domain is the constant functor at c. The components $(\lambda_j : c \to Fj)_{j\in J}$ of the natural transformation are called the legs of the cone. Explicitly, the data of a cone over $F : J \to \mathscr{C}$ with summit c is a collection of morphisms $\lambda_j : c \to Fj$, indexed by the objects $j \in J$. A family of morphisms $(\lambda_j : c \to Fj)_{j\in J}$ defines a cone over F if and only if, for each morphism $f : j \to k$ in J, the following triangle commutes in $\mathscr{C}$:*

$$\begin{tikzcd}
& c \arrow[dl, "\lambda_j"'] \arrow[dr, "\lambda_k"] & \\
Fj \arrow[rr, "Ff"'] & & Fk
\end{tikzcd}$$

Definition 2.2.32 (Limit, Colimit)**.** *Let I be a small category and $X \in \mathscr{C}$ be an object. Let $c_X : I \to \mathscr{C}$ be the constant functor and $F : I \to \mathscr{C}$ be some other functor. A morphism $X \to Y$ induces a natural transformation $c_X \to c_Y$, so we have a functor $Cone(-, F) : \mathscr{C}^\circ \to$ **Set** given by $X^\circ \to \mathbf{Mor}(c_X, F)$, set of cones over F with summit c. The limit of F is an object $\lim F$ in $\mathscr{C}$ corepresenting this functor, if it exists.*

*The colimit of F is an object colim F representing the functor $\mathscr{C} \to$ **Set** given by $X \to \mathbf{Mor}(F, c_X)$.*

Remark 2.2.33. $\mathbf{Mor}_{\mathscr{C}}(X, \lim F) \cong \mathbf{Mor}_{\mathbf{Func}}(c_X, F) = Cone(-, F)$.

$\mathbf{Mor}_{\mathscr{C}}(colim\ F, X) \cong \mathbf{Mor}_{\mathbf{Func}}(F, c_X) = Cone(F, -)$.

Remark 2.2.34 (Universal Property of Limit)**.** *Let $(\lim F, \lambda : \lim F \to F)$ be the limit over $F : \mathscr{J} \to F$ with object $\lim F$ and cone (natural transformation) $\lambda : \mathbf{id}_{\lim F} \to F$,* *such that for any other object T with cone $\tau : \mathbf{id}_T \to F$, there is a unique morphism $u : T \to \lim F$ such that the following diagram commutes for all $j \in \mathcal{J}$:*

$$\begin{tikzcd}
T \arrow[rr, "\exists ! u"] \arrow[dr, "\tau_j"'] & & \lim F \arrow[dl, "\lambda_j"] \\
& Fj &
\end{tikzcd}$$

Figure 2.8: Universal Property of Limit

Proposition 2.2.35. *A limit is a terminal object in the category of cones over F.*

Example 2.2.36. 1. *Let I be a set (as a category with no morphisms other than the identity morphisms). For the family of objects $(X_i)_{i \in I}$ in $\mathscr{C}$, the diagram F of shape I has $\lim F = \prod\limits_{i \in I} X_i$ and colimit $\coprod\limits_{i \in I} X_i$.*

2. *Consider the following diagram F*

$$\begin{tikzcd}
& B \arrow[d] \\
A \arrow[r] & C
\end{tikzcd}$$

The limit is $\lim F = \{(a, b) : f(b) = g(a)\}$, such that

$$\begin{tikzcd}
X \arrow[dr, dashed, "\exists !"] \arrow[drr, bend left] \arrow[ddr, bend right] & & \\
& \lim F \arrow[r] \arrow[d] & B \arrow[d, "f"] \\
& A \arrow[r, "g"'] & C
\end{tikzcd}$$

Note that this is exactly the pullback, i.e. fiber product.

Moreover, the colimit of the diagram is C, which is the final object of the diagram.

3. *Consider a group G as a category I, then $\mathbf{Ob}(I) = *$, $\mathbf{Mor}(*, *) = G$. Consider a functor $F : I \to \mathbf{Set}$. Note that for a set X, these morphisms $g \in G$ on X are equivalent to the G-actions on X.*

Consider the diagram

$$\begin{tikzcd}
Z \arrow[r, "\alpha"] \arrow[d, "\mathbf{id}"'] & X \arrow[d, "g \in G"] \\
Z \arrow[r, "\alpha"'] & X
\end{tikzcd}$$

Then $g \circ \alpha = \alpha$ for all $g \in G$, which means $\alpha(z) \in X^G$. One can check that the limit is X^G with

$$\begin{tikzcd}
Z \arrow[rr, "\alpha"] \arrow[dr, dashed, "\exists!"'] & & X \\
& \lim F = X^G \arrow[ur] &
\end{tikzcd}$$

On the other hand, the colimit is the set of orbits $X/\sim$ where the equivalence $x \sim gx$ is given by the G-action.

Proposition 2.2.37. *If $F : \mathscr{C} \to \mathscr{D}$ has a left adjoint, then F commutes with limits.*

Proof. See Homework 9, problem 1. □

Definition 2.2.38 (Equalizer)**.** *Let X, Y be sets with*

$$\begin{tikzcd}
X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y
\end{tikzcd}$$

The equalizer $\mathbf{Eq}^{\mathbf{Set}}(f, g) = \{x \in X : f(x) = g(x)\} \subseteq X$ satisfies the universal property

$$\begin{tikzcd}
Z \arrow[d, dashed, "\exists! k"'] \arrow[dr, "h"] & & \\
\mathbf{Eq}^{\mathbf{Set}}(f,g) \arrow[r, hook, "i"'] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y
\end{tikzcd}$$

such that $fi = gi$, and for all sets Z and $h : Z \to X$ such that $fh = gh$, then there is a unique $k : Z \to \mathbf{Eq}^{\mathbf{Set}}(f, g)$ with $i \circ k = h$. In particular, this induces

$$\begin{tikzcd}
\mathbf{Maps}(Z, \mathbf{Eq}^{\mathbf{Set}}(f,g)) \arrow[r, hook] & \mathbf{Maps}(Z, X) \arrow[r, shift left=2, "f"] \arrow[r, shift right=2, "g"'] & \mathbf{Maps}(Z, Y)
\end{tikzcd}$$

*In general, for a category $\mathscr{C}$ and diagram $X \underset{g}{\overset{f}{\rightrightarrows}} Y$, consider the functor $F : \mathscr{C}^\circ \to$ **Set** that sends Z to $\mathbf{Eq}^{\mathbf{Set}}(f_*, g_*)$. The equalizer $\mathbf{Eq}(f, g)$ corepresents F.*

There is the equalizer sequence

$$\begin{tikzcd}
\mathbf{Mor}_{\mathscr{C}}(Z, \mathbf{Eq}(f,g)) \arrow[r, hook] & \mathbf{Mor}_{\mathscr{C}}(Z, X) \arrow[r, shift left=2, "f_*"] \arrow[r, shift right=2, "g_*"'] & \mathbf{Mor}(Z, Y)
\end{tikzcd}$$

In particular, for $Z = \mathbf{Eq}(f,g)$*, there is* $\begin{tikzcd} \mathbf{Eq}(f,g) \arrow[r] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \end{tikzcd}$ *.*

Alternatively, the equalizer is the limit of the diagram of this shape.

In the dual argument, one can define the coequalizer by the following universal property:

$$\begin{tikzcd} X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \arrow[r, "h"] \arrow[dr, "k"] & W \arrow[d, dashed, "\exists! a"] \\ & & Z \end{tikzcd}$$

Similarly, the coequalizer is the colimit of the morphism pair.

Remark 2.2.39. *The equalizer is always monic, and the coequalizer is always epic.*

2.3 Additive and Abelian Category

Definition 2.3.1 (Pre-additive Category)**.** *A category* $\mathscr{C}$ *is pre-additive if* $\forall X, Y \in \mathscr{C}$*, there is a given structure of Abelian group on* $\mathbf{Mor}_{\mathscr{C}}(X,Y)$ *such that the composition is bilinear:*

- $(f+f') \circ g = f \circ g + f' \circ g$ *for* $f, f' \in \mathbf{Mor}_{\mathscr{C}}(X,Y)$ *and* $g \in \mathbf{Mor}_{\mathscr{C}}(W,X)$*.*
- $f \circ (g+g') = f \circ g + f \circ g'$ *for* $f \in \mathbf{Mor}_{\mathscr{C}}(Y,Z)$ *and* $g, g' \in \mathbf{Mor}_{\mathscr{C}}(X,Y)$*.*

In particular, for $X, Y \in \mathbf{Ob}(\mathscr{C})$*,* $0 \in \mathbf{Mor}_{\mathscr{C}}(X,Y)$ *is the zero morphism i.e.* $f \circ 0 = 0$*,* $0 \circ g = 0$*.*

Proposition 2.3.2. *If* $\mathscr{C}$ *is pre-additive, then initial objects and final objects are the same.*

Proof. Let X be a final object with $0_X, 1_X \in \mathbf{Mor}_{\mathscr{C}}(X,X)$, then $0_X = 1_X$, Take $Y \in \mathbf{Ob}(\mathscr{C})$ with $f : X \to Y$, then $f = f \circ 1_X = f \circ 0_X = 0$. Therefore, f has to be unique, which means X is initial. We can use the same trick to show that an initial object is always final. In particular, a zero object is an object that is both initial and terminal. Therefore, object is zero if and only if it is final if and only if it is initial. □

Definition 2.3.3 (Biproduct)**.** *For* $X, Y \in \mathscr{C}$*, a biproduct of* X *and* Y *is* (Z, i_1, i_2, p_1, p_2) *denoted below*

$$\begin{tikzcd}
X \arrow[dr, "i_1"] & & X \\
& Z \arrow[ur, "p_1"] \arrow[dr, "p_2"] & \\
Y \arrow[ur, "i_2"] & & Y
\end{tikzcd}$$

Figure 2.9: Biproduct

such that $p_1 \circ i_1 = \mathbf{id}_X$*,* $p_2 \circ i_2 = \mathbf{id}_Y$*,* $p_1 \circ i_2 = 0$*,* $p_2 \circ i_1 = 0$*, and* $i_1 \circ p_1 + i_2 \circ p_2 = \mathbf{id}_Z$*.*

Proposition 2.3.4. *Let* (Z, i_1, i_2, p_1, p_2) *be a biproduct of* X *and* Y*. Then* $Z = X \times Y$ *with respect to* p_1, p_2*, and* $Z = X * Y$ *with respect to* i_1, i_2*.*

Proof. Consider the following diagram:

$$\begin{tikzcd}
V \arrow[dr, dashed, "\exists ! h"] \arrow[drr, bend left, "f"] \arrow[ddr, bend right, "g"'] & & \\
& Z \arrow[r, "p_1"] \arrow[d, "p_2"] & X \\
& Y &
\end{tikzcd}$$

Define $h = i_1 \circ f + i_2 \circ g : V \to Z$. The two triangles commute:

- $p_1 \circ h = p_1 \circ i_1 \circ f + p_1 \circ i_2 \circ g = \mathbf{id}_X \circ f + 0_X \circ g = f$
- $p_2 \circ h = p_2 \circ i_1 \circ f + p_2 \circ i_2 \circ g = 0_Y \circ f + \mathbf{id}_Y \circ g = g$

Furthermore, for $h, h' : V \to Z$, $p_1 \circ h = f = p_1 \circ h'$ and $p_2 \circ h = g = p_2 \circ h'$, therefore $h' = \mathbf{id}_Z \circ h' = (i_1 \circ p_1 + i_2 \circ p_2) \circ h' = i_1 \circ p_1 \circ h' + i_2 \circ p_2 \circ h' = i_1 \circ f + i_2 \circ g = h$. Therefore, h is unique. In particular, $Z = X \times Y$.

In a similar fashion we can prove that $Z = X * Y$. Therefore, Z as the biproduct $X \oplus Y$ is equivalent to both the product $X \times Y$ and the coproduct $X * Y$. □

Definition 2.3.5 (Additive Category)**.** *A pre-additive category* $\mathscr{C}$ *is additive if* $\mathscr{C}$ *has zero object and finite products.*

Proposition 2.3.6. *In an additive category, every finite product is also a coproduct.*

Proof. Consider arbitrary objects $X, Y \in \mathscr{C}$, with the following diagram:

$$\begin{tikzcd}
 & Y \arrow[d, "i_2=(0,\mathbf{id}_Y)"] & \\
X \arrow[r, "i_1=(\mathbf{id}_X,0)"] & X \times Y \arrow[r, "p_1"] \arrow[d, "p_2"] & X \\
 & Y &
\end{tikzcd}$$

By definition, $p_1 \circ i_1 = \mathbf{id}_X$, $p_2 \circ i_2 = \mathbf{id}_Y$, and $p_2 \circ i_1 = 0$ and $p_1 \circ i_2 = 0$. Therefore, it suffices to check $i_1 \circ p_1 + i_2 \circ p_2 = \mathbf{id}_Z$.

Take $f = i_1 \circ p_1 + i_2 \circ p_2 : X \times Y \to X \times Y$. Then

$$\begin{aligned}
p_1 \circ f &= p_1 \circ (i_1 \circ p_1 + i_2 \circ p_2) \\
&= p_1 \circ i_1 \circ p_1 + p_1 \circ i_2 \circ p_2 \\
&= \mathbf{id}_X \circ p_1 + 0 \circ p_2 \\
&= p_1
\end{aligned}$$

Similarly, $p_2 \circ f = p_2$. Therefore, $(X \times Y, i_1, i_2, p_1, p_2)$ is a biproduct $X \oplus Y$, which is a coproduct. □

Example 2.3.7. *1.* **Ab** *is additive.*

2. A full subcategory of pre-additive category is pre-additive. A full subcategory of additive category that has finite products is additive. In particular, $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ is additive.

*3. Consider the functor $\mathscr{C} \hookrightarrow$ **Functors**$(\mathscr{C}^\circ, \mathbf{Ab})$, then there is a correspondence of additive categories.*

Definition 2.3.8 (Additive Functor)**.** *Let A, B be additive categories. A functor $F : A \to B$ is called additive if $F(g+h) = F(g) + F(h)$ for all $g, h \in \mathbf{Mor}_A(X, Y)$ and $F(0) = 0$.*

Remark 2.3.9. *A key characteristic of an additive functor is that it preserves finite biproduct.*

Consider biproduct $(X \oplus Y, i_1, i_2, p_1, p_2)$ as a biproduct of X and Y. Then $(F(X \oplus Y), F(i_1), F(i_2), F(p_1), F(p_2))$ is a biproduct of $F(X)$ and $F(Y)$. Therefore, $F(X \oplus Y) \cong F(X) \oplus F(Y)$. In this sense, F commutes with products and coproducts as well.

Also, note that since $0_0 = 1_0$, then $F(0_0) = F(1_0)$, i.e. $0_{F(0)} = 1_{F(0)}$ indicates $F(0) = 0$.

Example 2.3.10. 1. *Take $Y \in \mathbf{Ob}(\mathcal{A})$. Consider the Hom functor $R^Y : A \to \mathbf{Ab}$ that sends $X \in \mathcal{A}$ to $\mathbf{Mor}_{\mathcal{A}}(Y, X)$ and morphism f to f_* where $f_*(g) = f \circ g$.*

Observe that R^Y is an additive functor: $R^Y(g_1 + g_2)(f) = (g_1 + g_2)_*(f) = (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f = R^Y(g_1)(f) + R^Y(g_2)(f)$ for all arbitrary morphism f.

2. *Notice that most functors are not additive. For example, consider the constant functor $F : \mathcal{A} \to \mathcal{B}$, where $B \in \mathbf{Ob}(\mathcal{B})$ is fixed, and $F(X) = B$ for all objects $X \in \mathcal{A}$ and $F(f) = \mathbf{id}_B$ for all morphisms f in $\mathcal{A}$.*

Observe that $\mathbf{id}_B = F(f + g) \neq F(f) + F(g) = 2 \cdot \mathbf{id}_B$, which is true whenever $B \neq 0$.

Remark 2.3.11. *In the first example above, the hom functor is mapped into the category of Abelian groups. Here we are claiming that the set of morphisms, $\mathbf{Mor}_A(Y, X)$, has the "structure of a group", but not really an Abelian group. In fact, it is called a "group object", given by the properties of the data in the category. See the following definition. (Also, refer back to the definition of pre-additive category.)*

Definition 2.3.12 (Group Object)**.** *Let A be an additive category (or just a category with terminal object 1 as well as finite products). A group object G in A is an object together with morphisms*

- *$m : G \times G \to G$ (thought of as the "group multiplication")*
- *$e : 1 \to G$ (thought of as the "inclusion of the identity element")*
- *$\mathbf{inv} : G \to G$ (thought of as the "inversion operation")*

such that

- *m is associative, i.e. $m(m \times \mathbf{id}_G) = m(\mathbf{id}_G \times m)$ as morphisms $G \times G \times G \to G$, and where e.g. $m \times \mathbf{id}_G : G \times G \times G \to G \times G$; here we identify $G \times (G \times G)$ in a canonical manner with $(G \times G) \times G$.*
- *e is a two-sided unit of m, i.e. $m(\mathbf{id}_G \times e) = p_1$, where $p_1 : G \times 1 \to G$ is the canonical projection, and $m(e \times \mathbf{id}_G) = p_2$, where $p_2 : 1 \times G \to G$ is the canonical projection.*

- $\mathbf{inv}$ *is a two-sided inverse for* m*, i.e. if* $d : G \to G \times G$ *is the diagonal map, and* $e_G : G \to G$ *is the composition of the unique morphism* $G \to 1$ *(also called the counit) with* e*, then* $m(\mathbf{id}_G \times \mathbf{inv})d = e_G$ *and* $m(\mathbf{inv} \times \mathbf{id}_G)d = e_G$*.*

Example 2.3.13. *Consider the category* **Ab** *with morphism* $f : A \to B$*. There is the following sequence:*

$$\begin{tikzcd} A \arrow[r, two heads] & A/\ker(f) \arrow[r, "\cong"] & \mathbf{im}(f) \arrow[r, hook] & B \end{tikzcd}$$

In general, if $f : A \to B$ *is a morphism in an additive category. Notice that here we define* $\ker(f)$ *to be the equalizer for the morphism pair of* f *and zero morphism from* A *to* B*:*

$$\begin{tikzcd} \ker(f) \arrow[r, "i"] & A \arrow[r, "f"] & B \\ & X \arrow[u] \arrow[ur, "0"'] \arrow[ul, dashed, "\exists!"] & \end{tikzcd}$$

Then there is the following exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \mathbf{Mor}_A(X, \ker(f)) \arrow[r, "i_*"] & \mathbf{Mor}_A(X, A) \arrow[r, "f_*"] & \mathbf{Mor}_A(X, B) \end{tikzcd}$$

Dually, we know the cokernel of f*, i.e.* $B/\mathbf{im}(f)$ *is the coequalizer of* f *and zero morphism from* A *to* B*, described by the following diagram:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "0"'] & B \arrow[r, "j"] \arrow[d] & \mathbf{coker}(f) \arrow[dl, dashed, "\exists!"] \\ & X & \end{tikzcd}$$

with the following exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathbf{Mor}_A(\mathbf{coker}(f), X) \arrow[r, "j^*"] & \mathbf{Mor}_A(B, X) \arrow[r, "f^*"] & \mathbf{Mor}_A(A, X) \end{tikzcd}$$

In particular, notice that $\ker(f_*)$ *is corepresented by* $\ker(f)$*, and* $\ker(f^*)$ *is represented by* $\mathbf{coker}(f)$*, in the following sense: for example, consider* $\ker(f_*)$ *as the set of morphisms* $\mathbf{Mor}_A(X, \ker(f))$*, then this is essentially a functor given by* $\mathbf{Mor}_A(-, \ker(f))$*.*

We sometimes write the coimage of f *as* $\mathbf{coim}(f) = A/\ker(f)$*.*

Definition 2.3.14 (Pre-Abelian Category)**.** *An additive category is pre-Abelian if all kernels and cokernels of morphisms exist.*

Example 2.3.15. *We want to find similar constructions as the one described in the previous example.*

Let $f : A \to B$ be a morphism. By definition, we have that $\mathbf{im}(f) = \ker(j : B \twoheadrightarrow \mathbf{coker}(f))$. Dually, $\mathbf{coim}(f) = \mathbf{coker}(i : \ker(f) \to A)$.

This induces the following universal property in terms of kernel:

$$\begin{tikzcd}
\mathbf{im}(f) \arrow[r, "t"] \arrow[rr, bend left, "0"] & B \arrow[r, "j"] & \mathbf{coker}(f) \\
A \arrow[u, dashed, "\exists!k"] \arrow[ru, "f"] \arrow[rru, "0"'] & &
\end{tikzcd}$$

Moreover, if we add in the object $\ker(f)$, we have the following diagram:

$$\begin{tikzcd}
\mathbf{im}(f) \arrow[r, "t"] \arrow[rr, bend left, "0"] & B \arrow[r, "j"] & \mathbf{coker}(f) \\
A \arrow[u, dashed, "\exists!k"] \arrow[ru, "f"] \arrow[rru, bend right, "0"'] & & \\
\ker(f) \arrow[u, "i"] \arrow[uu, dashed, bend left] \arrow[ruu, bend right, "0"'] \arrow[rruu, bend right, "0"'] & &
\end{tikzcd}$$

By the universal property, the morphism $\ker(f) \to \mathbf{im}(f)$ is zero morphism.

On the other hand, we induce the following diagram from above:

$$\begin{tikzcd}
\ker(f) \arrow[r, "i"] \arrow[rd, "0"'] & A \arrow[r, "l"] \arrow[d, "k"] & \mathbf{coim}(f) \arrow[ld, dashed, "\exists!s"] \\
& \mathbf{im}(f) &
\end{tikzcd}$$

This is true because recall that $\mathbf{coim}(f) = A/\ker(f)$, then by the universal property of the quotinet we have the diagram above.

Therefore, f is essentially a sequence:

$$\begin{tikzcd}
A \arrow[r, "l"] \arrow[rr, bend left, "k"] & \mathbf{coim}(f) \arrow[r, "s"] & \mathbf{im}(f) \arrow[r, "t"] & B
\end{tikzcd}$$

In this case, note that s is not necessary an isomorphism. i.e. The First Isomorphism Theorem may not hold in these cases.

Definition 2.3.16 (Abelian Category)**.** *A pre-Abelian category $\mathcal{A}$ is Abelian if $s : \mathbf{coim}(f) \to \mathbf{im}(f)$ is an isomorphism $\forall f : A \to B$ morphism in $\mathcal{A}$.*

Example 2.3.17.

1. *If $\mathcal{A}$ is Abelian, then $\mathcal{A}^\circ$ is Abelian as well.*
2. ***Ab**, R-mod (left module), Mod-R (right module) are Abelian categories.*
3. *The finite Abelian groups $\mathbf{FinAb} \subseteq \mathbf{Ab}$ is also an Abelian category.*
4. *Category of free Abelian groups (i.e. $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$) is a full subcategory of **Ab**, but it is not even pre-Abelian.*

Example 2.3.18. *The construction of sequences provide us with other good constructions. Consider the following diagram:*

$$\begin{tikzcd}
\ker(f) \arrow[r] \arrow[rr, bend left, "0"] \arrow[d, "\exists!"] & A \arrow[r, "f"] \arrow[d] & B \arrow[d] \\
\ker(f') \arrow[r] & A' \arrow[r, "f'"] & B'
\end{tikzcd}$$

This induces the following diagram:

$$\begin{tikzcd}
\ker(f) \arrow[r] \arrow[rr, bend left, "0"] \arrow[d, "\exists!"'] \arrow[dr, dashed] \arrow[drr, dashed, "0"] & A \arrow[r, "f"] \arrow[d] & B \arrow[d] \\
\ker(f') \arrow[r] & A' \arrow[r, "f'"'] & B'
\end{tikzcd}$$

This induces a functor $\mathbf{Arr}(A) \to A$ by mapping f to $\ker(f)$.

In a dual argument, we have the following diagram with similar properties:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d] & B \arrow[r] \arrow[d] & \mathbf{coker}(f) \arrow[d] \\
A' \arrow[r, "f'"] & B' \arrow[r] & \mathbf{coker}(f')
\end{tikzcd}$$

Remark 2.3.19. *We also want to construct the notion of an exact sequence in these cases. Suppose we have the following diagram where $t : B \to \mathbf{coker}(s) \to C$ satisfies $t \circ s = 0$:*

$$\begin{tikzcd} A \arrow[r, "s"] & B \arrow[r, "t"] \arrow[d] & C \\ & \mathbf{coker}(s) & \end{tikzcd}$$

By rearranging it, we have the following diagram:

$$\begin{tikzcd} A \arrow[r, "s"] \arrow[dr, "0"] & B \arrow[r, "j"] \arrow[d, "t"] & \mathbf{coker}(s) \arrow[dl, dashed] \\ & C & \end{tikzcd}$$

Note that the dashed morphism is induced by the universal property of cokernel (as a coequalizer).

This induces a morphism from $\ker(j)$ *to* $\ker(t)$*. Note that* $\ker(j) = \mathbf{im}(s)$*, then this induces a morphism from* $\mathbf{im}(s)$ *to* $\ker(t)$ *as well.*

Definition 2.3.20 (Exact Sequence)**.** *We say that the first diagram in the previous remark is exact if* $\mathbf{im}(s) \to \ker(t)$ *is an isomorphism (which implies* $t \circ s = 0$*).*

Definition 2.3.21 (Monomorphism, Epimorphism)**.** *Let* $\mathcal{A}$ *be an additive category, then* $f : A \to B$ *is a monomorphism if* $\forall g : X \to A$ *such that* $f \circ g = 0$*, we have* $g = 0$*. In particular, that is equivalent to having the morphism* $f_* : \mathbf{Mor}_{\mathcal{A}}(X, A) \to \mathbf{Mor}_{\mathcal{A}}(X, B)$ *by post-composing* f *as an injection.*

Let $\mathcal{A}$ *be an additive category, then* $f : A \to B$ *is an epimorphism if* $\forall g : B \to X$ *such that* $g \circ f = 0$*, we have* $g = 0$*. In paraticular, that is equivalent to having the morphism* $f^* : \mathbf{Mor}_{\mathcal{A}}(B, X) \to \mathbf{Mor}_{\mathcal{A}}(A, X)$ *by pre-composing* f *as a surjection.*

Proposition 2.3.22. *Let* $\mathcal{A}$ *be a pre-Abelian category, and let* $f : A \to B$ *be a morphism. The following are equivalent:*

1. *The sequence* $0 \to A \xrightarrow{f} B$ *is exact.*

2. $\ker(f) = 0$.

3. f *is a monomorphism.*

Proof. Observe that 1) and 2) are equivalent: $A \xrightarrow{f} B$ is exact if and only if $0 = \mathbf{im}(0) \xrightarrow{\sim} \ker(f)$.

We now show that 2) implies 3). Observe that $0 \to \mathbf{Mor}(X, \ker(f)) \to \mathbf{Mor}(X, A) \xrightarrow{f_*} \mathbf{Mor}(X, B)$ is an exact sequence of Abelian groups. Notice that f_* is an injection, which means f is a monomorphism.

Finally, we show that 3) implies 2). Since f is a monomorphism, then f_* is injective. Again, consider the sequence $0 \to \mathbf{Mor}(X, \ker(f)) \to \mathbf{Mor}(X, A) \xrightarrow{f_*} \mathbf{Mor}(X, B)$. In particular, $\mathbf{Mor}(X, \ker(f)) = 0$ for all $x \in \mathcal{A}$ because $f_* \circ i = f_* \circ 0$. Therefore, $\ker(f)$ is the final object in the category, which means $\ker(f) = 0$. □

Lemma 2.3.23. *Let $\mathcal{A}$ be an Abelian category and $f : A \to B$ is a monomorphism. Then $\mathbf{im}(f) = A$.*

Proof. Note that $\mathbf{im}(f) \cong \mathbf{coim}(f) = \mathbf{coker}(\ker(f) \to A) = A$.

The first relation is by the definition of Abelian category. The second relation is a direct result from the definition. The last result is from the fact that $\ker(f) = 0$. □

Remark 2.3.24. *In an Abelian category, if $f : A \to B$ is a monomorphism, then it is the kernel of $g : B \to \mathbf{coker}(f)$ (canonical surjective homomorphism) and zero morphism. Indeed, $g \circ f = 0 \circ f = 0$ by definition. Also, it satisfies the universal property because suppose there is some $k : C \to B$ satisfies the same property $g \circ k = 0$. By definition, the image of k is contained in the image of f. By the lemma, there is $\mathbf{im}(f) \cong A$. In particular, there is some inverse $f' : B \to A$ of f. Therefore, the image of k is contained in A. Therefore, let $h : C \to A$ be defined as taking c to $f'(k(c)) \in A$. Therefore, we have $f \circ h = ff'k = k$ by definition. Note that since f is a monomorphism, so by left cancellation h is unique.*

$$\begin{tikzcd}
A \arrow[r, "f"] & B \arrow[r, "g"] & B/\mathbf{im}(f) \\
C \arrow[u, dashed, "h"] \arrow[ur, "k"'] & &
\end{tikzcd}$$

In a dual fashion, if $f : A \to B$ is an epimorphism, then it is the cokernel of $g : C \to A$.

Proposition 2.3.25. *In an Abelian category, the sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ is exact if and only if $A = \ker(g)$.*

Proof. Recall that the sequence is exact if and only if f is a monomorphism and $\mathbf{im}(f) \xrightarrow{\sim} \ker(g)$.

By the previous lemma, $\mathbf{im}(f) = A$, so $A \cong \ker(g)$.

On the other hand, if $A = \ker(g)$, then there is the following exact sequence:

$$0 \longrightarrow \mathbf{Mor}(X, A) \xrightarrow{f_*} \mathbf{Mor}(X, B) \xrightarrow{g_*} \mathbf{Mor}(X, C)$$

This means that f is a monomorphism, so $\mathbf{im}(f) = A = \ker(g)$. □

From this point on, we work on Abelian categories unless specified otherwise.

Corollary 2.3.26. *Dually, the sequence* $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *is exact if and only if* $\mathbf{coker}(f) \cong C$.

Proposition 2.3.27. 1. *A sequence* $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ *is exact in* $\mathcal{A}$ *if and only if for all objects* X *in* $\mathcal{A}$*, the sequence*

$$0 \longrightarrow \mathbf{Mor}(X, A) \xrightarrow{f_*} \mathbf{Mor}(X, B) \xrightarrow{g_*} \mathbf{Mor}(X, C)$$

is exact.

2. *A sequence* $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *is exact in* $\mathcal{A}$ *if and only if for all objects* X *in* $\mathcal{A}$*, the sequence*

$$0 \longrightarrow \mathbf{Mor}(C, X) \xrightarrow{g^*} \mathbf{Mor}(B, X) \xrightarrow{f^*} \mathbf{Mor}(A, X)$$

is exact.

Proof. We prove the first statement. Note that the first sequence is exact if and only if $A = \ker(g)$ if and only if the second sequence is exact. □

Definition 2.3.28 (Exact)**.** *The sequence*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is exact if and only if $A = \ker(g)$, $C = coker(f)$ *and* f *is a monomorphism and* g *is an epimorphism.*

Definition 2.3.29 (Left Exact, Right Exact, Exact)**.** *Let* $F : \mathcal{A} \to \mathcal{B}$ *be an additive functor between Abelian categories. We say that* F *is left exact if for every short exact sequence* $0 \to A \to B \to C \to 0$ *in* $\mathcal{A}$*, the sequence* $0 \to F(A) \to F(B) \to F(C)$ *is exact in* $\mathcal{B}$.

We say that F *is right exact if for every short exact sequence* $0 \to A \to B \to C \to 0$ *in* $\mathcal{A}$*, the sequence* $F(A) \to F(B) \to F(C) \to 0$ *is exact in* $\mathcal{B}$.

We say that F *is exact if it is both left exact and right exact.*

Example 2.3.30. 1. *Let* $X \in \mathcal{A}$*. Consider the covariant Hom functor* $R^X : \mathcal{A} \to \mathbf{Ab}$ *by mapping* $Y \mapsto \mathbf{Mor}_{\mathcal{A}}(X, Y)$*, then* R^X *is left exact.*

2. *Let $X \in \mathcal{A}$. Consider the contravariant Hom functor $R_X : \mathcal{A} \to \mathbf{Ab}$ by mapping $Y \mapsto \mathbf{Mor}_{\mathcal{A}}(Y, X)$, then R_X is left exact.*

Theorem 2.3.31 (Mitchell)**.** *Let $\mathcal{A}$ be a small Abelian category. Then there is a ring R and exact fully faithful functor $F : \mathcal{A} \to R$-modules, which is an Abelian category.*

Remark 2.3.32. *Consider the two parallel exact sequences*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "u"] & B \arrow[r, "g"] \arrow[d, "v"] & C \arrow[r] \arrow[d, "w"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0
\end{tikzcd}$$

Then there is a corresponding diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \ker(u) \arrow[r] & \ker(v) \arrow[r] & \ker(w) \arrow[dll, "\delta"] & \\
 & \mathbf{coker}(u) \arrow[r] & \mathbf{coker}(v) \arrow[r] & \mathbf{coker}(w) \arrow[r] & 0
\end{tikzcd}$$

Figure 2.10: Snake Lemma

where $\delta : \ker(w) \to coker(u)$ is defined as the following:

Take arbitrary $c \in \ker(w)$, then c can be lifted back to $b \in B$ with $g(b) = c$. Then there is $b' \in B'$ correspondingly, and there is $a' \in A'$ as the lift for $b' \in B'$. Therefore, define $c \mapsto \delta(c) = a' + \mathbf{im}(u) \in A'/\mathbf{im}(u) = \mathbf{coker}(u)$.

Lemma 2.3.33 (Snake Lemma)**.** *The sequence in **Figure 2.10** is exact.*

Proof. See Homework 9, problem 10. □

Proposition 2.3.34. *Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence in an Abelian category. Then the following are equivalent:*

1. *$\exists h : C \to B$ such that $g \circ h = 1_C$.*

2. *$\exists k : B \to A$ such that $k \circ f = 1_A$.*

3. *There exists a biproduct (B, f, h, k, g).*

4. *The short exact sequence is isomorphic to*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "{(1,0)}"] & A \oplus C \arrow[r, "{(0,1)}"] & C \arrow[r] & 0
\end{tikzcd}$$

Definition 2.3.35 (Split). *We say the short exact sequence is split if (1) - (4) above hold.*

Proof. We first show that (1) ⇒ (2).

Define $k' : 1_B - h \circ g : B \to B$. Then there is the following diagram:

$$\begin{tikzcd}
& & B \arrow[dl, dashed, "k"'] \arrow[d, "k'"] \arrow[dr, dashed, "0"] & & \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, bend left, "g"] & C \arrow[l, bend left, "h"] \arrow[r] & 0
\end{tikzcd}$$

Note that $g \circ k' = g \circ (1_B - h \circ g) = g - g \circ h \circ g = g - g = 0$.

Now $A = \ker(g)$, so there exists a unique $k : B \to A$ such that $f \circ k = k'$. In particular, $f \circ k \circ f = k' \circ f = (1_B - h \circ g) \circ f = f - h \circ g \circ f = f$. Thus, $f \circ (k \circ f - 1_A) = 0$, but f is a monomorphism, so $k \circ f = 1_A$.

Similarly, one can show that (2) ⇒ (1). So (1) and (2) are equivalent.

We now show that (2) implies (3). Note that we can use the fact that (1) and (2) are equivalent. Therefore, we have k and h: $g \circ h = 1_C$, $k \circ f = 1_A$. Then we have the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, bend left, "f"] & B \arrow[l, bend left, "k"] \arrow[r, bend left, "g"] & C \arrow[l, bend left, "h"] \arrow[r] & 0
\end{tikzcd}$$

We know $g \circ f = 0$. Note $f \circ k \circ h = k' \circ h = (1_B - h \circ g) \circ h = h \circ h = 0$. But f is a monomorphism, so $k \circ h = 0$.

Finally, we check $f \circ k + h \circ g = 1_B$. This is obvious as $k' = f \circ k = 1_B - h \circ g$.

We then show that (3) implies (4). One can check that $(k, g) : B \to A \oplus C$ is an isomorphism such that the following diagram commutes.

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, equal] & B \arrow[r, "g"] \arrow[d, "{(k,g)}"] & C \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & A \arrow[r] & A \oplus C \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

Finally, we check that (4) ⇒ (1). This is obvious because we have $(0, 1) : C \to A \oplus C$ as an inverse:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] & A \oplus C \arrow[r, bend left] & C \arrow[l, bend left, "{(0,1)}"] \arrow[r] & 0
\end{tikzcd}$$

□

Now let A be an Abelian category. Recall that for $X \in \mathbf{Ob}(\mathscr{C})$, $R^X : A \to \mathbf{Ab}$ that sends Y to $\mathbf{Mor}_A(X, Y)$ is left exact.

Definition 2.3.36 (Projective)**.** *We say X is projective if R^X is exact.*

Recall that if $0 \to A \to B \to C$ is a short exact sequence, then

$$0 \longrightarrow \mathbf{Mor}(X, A) \xrightarrow{f_*} \mathbf{Mor}(X, B) \xrightarrow{g_*} \mathbf{Mor}(X, C)$$

is exact as well. In particular, denote $B \twoheadrightarrow C$ as an epimorphism.

If X is projective, $\forall k : X \to C$, there exists $h : X \to B$ such that $g \circ h = k$.

Definition 2.3.37 (Lift)**.** *We say such morphism h is a lift:*

$$\begin{tikzcd}
& X \arrow[d, "k"] \arrow[dl, dashed, "h"'] \\
B \arrow[r, two heads] & C
\end{tikzcd}$$

Figure 2.11: Lift

Remark 2.3.38. *Suppose $0 \to A \to B \to C \to 0$ is a short exact sequence where C is projective, then the short exact sequence splits because there is some $h : C \to B$ such that the following diagram commutes:*

$$\begin{tikzcd}
& C \arrow[d, "1_C"] \arrow[dl, dashed] \\
B \arrow[r] & C
\end{tikzcd}$$

Dually, consider $R_X : A^\circ \to \mathbf{Ab}$.

Definition 2.3.39 (Injective)**.** *We say X is injective if R_X is exact.*

Thus, $\forall k : A \to X$, $\exists h : B \to X$ such that $h \circ f = k$. Here we denote $A \hookrightarrow B$ as a monomorphism. Then, we have:

$$\begin{tikzcd}
A \arrow[r, hook, "f"] \arrow[d, "k"'] & B \arrow[dl, dashed, "h"] \\
X &
\end{tikzcd}$$

Remark 2.3.40. *In particular, if $0 \to A \to B \to C \to 0$ is a short exact sequence where A is injective, then the short exact sequence splits.*

3 Ring Theory

3.1 Definition of Rings

Definition 3.1.1 (Ring)**.** *A ring is a set R together with two binary operations $+, \cdot$, such that:*

1. *$(R, +)$ is Abelian group.*

2. *$\exists 1 \in R$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$.*

3. *$(xy)z = x(yz)$ for all $x, y, z \in R$.*

4. *$(x + y)z = xz + yz$, $z(x + y) = zx + zy$ for all $x, y, z \in R$.*

Finally, we say R is a commutative ring if $xy = yx$ for all $x, y \in R$.

Property 3.1.2.

1. *1 is unique.*

2. *$x \cdot 0 = 0 \cdot x = 0$ for all $x \in R$.*

3. *$(-x) \cdot y = -(xy) = x \cdot (-y)$ for all $x, y \in R$.*

Definition 3.1.3 (Invertible)**.** *We say $x \in R$ is invertible if $\exists y \in R$ such that $xy = yx = 1$. We write $y = x^{-1}$, so $(x^{-1})^{-1} = x$ if it is well-defined. Moreover, $(x_1 x_2)^{-1} = x_2^{-1} x_1^{-1}$.*

We denote $R^\times$ as the group of all invertible elements in R.

Remark 3.1.4. *We say $R = \{0\}$ is the zero ring, then $1 = 0$. Moreover, the converse is also true: if $1 = 0 \in R$, then R is the zero ring.*

Definition 3.1.5 (Division Ring)**.** *A ring is called a division ring if $R \neq 0$ and every $x \neq 0$ is invertible, i.e. $R^\times = R \backslash \{0\}$.*

Remark 3.1.6. *A field is a commutative division ring.*

Definition 3.1.7 (Zero Divisor, Integral Domain)**.** *If R is commutative, for $0 \neq x \in R$, x is called a zero divisor if $\exists 0 \neq y \in R$ such that $xy = 0$.*

R is called an integral domain if $R \neq 0$ is a commutative ring and has no zero divisors.

Remark 3.1.8. *Fields are integral domains.*

Example 3.1.9.

1. *$\mathbb{Z}$ is a ring, an integral domain, but not a field. In particular, $\mathbb{Z}^\times = \{\pm 1\}$.*
2. *$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are fields.*
3. *Let R be a ring with integer $n > 0$. $M_n(R)$ is the set of $n \times n$ matrices with entries in R. This is a ring as well. Note that $M_n(R)^\times = \mathbf{GL}_n(R)$, which is the group of all invertible $n \times n$ matrices with R-entries.*
4. *$\mathbb{Z}/n\mathbb{Z}$ is a commutative ring. It is an integral domain if and only if n is a prime integer, if and only if $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. Moreover, $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group of order $\varphi(n)$.*
5. *Let A be an Abelian group. Let R be the set of endomorphisms of A, i.e. the set of homomorphisms from A to itself. Then $R = \mathbf{End}_R(A) = \mathbf{Hom}(A, A)$ is a ring with usual addition and composition as multiplication, called the ring of endomorphisms of an Abelian group A. Note that $\mathbf{End}(A)^\times$ is the group of automorphisms of A, i.e. $\mathbf{Aut}(A)$.*
6. *Let $\mathbb{H}$ be a vector space over $\mathbb{R}$ with basis $\{1, i, j, k\}$. We can then figure out its multiplication table, which gives $k = ij = -ji$. Therefore, $\mathbb{H}$ is a ring, and is a non-commutative division ring in particular. We now look at the norm defined by $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$ with $N(z_1 z_2) = N(z_1)N(z_2)$. In particular, $N(z) > 0$ if $z \neq 0$.*

   Denote $z = a + bi + cj + dk$, then let $\bar{z} = a - bi - cj - dk$, then $z\bar{z} = \bar{z}z = N(z) \cdot 1$. In particular, $z^{-1} = \frac{\bar{z}}{N(z)}$. This give the division ring structure.

   If we do the same thing over $\mathbb{C}$, then $\mathbb{H} \cong M_2(\mathbb{C})$, which is not a division ring.
7. *Let R be a ring. Let $R[t] = \{a_0 + a_1 t + \cdots + a_n t^n : a_i \in R\}$ be a set, then it is a ring in the usual sense. We call it the polynomial ring. Note that R is an integral domain if and only if $R[t]$ is an integral domain. However, $R[t]$ is never a field: t is not invertible.*

One can add more variables into the polynomial ring: $R[s,t] = (R[s])[t]$. Moreover, for any set X of variables, we define $R[x] = \bigcup_{Y \subseteq X} R[Y]$ for finite sets Y.

Moreover, let X be a set, then $R[X]$ is a polynomial ring with commuting variables in X. We also denote $R\langle X\rangle$ as the polynomial ring with non-commuting variables in X, i.e. $R\langle s,t\rangle \neq R[s,t]$. Alternatively, one can say that this is the set of R-linear combinations of monomials (a monomial is a word in X).

Definition 3.1.10 (Ring Homomorphism)**.** *Let R and S be rings. A map $f : R \to S$ is a ring homomorphism if*

- $f(x+y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $f(1_R) = 1_S$

The collection of rings and the homomorphisms between them form a category of rings **Ring**.

Example 3.1.11. *1. $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by taking $x \mapsto [x]_n$ is a ring homomorphism.*

2. $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ are inclusion ring homomorphisms.

3. $0 : R \to S$ sends $1_R \mapsto 0_S$, which means this is not a ring homomorphism if $S \neq 0$.

e.g. $\mathbf{Mor}(\mathbb{Q}, \mathbb{Z}) = \varnothing$.

*4. In **Ring**, the initial object is $\mathbb{Z}$ and the terminal object is 0.*

*5. Consider the forgetful functor F : **Ring** $\to$ **Set**. There is a left adjoint, the free functor G : **Set** $\to$ **Ring** which takes a set X to the ring $\mathbb{Z}\langle X\rangle$. i.e. there is an isomorphism $\mathbf{Hom}_{\mathbf{Set}}(X,R) \cong \mathbf{Hom}_{\mathbf{Ring}}(GX = \mathbb{Z}\langle X\rangle, R)$, where $g(x_1x_2\cdots x_n) = f(x_1)f(x_2)\cdots f(x_n)$. This works because the mapping from $\mathbb{Z}\langle X\rangle$ to R is determined by sending x to τ_x. Note that this is analogous to the operations we have on free groups, so we call $\mathbb{Z}\langle X\rangle$ the free polynomial ring.*

*Now consider the forgetful functor for the category of commutative rings (denoted as **CRing**) F : **CRing** $\to$ **Set**. It also has a left adjoint G : **Set** $\to$ **CRing** taking a set X to $\mathbb{Z}[X]$, i.e. $\mathbf{Hom}_{\mathbf{Set}}(X,R) \cong \mathbf{Hom}_{\mathbf{CRing}}(GX = \mathbb{Z}[X], R)$.*

6. *Consider a "semi-forgetful" functor F : **Ring** → **Grp** that sends $R \mapsto R^X$ and $(f : R \to S) \mapsto (Ff : R^\times \to S^\times)$. There is a left adjoint H : **Grp** → **Ring** that takes a group G to $\mathbb{Z}[G] = \{\sum\limits_{g\in G} n_g \cdot g, n_g \in \mathbb{Z},$ where almost all $n_g = 0\}$. This is sometimes denoted at $\mathbb{Z}^{(G)}$, a set of maps between G and $\mathbb{Z}$ by sending $g \mapsto n_g$. The construction $\mathbb{Z}[G]$ is called the group ring of G.*

   In particular, denote a ring homomorphism $f : \mathbb{Z}[G] \to R$ by sending $G \subseteq \mathbb{Z}[G]^\times \mapsto F(R) = R^\times$. There is $\mathbf{Hom_{Ring}}(\mathbb{Z}[G], R) \xrightarrow{\sim} \mathbf{Hom_{Grp}}(G, R^\times = F(R))$. One can define the inverse of f in the following way. Take $h : G \to R^\times$ a group homomorphism, then $f : \mathbb{Z}[G] \to R$ is defined by $f(\sum\limits_{g\in G} n_g \cdot g) = \sum\limits_{g\in G} n_g \cdot h(g) \in R$.

   Note that if G is an infinite cyclic group, then there is a generator t, now $\mathbb{Z}[G] = \mathbb{Z}[t, t^{-1}]$.

7. *In general, for a ring R and a group G, we can define a group ring $R[G]$ to be $\{\sum\limits_{g\in G} \tau_g \cdot g, \tau_g \in R,$ almost all $\tau_g = 0\}$. This gives the action $(\tau g)(\tau' g') = (\tau\tau')(gg')$, with the action $G \subseteq R[G]^\times$ defined from g to $1 \cdot g$.*

Definition 3.1.12 (Subring). *Let S be a ring. A subset $R \subseteq S$ is a subring if $(R, +)$ is a subgroup of $(S, +)$, and for all $x, y \in R$, there is $xy \in R$, and we have $1_S \in R$.*

Note that this implies $1_R = 1_S$.

Example 3.1.13. 1. *$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are subrings.*

2. *If $f : R \to S$ is a ring homomorphism, then **im**(f) is a subring of S.*

3. *Consider the subset $\left\{ \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \right\} \subseteq M_2(\mathbb{Q})$. Note that the subset is a ring with identity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, but the identity of $M_2(\mathbb{Q})$ is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore, this is not a subring.*

3.2 Ideal

Definition 3.2.1 (Ideal). *Let R be a ring. A subset $I \subseteq R$ is called a left ideal if*

1. *$(I, +)$ is a subgroup of $(R, +)$.*

2. *For all $x \in R$, $y \in I$, we have $xy \in I$.*

Similarly, $I \subseteq R$ is a right adjoint if

1. *$(I,+)$ is a subgroup of $(R,+)$.*
2. *For all $x \in R$, $y \in I$, we have $yx \in I$.*

An ideal, or a two-sided ideal, is both a left ideal and a right ideal.

Example 3.2.2. 1. *There are two trivial ideals: the zero ideal $0 = \{0\} \subseteq R$ and the unit ideal $R \subseteq R$.*

2. *Let $(I_k)_{k\in K}$ be a family of (left) ideals, then their intersection $\bigcap\limits_{k\in K} I_k$ is a (left) ideal.*

3. *Let $a \in R$. $Ra = \{xa : x \in R\}$ is called the left-principal ideal (generated by a).*

   Similarly, $aR = \{ax : x \in R\}$ is the right principal ideal generated by a.

4. *Let $A \subseteq R$ be a subset. Denote $\langle A\rangle_l = \{\sum\limits_{a\in A} x_a \cdot a : x_a \in R,$ almost all x_a are zero$\}$ as the left ideal generated by A. Similarly, there is a right ideal generated by A.*

   Also note that Ra is the left ideal generated by the singleton set $\{a\}$.

5. *Let $I \subseteq R$ be a left ideal (respectively, right ideal, two-sided ideal) such that $I \cap R^\times \neq \varnothing$, then $I = R$ is the unit ideal.*

   Proof. Take $a \in I \cap R^\times$, then $1 = a^{-1} \cdot a \in I$. Therefore, for all $x \in R$, $x = x \cdot 1 \in I$, so $I = R$. □

6. *Let* $I = \left\{ \begin{pmatrix} * & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & 0 & \cdots & 0 \end{pmatrix} \right\} \subseteq M_n(R)$. *Then I is a left ideal but not a right ideal.*

7. *Let $f : R \to S$ be a ring homomorphism, then $\ker(f) \subseteq R$ is a two-sided ideal.*

Definition 3.2.3 (Factor Ring)**.** *Let $I \subseteq R$ be an ideal. Now R/I is a factor group. Define $(x+I)\cdot(y+I) = xy+I$. This is well-defined: if $x_1+I = x_2+I$ and $y_1+I = y_2+I$, then $x_1-x_2 \in I$ and $y_1-y_2 \in I$. Therefore, $x_1y_1-x_2y_2 = (x_1y_1-x_2y_1)+(x_2y_1-x_2y_2) = (x_1-x_2)y_1 + x_2(y_1-y_2) \in I$. We now say R/I is a factor ring where $0_{R/I} = 0 + I = I$ and $1_{R/I} = 1 + I$.*

Remark 3.2.4. *Note that I has to be a two-sided ideal, i.e. the construction does not work on a left ideal or a right ideal.*

Consider the canonical ring homomorphism $\pi : R \twoheadrightarrow R/I$ that sends $a \mapsto a + I$. Then $\ker(\pi) = I$ has to be a two-sided.

The isomorphism theorems in groups also holds in rings, for example:

Theorem 3.2.5 (First Isomorphism Theorem of Rings)**.** *Let $f : R \to S$ be a ring homomorphism. Then $\mathbf{im}(f)$ is a subring of S. Moreover, the map $\bar{f} : R/\ker(f) \to \mathbf{im}(f)$ defined by $\bar{f}(a + \ker(f)) = f(a)$ is a ring isomorphism.*

Example 3.2.6. *Consider the surjective ring homomorphism $f : \mathbb{R}[t] \twoheadrightarrow \mathbb{C}$ that sends $t \mapsto i$, $a + bt \mapsto a + bi$, $1 + t^2 \mapsto 1 + i^2 = 0$, then $\ker(f) = (1 + t^2) \cdot \mathbb{R}[t]$.*

In particular, $\mathbb{C} \cong \mathbb{R}[t]/((1 + t^2) \cdot \mathbb{R}[t])$. This is an algebraic definition of the set of complex numbers.

Let R_i be rings for $i \in I$. Similar as in **Grp**, $\prod\limits_{i\in I} R_i$ is the product in **Ring**.

Suppose R is the product of finitely many rings, i.e. $R = R_1 \times \cdots \times R_n$. Now let $e_i = (0, \cdots, 0, 1, 0, \cdots, 0) \in R$ for $i \in \{1, \cdots, n\}$ where the 1-entry is on the i-th slot. These elements satisfy the following properties:

1. Idempotent: $e_i^2 = e_i$.

2. Orthogonality: $e_i e_j = 0$ for all $i \neq j$.

3. Partition of Unity: $e_1 + \cdots + e_n = 1$.

4. $e_i \in Z(R)$: $e_i x = x e_i$ for all $x \in R$, for all i.

Note that $R_i = Re_i$, so $(xe_i)(ye_i) = xye_i \in R_i$. Therefore, R_i is a ring with identity e_i.

Consider the map $f : R_1 \times \cdots \times R_n \to R$ that sends $(x_1, \cdots, x_n) \mapsto x_1 + \cdots + x_n$. This is a ring homomorphism, where the multiplication comes from

$$\begin{aligned} f(x_1y_1, \cdots, x_ny_n) &= x_1y_1 + \cdots + x_ny_n \\ &= (x_1 + \cdots + x_n)(y_1 + \cdots + y_n) \end{aligned}$$

where $x_iy_j = 0$ for all $i \neq j$.

Moreover, for $x \in R$, $x = \sum\limits_{i \in I} xe_i = f(xe_1, \cdots, xe_n)$. One can check that this is a ring isomorphism.

Example 3.2.7. *Let R be a ring. Take* $S = \left\{ \begin{pmatrix} * & 0 & \cdots & 0 \\ 0 & * & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & * \end{pmatrix} \right\} \subseteq M_n(R)$.

Note that $e_i = e_{i,i}$, i.e .having entry 1 on the (i,i)-th position and 0 elsewhere.

In particular, $Se_i \cong R$, so $S \cong R \times \cdots \times R$, with n copies.

Theorem 3.2.8 (Chinese Remainder)**.** *Let $I_1, \cdots, I_n$ be ideals in a ring R such that $I_k + I_l = R$ for all $k \neq l$. Let $a_1, \cdots, a_n \in R$. Then there is $a \in R$ such that $a \equiv a_i \pmod{I}_i$ for all $i = 1, \cdots, n$, i.e. $a - a_i \in I_i$.*

Proof. This can be done by induction on n.

Note $n = 1$ is obvious. Consider the case where $n = 2$, i.e. we have $a_1 = a_2 \in I = I_1 + I_2$, which means $a_1 - a_2 = x_1 + x_2$ for some $x_i \in I_i$.

Define $a = a_1 - x_1 = a_2 + x_2$, then such a satisfies $a - a_1 = -x_1 \in I_1$ and $a - a_2 = x_2 \in I_2$. Then we are done.

We use this idea in the inductive step, i.e. suppose case $n-1$ is true, show that the case is true at n.

By induction hypothesis, there exists $b \in R$ such that $b \equiv a_i \pmod{I}_i$ for all $i = 1, \cdots, n-1$.

We claim that $(\bigcap\limits_{i \leq i \leq n-1} I_i) + I_n = R$.

By definition, $I_i + I_n = R$ for all $i = 1, \cdots, n-1$. Therefore, $x_i + y_i = 1$ for some $x_i \in I_i$ and $y_i \in I_n$ for $i = 1, \cdots, n-1$.

Now $\prod\limits_{1 \leq i \leq n-1} (x_i + y_i) = 1$. By decomposing, $x_1 x_2 \cdots x_{n-1} \in \bigcap\limits_{1 \leq i \leq n-1} I_i$, and the other terms in the product are monomials that contain at most one $y_i = 1$, which is in I_n.

Now, apply the $n = 2$ case to $\bigcap\limits_{1 \leq i \leq n-1} I_i$ and I_n, and two elements b and a_n. In particular, there exists some $a \in R$ such that $a \equiv b \pmod{()} \bigcap\limits_{1 \leq i \leq n-1} I_i)$ and $a \equiv a_n \pmod{I}_n$.

This concludes the proof because $b \equiv a_i \pmod{I}_i$ for $i = 1, \cdots, n-1$ and so $a \equiv a_i \pmod{I}_i$ for $i = 1, \cdots, n-1$. □

Consider the map $f : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$ that sends $a \mapsto (a + I_1, \cdots, a + I_n)$. The Chinese Remainder Theorem concludes that f is a surjective map. Furthermore, the kernel is $\bigcap\limits_{1\le i\le n} I_i$.

Therefore, $R/\bigcap\limits_{1\le i\le n} I_i \cong R/I_1 \times \cdots \times R/I_n$.

Example 3.2.9. *Consider $R = \mathbb{Z}$, and $I_i = \mathbb{Z}\cdot n_i$ where $i = 1, \cdots, m$ for $\gcd(n_i, n_j) = 1$ for all $i \neq j$, which is equivalent to saying $\mathbb{Z}\cdot n_i + \mathbb{Z}\cdot n_j = \mathbb{Z}$.*

Then $\bigcap\limits_{1\le i\le n} I_i = \mathbb{Z}\cdot(n_1 \cdots n_m)$.

Hence, $\mathbb{Z}/n_1 \cdots n_m\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$.

We saw that the product in rings is the same as that in groups. However, the coproduct is different.

Consider a ring R with generating set $X \subseteq R$. Take $I = \ker(\mathbb{Z}\langle X\rangle \twoheadrightarrow R) \subseteq \mathbb{Z}\langle X\rangle$. Now $R \cong \mathbb{Z}\langle X\rangle / I$.

Suppose we have a family of rings $(R_i)_{i\in I}$ with $R_i \cong \mathbb{Z}\langle x_i\rangle / I_i$ where I_i is the kernel of $\mathbb{Z}\langle x_i\rangle \twoheadrightarrow R_i$, and $X_i \subseteq R_i$ is the generating subset of R_i.

Now $\coprod\limits_{i\in I} R_i = \mathbb{Z}\left\langle \coprod\limits_{i\in I} X_i \right\rangle / \langle\text{ideal generated by } I_i\rangle$. Note $I_j \subseteq \mathbb{Z}\langle X_j\rangle \subseteq \mathbb{Z}\left\langle \coprod\limits_{i\in I} X_i \right\rangle$. This setting has the universal property as follows:

$$\begin{tikzcd}
\mathbb{Z}\langle X_i\rangle \arrow[d, two heads] \arrow[dr, dashed, "f_i"] & \\
R_i \arrow[r] & S
\end{tikzcd}$$

This induces $g : \mathbb{Z}\left\langle \coprod\limits_{i\in I} X_i \right\rangle \to S$, which factors through ring homomorphism.

However, consider the category of commutative rings instead. Then $R_i \cong \mathbb{Z}[X_i]/I_i$ with the same setting as above.

In particular, $\coprod\limits_{i\in I} R_i \cong \mathbb{Z}[\coprod\limits_{i\in I} X_i]/\langle\text{ideal generated by } I_i\rangle$. Here, $R_1 \coprod R_2 = R_1 \otimes_{\mathbb{Z}} R_2$ is the tensor product.

Definition 3.2.10 (Prime Ideal)**.** *Let R be a commutative ring and $P \subseteq R$ be an ideal. P is a prime ideal if $P \neq R$ and whenever $xy \in P$, either $x \in P$ or $y \in P$.*

This is equivalent to having $R/P \neq 0$ and R/P having no zero divisors, which is equivalent to having R/P as an integral domain.

Example 3.2.11. *Take $R = \mathbb{Z}$. Every ideal in $\mathbb{Z}$ is principal.*

Note that $\mathbb{Z}\cdot n$ is prime if and only if $n = 0$ or $n = \pm p$ for some prime p, i.e. prime p multiplied by a unit.

Definition 3.2.12 (Maximal Ideal). *Let R be a commutative ring and ideal $M \subseteq R$.*

We say M is maximal if $M \neq R$ and if $M \subseteq M' \subseteq R$ for some ideal M', then either $M' = M$ or $M' = R$.

Note that M is maximal if and only if ($R/M \neq 0$ and) R/M is a field.

Lemma 3.2.13. *A commutative ring R has exactly two ideals if and only if R is a field.*

Example 3.2.14. *1. The zero ring has no prime or maximal ideals.*

2. Let $R = \mathbb{Z}$ and $n \geq 0$. Then $n\mathbb{Z}$ is prime if and only if $n = 0$ or $n = p$ isprime. It is maximal if and only if $n = p$ is prime.

Theorem 3.2.15 (Correspondence). *Let $I \subseteq R$ be an ideal in a ring. There is a bijective correspondence between ideals of R/I and ideals of R containing I, given by $J \mapsto \bar{J} = J/I$ and $\bar{J} \mapsto J = \pi^{-1}(J)$.*

Remark 3.2.16. *A maximal ideal is always a prime ideal. This is true because a field is always a ring.*

Note that zero rings have no maximal or prime ideals because for the quotient to be a field or domain, it has to be nonzero.

Theorem 3.2.17. *If $R \neq 0$, then there is a maximal ideal in R.*

Proof. The proof involves Zorn's Lemma.

Consider the set $A = \{I \subseteq R \text{ ideal} : I \neq R\}$. As $0 \neq R$, then $0 \in A$ and so $A \neq \varnothing$.

We say $I \leq J$ in $\mathcal{A}$ if $I \subseteq J$. This gives a partial order.

Let B be a chain of ideals included in $\mathcal{A}$. This means for all ideals $I, J \in B$, either $I \leq J$ or $J \leq I$.

Now let $K = \bigcup_{I \in B} I$. Note that K is an ideal in R. Take arbitrary $x, y \in K$. By definition, $x \in I$ and $y \in J$ for some $I, J \in B$. Without loss of generality, $I \leq J$, so $x + y \in J \subseteq K$. Similarly, K is closed under scalar multiplication. Therefore, this verifies K is an ideal.

Note $1 \notin K$ so $K \neq R$. By definition, $K \supseteq I$ for all $I \in B$, i.e. $K \geq I$. Therefore, K is an upper bound of B, and is contained in A.

In particular, every chain in A has an upper bound in A. (Since A is not empty.)

By Zorn's Lemma, A has a maximal element M: if $M \subseteq I$, $I \in A$, then $M = I$.

Therefore, M is a maximal ideal in R. □

Corollary 3.2.18. *Every non-zero commutative ring has a prime ideal.*

Definition 3.2.19 (Principal Ideal Ring)**.** *Take $a \in R$, then aR is a principal ideal. We say R is a principal ideal ring if every ideal in R is principal.*

Example 3.2.20.

1. *Fields.*
2. $\mathbb{Z} \supseteq n\mathbb{Z}$.
3. $\mathbb{Z}/n\mathbb{Z}$ *is a principal ideal ring* $\forall n > 0$.

Note that the first two examples are also PID (principal ideal domain).

Definition 3.2.21 (Euclidean Ring)**.** *A Euclidean ring is a commutative ring R together with a function $\varphi : R\backslash\{0\} \to \mathbb{Z}^{\geq 0}$ such that for every $a, b \in R$, $a \neq 0$, there exists $q, r \in R$ such that $b = aq + r$, with either $r = 0$ or $\varphi(r) < \varphi(a)$.*

Theorem 3.2.22. *Every Euclidean ring is a principal ideal ring.*

Proof. Take ideal $I \subseteq R$ with $I \neq 0$. Now $\min\limits_{0 \neq a \in I} \varphi(a) = n \geq 0$.

Take $a \in I$ such that $\varphi(a) = n$. We claim that $I = aR$. Obviously $aR \subseteq I$.

Take $b \in I$. Then there exists q, r such that $b = aq+r$, where $r = 0$ or $\varphi(r) < \varphi(a) = n$.

If $\varphi(r) < \varphi(a)$, then $r = b - aq \in I$ as $b \in I$ and $aq \in I$, then $\varphi(r) < n$, contradiction. Hence, $b = aq$. It follows that $I = aR$, which concludes the proof. □

Example 3.2.23.

1. $R = \mathbb{Z}$ *with* $\varphi(a) = |a|$.
2. *Let F be a field, take $R = F[t]$ with $\varphi(f) = \deg(f) \geq 0$.*

   This setting is required for us to divide the highest coefficient, e.g. consider dividing $t + 1$ by $2t$ in $\mathbb{Q}[t]$, which is just $t + 1 = 2t \cdot \frac{1}{2} + 1$.

   Note that $R = \mathbb{Z}[t]$ is not a Euclidean ring, nor a PID: $2R+tR \subsetneq R$ is not principal.
3. *Let $R = \mathbb{Z}[i] = \{a+bi, a, b \in \mathbb{Z}\}$ as the Gaussian integers, with $\varphi(a+bi) = a^2+b^2 = |a + bi|^2$, i.e. $\varphi(z) = |z|^2$.*

   Why does this φ works?

   Consider $u, v \in R$ with $v \neq 0$. We can write $\frac{u}{v} = \alpha + \beta i \in \mathbb{C}$ where $\alpha, \beta \in \mathbb{R}$.

   We can find $a, b \in \mathbb{Z}$ such that $|\alpha - a| \leq \frac{1}{2}$, $|\beta - b| \leq \frac{1}{2}$. i.e. give an approximation by integers.

   Then $\frac{u}{v} = q + s$ where $q = a + bi$ and $s = (\alpha - a) + (\beta - b)i$, one can see that $|s|^2 < 1$.

Now $u = vq + vs$, but as $u, vq \in R$, we have $r = vs \in R$. This is the remainder.

In particular, $\varphi(r) = |r|^2 = |v|^2 \cdot |s|^2 < |v|^2 = \varphi(v)$.

Therefore, the ring of Gaussian integers a Euclidean ring, and also a PID.

3.3 Factorization in Commutative Rings

Definition 3.3.1 (divisibility)**.** *Let R be a commutative ring. Let $a, b \in R$ with $a \neq 0$.*

We say b is divisible by a if $\exists c \in R$ such that $b = ac$.

Alternatively, we say a divides b, i.e. $a \mid b$, which is true if and only if $aR \supseteq bR$.

Remark 3.3.2. *Note that $a \neq 0$ if and only if $aR \neq 0$, and $a \in R^\times$ if and only if $aR = R$.*

Property 3.3.3.

1. *If $a \mid b_1$ and $a \mid b_2$, then $a \mid b_1 + b_2$.*

2. *If $a \mid b$, then $a \mid bc$ for all c. In particular, $a \mid 0$.*

3. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

4. *We say $a \sim b$ are associates if $a \mid b$ and $b \mid a$, i.e. $aR = bR$.*

   Let R be an integral domain, then $a \sim b$ if and only if there exists $u \in R^\times$ such that $b = au$.

   Indeed, if $a \mid b$ and $b \mid a$, then $b = ax = bxy$ for some y such that $a = by$. In particular, $1 = xy$ for $x \in R^\times$.

   Note that if $a \sim a'$ and $b \sim b'$, then $a \mid b$ if and only if $a' \mid b'$. In particular, $aR = a'R$ and $bR = b'R$.

Definition 3.3.4 (Prime)**.** *Let R be a domain, we say $p \in R$ is prime if*

1. *$p \neq 0$,*

2. *$p \notin R^\times$,*

3. *if $p \mid ab$ in R, then $p \mid a$ or $p \mid b$.*

Remark 3.3.5. *Note that $p \in R$ is prime if and only if pR is a prime ideal. (i.e. $pR \neq 0, R$, and $ab \in pR$ indicates $a \in pR$ or $b \in pR$.)*

Definition 3.3.6 (Irreducible)**.** *We say $c \in R$ is irreducible if*

1. $c \neq 0$,

2. $c \notin R^\times$,

3. *if* $c = ab$, *then either* $a \in R^\times$ *or* $b \in R^\times$.

Claim 3.3.7. $c \in R$ *is irreducible if and only if* cR *is maximal in the set of principal ideals* $aR \neq R$.

Proof. Suppose c is irreducible, then $cR \neq R$. Suppose $cR \subseteq aR$, then $c = ab$ for some b, then either $a \in R^\times$ or $b \in R^\times$.

If $a \in R^\times$, then $aR = R$. If $b \in R^\times$, then $cR = aR$.

Suppose cR is maximal in the set of principal ideals $aR \neq R$. Then $c = ab$ for $a \notin R^\times$. In particular, $cR \subseteq aR \neq R$, but cR is maximal, so $cR = aR$. In particular, $c = ab$ for some $b \in R^\times$. □

Example 3.3.8. $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

Claim 3.3.9. 2 *is irreducible but not prime in* R.

Proof. Note that $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$, but $2 \nmid 1 \pm \sqrt{-5}$: $\frac{1}{2} \pm \frac{1}{2}\sqrt{-5} \notin R$. Therefore, 2 is not prime.

Take $2 = xy$ for $x, y \in R$. Then $|x|^2, |y|^2 \in \mathbb{Z}$. Note $4 = |2|^2 = |x|^2|y|^2$. Without loss of generality, say $|x|^2 \leq 2$, then as $x = a + b\sqrt{-5}$ for $a, b \in \mathbb{Z}$, $|x|^2 = a^2 + 5b^2 \leq 2$.

Therefore, $b = 0$ and $|a| \leq 1$, which means $a = \pm 1$. In particular, $x = \pm 1 \in R^\times$. Therefore, 2 is irreducible by definition. □

Proposition 3.3.10. *Every prime element is irreducible.*

Proof. Let p be a prime. Suppose $p = ab$. Since $p \mid ab$, then $p \mid a$ or $p \mid b$. Suppose $a = pq$. Then $p = pqb$, which means $1 = qb$. Hence, $b \in R^\times$, which means p is irreducible. □

Proposition 3.3.11. *If* R *is a PID, then primes and irreducibles are the same.*

Proof. We only have to show that every irreducible element is prime.

Let $c \in R$ be irreducible. Then cR is maximal among principal ideals that are distinct from R. But every ideal in R is principal. Therefore, cR is a maximal ideal, which is a prime ideal, and so c is prime. □

Definition 3.3.12 (Unique Factorization). *Let R be a domain. We say the factorization in R is unique if $c_1c_2\cdots c_n = d_1d_2\cdots d_m$ where c_i and d_j are irreducible, $n = m$, and there exists $\sigma \in S_n$ such that $d_i \sim c_{\sigma(i)}$ for all $i = 1, \cdots, n$.*

Definition 3.3.13 (Admit Factorization). *We say R admits factorization if every $0 \neq x \in R$ with $x \notin R^\times$ can be written as $x = c_1c_2\cdots c_n$ for c_i irreducible.*

Definition 3.3.14 (Unique Factorization Domain). *R is a unique factorization domain if R admits a unique factorization. We say R is a UFD.*

Theorem 3.3.15. *In a UFD, the primes and irreducibles are the same.*

Proof. Again, it suffices to show that every irreducible is a prime element. Take $c \in R$ to be irreducible. Consider $c \mid ab$. We can write $ab = cx$ for some $x \in R$.

Let $a = c_1\cdots c_n$ and $b = d_1\cdots d_m$ and $x = e_1\cdots e_k$. Then $c_1\cdots c_n d_1\cdots d_m = ce_1\cdots e_k$. Note that $c \sim c_i$ or $c \sim d_j$ for some i, j.

If $c \sim c_i \mid a$, then $c \mid a$. Similarly, if $c \sim d_j \mid b$, then $c \mid b$. Therefore, c is a prime. □

Theorem 3.3.16. *Let R admit factorization and suppose the primes and the irreducibles are the same. Then R is a UFD.*

Proof. Consider $c_1\cdots c_n = d_1\cdots d_m$ where c_i, d_j are irreducibles. Then $c_n \mid d_1\cdots d_m$ where c_n is prime. In particular, $c_n \mid d_j$ for some j. We write $c_nx = d_j$ irreducible. But as c_n is irreducible, it is not a unit, then $x \in R^\times$, which means $d_j \sim c_n$. Without loss of generality, say $j = m$. Then $c_1\cdots c_{n-1} = (xd_1)d_2\cdots d_{m-1}$.

By performing induction on n, we conclude the proof. □

Proposition 3.3.17. *Let R be a commutative ring. The following are equivalent:*

1. *Every ideal of R is finitely generated.*
2. *For every chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$, there exists some $n > 0$ such that $I_n = I_{n+1} = \cdots$.*
3. *Every nonempty set of ideals contains a maximal ideal.*

Proof. We first show that 1) implies 2).

Take a chain of ideals $I_1 \subseteq I_2 \cdots \subseteq I_n \subseteq \cdots$. Take $\mathfrak{J} = \bigcup\limits_{k\geq 1} I_k$, so $\mathfrak{J} = \sum\limits_{i=1}^{n} a_iR$, where $a_i \in \mathfrak{J}$.

In particular, there exists $n > 0$ such that $a_1, \cdots, a_m \in I_n \subseteq \mathfrak{J}$. In particular, this indicates that $I_n = \mathfrak{J}$. However, $I_n \subseteq I_{n+i} \subseteq \mathfrak{J}$. Therefore, $I_{n+i} = \mathfrak{J}$ for all $i \geq 0$.

We now show that 2) implies 3).

Take a non-empty set of ideals. Take an ideal I_1 in the set. If it is maximal, we are done. If it is not maximal, it is contained in some ideal $I_2 \supsetneq I_1$. We perform this algorithm repeatedly. By property in 2), this algorithm has to stop at some point and we obtain a maximal element.

Finally, we show that 3) implies 1).

Let $I \subseteq R$ be an ideal. Consider the set $\{\mathfrak{J} \subseteq R \text{ ideals } : \mathfrak{J} \subseteq I, \mathfrak{J} \text{ is finitely generated}\}$. This set is not empty because it contains 0. In particular, it contains a maximal $\mathfrak{J}$. We claim that $I = \mathfrak{J}$. Suppose not, then $\mathfrak{J} \subsetneq I$, so there exists $a \in I \backslash \mathfrak{J}$. Then $\mathfrak{J} \subsetneq \mathfrak{J} + aR \subseteq I$, where $\mathfrak{J} + aR$ is still finitely generated because $\mathfrak{J}$ is finitely generated. But then $\mathfrak{J} + aR$ is in the set. This contradicts the fact that $\mathfrak{J}$ is maximal, contradiction. □

Definition 3.3.18. *If all the above properties hold, we say R is a Noetherian ring.*

Corollary 3.3.19. *Every PID is Noetherian.*

Theorem 3.3.20. *Noetherian domain admits factorization.*

Proof. Let $S = \{aR : a \text{ cannot be factored into product of irreducible elements}\}$. We want to show that $S = \varnothing$. Suppose not, then there is a maximal ideal $aR \in S$.

If a is irreducible, then it factors itself, so a is not irreducible, then $a = xy$ for some $x, y \notin R^\times$. In particular, $x \mid a$ and $y \mid a$. Therefore, $aR \subsetneq xR \notin S$ and $aR \subsetneq yR \notin S$. Therefore, x, y are products of irreducibles. Then so is a, contradiction. □

Proposition 3.3.21. *Let R be a domain, then*

1. *If primes and irreducibles are the same in R, then R has unique factorization.*
2. *If R is Noetherian and primes and irreducibles are the same in R, then R is a UFD.*

Corollary 3.3.22. *Every PID is a UFD.*

Proof. It suffices to show that if R is a PID, then irreducibles in R are prime. Let $p \in R$ be irreducible and suppose that $p \mid ab$ but $p \nmid a$. Pick $d \in R$ so that $pR + aR = dR$. Then $d \mid p$ and $d \mid a$, but $p \nmid a$, so since p is irreducible, d is a unit, without loss of generality we can say $d = 1$. There exists $r, s \in R$ so that $pr + as = 1$. Then $prb + abs = b$, and the left hand side is divisible by p, so $p \mid b$ as desired. □

Remark 3.3.23. *If $I, J \subseteq R$ are ideals, then $IJ = \{\sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J\}$ is an ideal in R.*

In particular, if we multiply two principal ideals, we have $(aR)(bR) = abR$, which is still a principal ideal.

Similarly, if $a = c_1 \cdots c_n$, then $aR = (c_1 R) \cdots (c_n R)$. This gives the existence of factorization of ideals. Also, if $(c_1 R) \cdots (c_n R) = (d_1 R) \cdots (d_m R)$ where c_i, d_j are irreducible, then the factorization is unique: $n = m$ and there exists $\sigma \in S_n$ such that $d_i \sim c_{\sigma(n)}$ for all $i = 1, \cdots, n$. Therefore, $d_i R = c_{\sigma(i)R}$.

Remark 3.3.24 (Greatest Common Divisor, Least Common Multiple)**.** *Let R be a UFD, and let $a_1, \cdots, a_n \in R$ be nonzero. Then there exists $c_1, \cdots, c_n$ distinct and irreducible, such that $a_i = u_i \prod_{j=1}^{m} c_j^{k_{ij}}$ where $k_{ij} \in \mathbb{Z}^{\geq 0}$ and $u_i \in R^{\times}$ (i.e. up to units).*

Correspondingly, $a_i R = \prod_{j=1}^{m} (c_j R)^{k_{ij}}$. This decomposition is unique up to permutation of terms.

One can define greatest common divisors as ideals: $\gcd(a_i R) = \prod_{j=1}^{m} (c_j R)^{s_j}$ *where* $s_j = \min_i(k_{ij})$*. Similarly, we can define the least common multiples as ideals* $\mathbf{lcm}(a_i R) = \prod_{j=1}^{m} (c_j R)^{s_j}$ *where* $s_j = \max_i(k_{ij})$*.*

We say ideals $a_1 R, \cdots, a_n R$ are relatively prime (or correspondingly, $a_1, \cdots, a_n$ are relatively prime) if $\gcd(a_i R) = R$*.*

Note that greatest common divisors are up to units.

Proposition 3.3.25. *In a UFD, the greatest common divisor of a finite set of elements exists.*

Proof. Let $a_1, \cdots, a_n$ be elements in a UFD R, and let $p_1, \cdots, p_r$ be all of the primes appearing in the factorizations of $a_1, \cdots, a_n$ (up to units), so that for each i, $a_i = p_1^{e_{i,1}} \cdots p_r^{e_{i,r}}$ for $e_{ij} \geq 0$.

The greatest common divisor is then $\gcd(a_1, \cdots, a_n) = p_1^{\min(e_{1,1}, \cdots, e_{n,1})} \cdots p_r^{\min(e_{1,r}, \cdots, e_{n,r})}$.

□

3.4 Factorization in Polynomial Rings

Let R be a commutative ring, then $R[x]$ is a polynomial ring. (Inductively, one can construct $R[x_1, \cdots, x_n]$.)

We aim to prove the following theorem in this section:

Theorem 3.4.1. *If R is a UFD, then so is $R[x]$.*

Note that if $R \to S$ is a ring homomorphism, then there is an induced homomorphism $R[x] \to S[x]$. Therefore, this is a functor from the category of rings to itself.

If R is a domain, then $\deg(fg) = \deg(f) + \deg(g)$, and $\deg(0) = -\infty$ by convention. Therefore, $\deg(f) \leq 0$ if and only if $f \in R$. Note that $R \subseteq R[x]$ is a subring.

Consider the invertible elements in this ring. Let $f \in R[x]^\times$, then if $fg = 1$, we have $\deg(f) + \deg(g) = 0$. Therefore, since the degrees are non-negative, we have $\deg(f) = 0$ and $\deg(g) = 0$, so $f, g \in R^\times$. Hence, $R[x]^\times = R^\times$.

We say that a polynomial $f \in R[x]$ is irreducible if f is an irreducible element of $R[x]$.

Definition 3.4.2 (Quotient Field). *Let R be a domain, we define a field F containing R as the set of all pairs (a, b) where $a, b \in R$, $b \neq 0$. This is called the quotient field of R.*

We introduce the equivalence relation where $(a, b) \sim (a', b')$ if $ab' = a'b$.

We define $\frac{a}{b}$ is defined as the equivalence class of (a, b). Then F is the set of equivalence classes $\{\frac{a}{b} : a, b \in R, b \neq 0\}$. The operations defined on the set are

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

Note that F is a field because for $a, b \neq 0$, $(\frac{a}{b})^{-1} = \frac{b}{a}$.

In particular, there is an embedding $R \hookrightarrow F$ given by $a \mapsto \frac{a}{1}$. This homomorphism is unique.

Remark 3.4.3. *Define $F(x) = \{\frac{f}{g} : f, g \in R[x], g \neq 0\}$ to be a ring. This is called the quotient field of $R[x]$ (and of $F[x]$), also called the field of rational functions. Note that $F(x)$ contains both $R[x]$ and $F[x]$.*

Also note that $F[x]$ is not a field, but it is a PID (and a UFD).

Example 3.4.4. *$\mathbb{Z}[x]$ is not a PID: $\langle 2, x\rangle$ is not principal.*

Similarly, $F[x, y]$ is not a PID because $\langle x\rangle$ is not principal.

Remark 3.4.5. *Note that irreducible element are with respect to fields.*

1. *Consider $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, where $2x$ is an element of both rings. However, $2x$ is not irreducible in $\mathbb{Z}[x]$, but it is irreducible in $\mathbb{Q}[x]$ (because 2 is a unit in $\mathbb{Q}[x]$.*

2. *Consider $\mathbb{R}[x] \subseteq \mathbb{C}[x]$, where $x^2 + 1$ is is an irreducible element of $\mathbb{R}[x]$, but not an irreducible element in $\mathbb{C}[x]$.*

Definition 3.4.6 (Content, Primitive)**.** *Let R be a UFD. Take $f = a_n x^n + \cdots + a_1 x + a_0$ for $a_i \in R$. Suppose $f \neq 0$.*

We say that $\gcd(a_0 R, \cdots, a_n R) = bR$ is the content of f, denoted $C(f)$.

We say that f is primitive if $C(f) = R$.

Remark 3.4.7. *If f is monic, then f is primitive.*

Also,

1. *$C(af) = aC(f)$ where $0 \neq a \in R$ and $0 \neq f \in R[x]$.*

2. *$C(f) = R$ for monic f.*

Lemma 3.4.8 (Gauss)**.** *If R is a UFD, and $f, g \in R[x]$ are primitive, then fg is primitive.*

Proof. Take $c \in R$ prime, then $cR \subseteq R$ is prime.

Let $\bar{R} = R/cR$ be a domain. Then there is a surjection

$$R[x] \to \bar{R}[x]$$
$$R \mapsto \bar{R}$$
$$f \mapsto \bar{f}$$

Since f, g are primitive, then $\bar{f}, \bar{g} \neq 0$ in $\bar{R}[x]$ domain. Then $\bar{f}\bar{g} \neq 0$, which means $\bar{f g} \neq 0$. Therefore, not all coefficients of fg are divisible by c. In particular, fg is primitive by definition. □

Corollary 3.4.9. $C(fg) = C(f) \cdot C(g)$.

Proof. Let $f = a \cdot f'$ for f' primitive, then $C(f) = aR$.

Similarly, let $g = b \cdot g'$ for g' primitive, then $C(g) = bR$.

Then $fg = abf'g'$, where $f'g'$ is primitive by Gauss Lemma.

In particular, $C(fg) = abC(f'g') = abR = (aR) \cdot (bR) = C(f) \cdot C(g)$. □

Lemma 3.4.10. *Let f and g be non-zero polynomials in $R[x]$, and f is primitive. If $f \mid g$ in $F[x]$, then $f \mid g$ in $R[x]$.*

Remark 3.4.11. *Note that the primitive condition is necessary: note $2x \mid x^2 \in \mathbb{Q}[x]$, but $2x \nmid x^2 \in \mathbb{Z}[x]$.*

Proof. Let $g = fh$ where $h \in F[x]$, then there exists $0 \neq a \in R$ such that $a \cdot h \in R[x]$. Therefore, $ag = f \cdot (ah) \in R[x]$.

In particular, $aC(g) = C(ag) = C(f) \cdot C(ah) = C(ah)$. Note that all coefficients of ah are divisible by a.

Therefore, $h \in R[x]$. By definition, $f \mid g$ in $R[x]$. □

Lemma 3.4.12. *Let F be a UFD and let $f \in R[x]$ be irreducible, then f is primitive.*

Proof. Let dR to be the content of f for some $d \in R$. Then $f = d \cdot f'$ for some $f' \in R[x]$. Since f is irreducible, either d or f' has to be a unit. Obviously d has to be the unit. In particular, $C(f) = dR = R$. □

Lemma 3.4.13. *Let R be a UFD and let $f \in R[x]$ be a nonconstant polynomial. Then f is irreducible in $R[x]$ if and only if f is primitive and irreducible in $F[x]$.*

Proof. ($\Longrightarrow$): Since f is irreducible over UFD, then it is primitive. Suppose, towards contradiction that f is not irreducible in $F[x]$, then $f = gh$ for some non-constant polynomials $g, h \in F[x]$, i.e. $\deg(g), \deg(h) < \deg(f)$.

Note that g, h may have denominators in their coefficients. We multiply a certain constant a, then $ag \in R[x]$. We then divide the greatest common divisor b of the coefficients of ag, then we get a primitive polynomial $\frac{a}{b}g$. In particular, $g = \alpha \cdot g'$ and similarly $h = \beta \cdot h'$ for $\alpha, \beta \in F^\times$ and $g', h' \in R[x]$ are primitive.

Hence, $f = \alpha\beta g'h'$. So $g'h' \mid f$ in $F[x]$. Note that $g'h'$ is primitive by Gauss' Lemma, then by lemma, $gh \mid f$ in $R[x]$. In particular, $\alpha\beta \in R$.

We now write $f = (\alpha\beta g') \cdot h'$ in $R[x]$, which is a non-trivial factorization. This is a contradiction to the fact that f is irreducible in $R[x]$.

($\Longleftarrow$): We write $f = gh$ in $R[x]$. We need to show that g or h is an irreducible constant in R. Note that this is also a factorization in $F[x]$. Since f is irreducible in $F[x]$, then either g or h is a scalar in F. Since $F \cap R[x] = R$, we see that $g \in R$ or $h \in R$. Without loss of generality, say $g \in R$. Now $R = C(f) = g \cdot C(h)$, and so $g \in R^\times$. □

Theorem 3.4.14. *If R is a UFD, then so is $R[x]$.*

Proof. We prove by induction on the degree of polynomials that we can factor polynomial $f \in R[x]$.

When $\deg(f) = 0$, then $f \in R$ is a nonzero scalar. In particular, f factors as a product of irreducibles because R is a UFD. Note that irreducibles in R are still irreducible in $R[x]$.

Now assume that the case for $\deg(f) = n \geq 0$ is true. We want to prove the case for $\deg(f) = n + 1 > 0$. Then $f = a \cdot f'$ for some $a \in R$ such that f' is primitive. Recall that $aR = C(f)$, then it is possible to assume f is primitive.

Assume $f = gh$ in $R[x]$ is a non-trivial factorization, i.e. g, h are not irreducible constants. Note that then g, h should not be constants, i.e. $g, h \notin R$: for example if $g \in R$, then $R = C(f) = g \cdot C(h)$, but that means $g \in R^\times$, contradiction.

Therefore, $\deg(g), \deg(h) < \deg(f)$. By induction, we can factor both g and h. Therefore, we can factor f.

This proves the existence of factorization. We now show its uniqueness. It suffices to show that every irreducible in $R[x]$ is a prime.

Take an irreducible polynomial f in $R[x]$. Suppose $f \mid gh$ where $g, h \in R[x] \subseteq F[x]$, where F is the quotient field of R. Therefore, $f \mid gh$ in $F[x]$ (which is a UFD and a PID). Now, since f is irreducible in $R[x]$, then that means f is irreducible in $F[x]$. Then f is prime in $F[x]$. Therefore, $f \mid g$ or $f \mid h$ in $F[x]$. Without loss of generality say $f \mid g$. Recall that f is primitive, then $f \mid g$ in $R[x]$ by the lemma. □

Remark 3.4.15 (Factorization and Irreducible Elements in Polynomial Ring)**.** *Take $f \in R[x]$. If f is a constant, then $f \in R$ which is a UFD, so assume f is not a constant. Then we can factor f in $F[x]$. We write it as a product of irreducibles in $F[x]$: $f = g_1 g_2 \cdots g_k$. There exists $\alpha_i \in F^\times$ such that $g_i = \alpha_i \cdot h_i$, where $h_i \in R[x]$ is primitive. Observe that h_i is still irreducible, then by lemma, h_i is irreducible in $R[x]$. Now $f = (\alpha_1 \cdots \alpha_k) h_1 h_2 \cdots h_k$ is a factorization in $F[x]$, but since h_i are primitive, so $h_1 h_2 \cdots h_k$ is primitive, then $h_1 h_2 \cdots h_k \mid f$ in $R[x]$, and thus $\alpha_1 \cdots \alpha_k \in R$. Therefore, $f = (\alpha_1 \cdots \alpha_k) h_1 h_2 \cdots h_k$ is a factorization in $R[x]$.*

The irreducibles in $R[x]$ are:

1. *Irreducibles in R, i.e. constants.*

2. *Nonconstant primitive $h \in R[x]$ that are irreducible in $F[x]$.*

Theorem 3.4.16 (Eisenstein Criterion)**.** *Let R be a UFD with quotient field F. Let $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$. Let $p \in R$ be an irreducible element such that*

1. $p \nmid a_n$*,*

2. $p \mid a_i$ *for* $i = 1, 2, \cdots, n-1$*,*

3. $p^2 \nmid a_0$*.*

Then f *is irreducible in* $F[x]$*.*

Proof. We first reduce the case to primitive polynomials. In general, we write $f = af'$ where $f' \in R[x]$ is primitive and $aR = C(f)$. Let $f = a_n x^n + \cdots + a_1 x + a_0$ for $a_i \in R$. We write $f' = b_n x^n + \cdots + b_1 x + b_0$ where $a_i = a \cdot b_i$. We claim that f' satisfies the same condition as f.

Note that

1. Since $p \nmid a_n$, then $p \nmid b_n$. Also, $p \nmid a$.

2. Since $p \mid a_i$ and $p \nmid a$, we have $p \mid b_i$.

3. Since $p^2 \nmid a_0$, then $p^2 \nmid b_0$.

Therefore, it suffices to prove the case for f': $f \sim f'$ in $F[x]$. Hence, assume that f is primitive from the start is reasonable.

Take $\bar{R} = R/pR$, then $\bar{R}$ is a domain because pR is prime. We have a homomorphism $R[x] \to \bar{R}[x]$ by sending $g \mapsto \bar{g}$. Then note that $\bar{f} = \bar{a_n} x^n$ where $\bar{a_n} \neq \bar{0}$. We need the primitive polynomial f to be irreducible in $F[x]$, which holds if and only if f is irreducible in $R[x]$.

Let $f = gh$ in $R[x]$. If we can show that $g \in R$, then $R = C(f) = gC(h)$ and so $g \in R^\times$.

Assume $\deg(g), \deg(h) < n$. Now $\bar{f} = \bar{g}\bar{h}$ in domain $R[x] \subseteq K[x]$, where $\bar{f} = \bar{a_n} x^n$ and K is the quotient field of $\bar{R}$. Therefore, we can write $\bar{g} = \alpha x^k$, $\bar{h} = \beta x^m$ for $\alpha, \beta \in K$, and $k, m > 0$.

In particular, as $\bar{g} \in \bar{R}[x]$, we know $\alpha \in \bar{R}$. Similarly, $\beta \in \bar{R}$. Note that $\bar{g}$ and $\bar{h}$ both have zero constant terms. Therefore, constant term of g and h are divisible by p. In particular, the constant term a_0 of $f = gh$ is divisible by p^2. However, $p^2 \nmid a_0$, contradiction. □

Example 3.4.17. *Let* $p \in \mathbb{Z}$ *be prime. Consider the polynomial* $f = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$*. We claim that* f *is irreducible in* $\mathbb{Q}[x]$*.*

Take $y = x - 1$, i.e. $x = y + 1$, then $f = \frac{x^p - 1}{x-1} = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{p-2} y + \binom{p}{p-1}$. Note that the Eisenstein Criterion holds. Therefore, the claim is true indeed.

Remark 3.4.18 (Classification of Domains)**.** *The class of Euclidean Domains is contained in the class of Principal Ideal Domains (e.g. $\mathbb{Z}$), which is contained in the class of Unique Factorization Domains (e.g. $\mathbb{Z}[x], \mathbb{Z}[x_1, \cdots, x_n, \cdots]$). There is also a class of Noetherian domains, which also contains the class of Principal Ideal Domains. Note that $\mathbb{Z}[x]$ is both a UFD and a Noethereian Domain, $\mathbb{Z}[\sqrt{-5}]$ is a Noetherian domain but not a UFD, and $\mathbb{Z}[x_1, \cdots, x_n, \cdots]$ is UFD but not Noetherian.*

4 Module Theory

4.1 Definition

Definition 4.1.1 (Module)**.** *Let R be a ring (associative, with unit, but not necessarily commutative). A left R-module is an Abelian group M (written additively) together with an operation $R \times M \to M$ by sending $(a, m) \mapsto a \cdot m$ (scalar multiplication) such that*

1. $a(m_1 + m_2) = am_1 + am_2$,

2. $(a + b)m = am + bm$,

3. $(ab)m = a(bm)$,

4. $1 \cdot m = m$.

Similarly, one can define a right R-module as an Abelian group M (written additively) together with an operation $M \times R \to M$ by sending $(m, a) \mapsto m \cdot a$ (scalar multiplication) such that

1. $(m_1 + m_2)a = m_1a + m_2a$,

2. $m(a + b) = ma + mb$,

3. $m(ab) = (ma)n$,

4. $m \cdot 1 = m$.

Remark 4.1.2. *If R is commutative, then every left R-module can be viewed as a right R-module via $ma = am$.*

Without loss of generality, we work on the left R-modules from this point on.

Property 4.1.3. 1. *$a \cdot 0 = 0$ in M.*

2. $0 \cdot m = 0$.

3. $(-a)m = -(am) = a \cdot (-m)$.

Example 4.1.4. *1. Let R be a field F, then R-modules are equivalent to vector spaces over F. Therefore, the notion of a module over ring is the generalization of the notion of a vector space over field.*

2. Let $R = \mathbb{Z}$. We have the operation $\cdot$ given by $1 \cdot m = m$, $2 \cdot m = (1+1) \cdot m = m+m$, and so on. Therefore, the operation is uniquely determined. In this case, the R-modules are equivalent to Abelian groups.

3. Left (Right) ideals in R are left (right) R-modules. R is both a left and right R-module.

4. Let $f : R \to S$ be a ring homomorphism. Let M be a (left) S-module, then M has a structure of a (left) R-module via $a \cdot m = f(a) \cdot m)$ for $a \in R$ and $m \in M$. This is a pullback action with respect to f.

5. Let A be an Abelian group (written additively). Then $\mathbf{End}(A)$ is the ring of endomorphisms of A is given by the set of homomorphisms $\{f : A \to A\}$. Then A is a left $\mathbf{End}(A)$-module, with the operation defined by $f \cdot m = f(m)$ for $f \in \mathbf{End}(A)$ and $m \in A$.

There is more analogies with group theory. Let M be a left R-module. For $a \in R$, one can define left multiplication $l_a : M \to M$ by $l_a(m) = am$. We can then rewrite the module axioms:

a) $l_a(m_1 + m_2) = l_a(m_1) + l_a(m_2)$, which implies $l_a \in \mathbf{End}(M)$.

b) $l_{a+b}(m) = l_a(m) + l_b(m)$, so the map $\varphi : R \to \mathbf{End}(M)$ where $a \mapsto l_a$ given by the previous axiom is additive.

c) $l_{ab}(m) = l_a(l_b(m)) = (l_a \circ l_b)(m)$. This says that φ is also multiplicative.

d) $l_1(m) = m$, i.e. $l_1 = \mathbf{id}$. This implies φ sends 1 to 1.

The properties above, shows that $\varphi : R \to \mathbf{End}(M)$ is a ring homomorphism. Therefore, every left module give raises to a ring homomorphism.

We can reverse the construction as well. Suppose we have an Abelian group A (written additively), and $\varphi : R \to \mathbf{End}(M)$ is a ring homomorphism. Then we make A a left R-module by writing $a \cdot m = \varphi(a)(m)$.

This induces a bijective correspondence between $\mathbf{Hom_{Ring}}(R, \mathbf{End}(A))$ *and left* R*-module structure on* A.

Note that for a ring homomorphism from R *to* $\mathbf{End}(A)$*, a left* R*-module structure on* A *is given by the pullback of the canonical left* $\mathbf{End}(A)$*-module structure on* A.

Definition 4.1.5 (Homomorphism)**.** *Let* R *be a ring and* M, N *be (left)* R*-modules. A map* $g : M \to N$ *is an* R*-module homomorphism if*

1. g *is a homomorphism of Abelian groups, and*
2. $g(am) = a \cdot g(m)$ *for all* $a \in R$ *and* $m \in M$.

The set of such morphisms is denoted as $\mathbf{Hom}_R(M, N)$*, and is an Abelian group.*

If we want to introduce categories, we consider R-**Mod** as a category of R-modules, with objects as left R-modules and morphisms as R-module homomorphisms.

Similarly, we can define a category of right R-modules, denoted **Mod-**R.

We will see that R-**Mod** (and similarly, **Mod-**R) is Abelian.

Property 4.1.6.

1. *If* R *is commutative, then* $\mathbf{R - Mod} \cong \mathbf{Mod - R}$ *because left and right modules then coincide.*
2. *If* $f : R \to S$ *is a ring homomorphism, then the pullback operation allows us to consider every* S*-module as* R*-module. We have a functor* $f^(: \mathbf{S - Mod} \to \mathbf{R - Mod}$ *given by* $N \mapsto f^*N$*, where the operation on* f^*N *is defined by* $r \cdot_R n = f(r) \cdot_S n$.

Definition 4.1.7 (Submodule)**.** *If* M *is a left* R*-module, then a subgroup* $N \subseteq M$ *is called a submodule if* $aN \subseteq N$ *for all* $a \in R$*. Submodules are modules.*

Remark 4.1.8. *Let* $\{N_i\}_{i \in I}$ *be a family of submodules of* M*, then* $\bigcap\limits_{i \in I} N_i \subseteq N$ *is a submodule. However, the union of modules is generally not a module. Instead, we consider the sum of submodules, which is the smallest module containing the family:* $\sum\limits_{i \in I} N_i = \{\sum\limits_{i \in I} n_i, \text{ almost all } n_i = 0\} \subseteq M$.

We can then define a factor module. If $N \subseteq M$ *is a submodule, then* $M/N = \{m + N, m \in M\}$ *is a factor module defined by* $a \cdot (m + N) = am + N$.

Let $g : M \to N$ *be a* R*-module homomorphism. Then* $\ker(g) \subseteq M$ *and* $\mathbf{im}(g) \subseteq N$ *are submodules as well.*

The three isomorphism theorems are also true in this setting, for example:

Theorem 4.1.9 (First Isomorphism Theorem). *Let $g : M \to N$ be an R-module homomorphism. Then $> / \ker(g) \to \mathbf{im}(g)$ defined by $m + \ker(g) \mapsto g(m)$*

Remark 4.1.10. *The direct sums and products of this category is essentially the same as those in* $\mathbf{Ab}$*, because the forgetful functor (forgets the scalar product structure) i : $\mathbf{R} - \mathbf{Mod} \to \mathbf{Ab}$ has a left adjoint $A \mapsto R \otimes_{\mathbb{Z}} A$.*

Then let $(M_i)_{i\in I}$ be R-modules, we have $\prod\limits_{i\in I} M_i = \{(m_i)_{i\in I}, m_i \in M_i\}$ and $\coprod\limits_{i\in I} M_i = \{(m_i)_{i\in I}, m_i \in M_i,$ almost all $m_i = 0\}$.

*Therefore, R-**Mod** (and similarly, **Mod**-R) should be Abelian.*

We can construct exact sequences and split exact sequences in this category.

Definition 4.1.11 (Finitely Generated). *We say a (left) R-module is finitely generated if $\exists m_1, m_2, \cdots, m_n \in M$ such that every $M \in M$ can be written as a linear combination $m = \sum\limits_{1\leq i\leq n} a_i m_i$ for $a_i \in R$.*

4.2 Free Module

We first define the notion of a basis for modules.

Definition 4.2.1 (Basis, Free). *Let M be a (left) R-module. A subset $S \subseteq M$ is called a basis for M if every $m \in M$ can be written as $m = \sum\limits_{s\in S} a_s \cdot s$ for unique $a_s \in R$ where almost all coefficients are zero.*

We say that M is free if M has a basis.

The "almost" condition is here to justify the summation operation.

Example 4.2.2. *For $R = \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ is not free, because $\tilde{1} = 3 \cdot \tilde{1}$.*

Every vector space is free (even if it is infinite-dimensional).

In cases of vector spaces, the cardinality of a basis is well-defined. However, for R-modules, different bases may have different cardinalities.

Remark 4.2.3 (Structure on a Free Module). *Let I be a set, then the coproduct $\coprod\limits_{i\in I} R = R^{(I)} = \{(a_i)_{i\in I},$ almost all a_i are $0\}$. This module is free. For $i \in I$, let $e_i = (a_j)_{j\in I}$ where $a_j = 1$ if $j = i$ and $a)j = 0$ if $j \neq i$. Now, $\{e_i\}_{i\in I}$ forms a basis for $R^{(I)}$. Therefore, $R^{(I)}$ is free.*

In fact, if I has finitely many elements, we write $R^{(I)}$ as R^n, where n is the cardinality of I.

Suppose M is a free R-module, and we choose a basis $(m_i)_{i\in I}$ for M. We then have a well-defined homomorphism $R^{(I)} \to M$ by sending $(a_i)_{i\in I} \mapsto \sum\limits_{i\in I} a_i m_i$. This is an isomorphism of modules because in definition, every element in M can be written uniquely as this sum.

As a conclusion, every free (left) R-module is isomorphic to $R^{(I)}$ for some set I.

Given by this setting, we can construct homomorphisms from free modules to other modules. If we have M be a (left) R-module, we can construct a set map $f : I \to M$, and then there is a R-module homomorphism given by $\bar{f} : R^{(I)} \to M$ such that $\bar{f}(ax) = \sum\limits_{x\in I} a_x \cdot f(x)$.

Conversely, if we think of $I \subseteq R^{(I)}$, then an R-module homomorphism $g : R^{(I)} \to M$ can be restricted to a set map $f = g\mid_I\colon I \to M$.

This induces an isomorphism $\mathbf{Mor}_{\mathbf{Set}}(I, M) \cong \mathbf{Hom}_R(R^{(I)}, M)$. This is essentially an adjunction between R-***Mod*** and $\mathbf{Set}$. The left adjoint is the forgetful functor that forgets the module structure, and the right adjoint takes a set X to the free module $R^{(X)}$. This is a typically forgetful-free adjunction.

In particular, the hom functor from free module is exact, so if F is a free left R-module, then there is an isomorphism $F \cong R^{(X)}$ for some set X.

This gives an exact functor $\mathbf{R} - \mathbf{Mod} \to \mathbf{Ab}$ that takes a module M to $\mathbf{Hom}_R(F, M)$. In general, the functor is left exact; the exactness comes from the free module. The right exactness comes from

$$\begin{tikzcd}
 & & & F = R^{(X)} \arrow[dl, dashed] \arrow[d] & \\
0 \arrow[r] & P \arrow[r] & M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

The morphism from F to M is generated by the adjunction: it is the same as having

$$\begin{tikzcd}
 & X \arrow[dl, dashed, "h"'] \arrow[d, "f"] \\
M \arrow[r, two heads] & N
\end{tikzcd}$$

where the map h is induced by the surjection: for $x \in X$, we have $f(x) \in N$, and there is $h(x) \in M$ that is a preimage of the map from M to N.

This shows that the functor is exact.

Another nice feature of free module is that every module is a factor module of a free module.

Let M be a (left) R-module, and pick a set of generators $X \subseteq M$. There is an embedding $X \hookrightarrow M$ gives an R-module homomorphism $g : R^{(X)} \twoheadrightarrow M$ by adjunction, which is a surjection because X is a generating set. Therefore, $M \cong R^{(X)}/\ker(g)$.

If M is finitely generated, then X can be chosen finite. Therefore, $M \cong R^n/(\cdots)$.

Finally, we can think about how to view morphisms between free modules. In general, if we have a collection of modules $(M_i)_{i\in I}$ and $(N_j)_{j\in J}$, then we can form a direct sum of M_i's and a direct product of N_j's, and we have

$$\mathbf{Hom}_R(\coprod_i M_i, \prod_j N_j) = \prod_{i,j} \mathbf{Hom}_R(M_i, N_j).$$

In particular, if I and J are finite, the product and the coproduct are the same. In that case, $\mathbf{Hom}_R(M_i, N_j)$ are just matrices formed by homomorphisms. Composition then corresponds to multiplication of matrices. In particular, if we take for all $M_i = R = N_j$ realized as a left module over itself, then we have $\mathbf{Hom}_R(R^n, R^m)$, which is just the set of $m \times n$ matrices. (Note that $\mathbf{Hom}_R(R, M) = M$.)

4.3 Projective and Injective Module

Since modules form an Abelian category, and we have defined projective and injective objects, then we don't actually have to define them again. Recall that

Definition 4.3.1 (Projective)**.** *A (left) R-module P is projective if the functor $\mathbf{Hom}_R(P, -)$ is exact.*

Remark 4.3.2. *Free modules are projective.*

Theorem 4.3.3. *A (left) R-module P is projective if and only if P is a direct summand of a free module, i.e. there exists a (left) R-module P' such that $P \otimes P'$ is free.*

Proof. Suppose P is projective, then the sequence

$$0 \longrightarrow N \longrightarrow F \longrightarrow P \longrightarrow 0$$

where F is free. This sequence is split because P is projective, and so $F \cong P \oplus N$.

Suppose $P \oplus N$ is free, then $\mathbf{Hom}_R(P, -)$ is corepresented by R_p. Then the represented functor $R_{P\oplus N} = R_P \oplus R_N$ and is exact because $P \oplus N$ is free. It is an easy exercise to see that R_P is exact, and so P is projective. □

Example 4.3.4. *1. Take $R = R_1 \times R_2$ as a product of two rings. Take $P_1 = R_1 \times 0$ and $P_2 = 0 \times R_2$ as two ideals in R, and therefore are modules. In particular, we have $R \cong P_1 \oplus P_2$. Therefore, P_1 and P_2 are projectives.*

2. Let F be a field. Take $R = F[x, y, z]/(x^2 + y^2 + z^2 - 1) \cdot R[x, y, z]$. This is the ring of polynomial functions on the sphere S given by $x^2 + y^2 + z^2 = 1$.

Recall that the homomorphism between free modules is given by matrices. Therefore, consider the homomorphism $f : R^3 \to R$ given by $\begin{pmatrix} x & y & z \end{pmatrix}$, sending $\begin{pmatrix} f \\ g \\ h \end{pmatrix}$ to $xf + yg + zh$. This map is surjective, and is therefore split. We can define the retraction $R \to R^3$ given by the matrix $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$. Let P be the kernel of f. Then we have a split short exact sequence given by

$$0 \longrightarrow P \longrightarrow R^3 \xrightarrow{f} R \longrightarrow 0$$

Therefore, $R^3 \cong P \oplus R$. Hence, the kernel P is projective and stably free. In particular, $P = \{ \begin{pmatrix} f \\ g \\ h \end{pmatrix} : xf + yg + zh = 0\}$. This is the R-module of tangent fields on a sphere.

Now, suppose P is free, i.e. $P \cong R^2$, then P has a basis given by $t, s \in P$. So for all $u \in S$, $\{t(u), s(u)\}$ forms a basis for the tangent plane at u. In particular, $t(u) \neq 0$ for all $u \in S$.

From the point of view of topology, if the base field $F = \mathbb{R}$, then there is no everywhere nonzero tangent vector field on the sphere.

Therefore, P is not free. (If the base field is $\mathbb{C}$, then it is free. Note that P is not free over any subfield of $\mathbb{R}$.)

Definition 4.3.5 (Injective)**.** *A (left) module Q is injective if $\mathbf{Hom}_R(-, Q)$ is exact. In particular, this means every exact sequence*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d] & S \arrow[r] \arrow[dl, dashed] & T \arrow[r] & 0 \\
& Q & & &
\end{tikzcd}$$

Remark 4.3.6. *One would expect a similar description of injective modules to exist, but there is none. The reason is that the dual category of the category of R-modules is not equivalent to a category of modules over some ring.*

Remark 4.3.7. *Now consider a special case of exact sequence*

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[d] & R \arrow[r] \arrow[dl, dashed] & R/I \arrow[r] & 0 \\
 & Q & & &
\end{tikzcd}$$

where I is a left ideal in the ring R. Suppose Q is injective, then we have a natural extension as above. However, every homomorphism from R to Q is of the form that sends a to aq for a fixed element $q \in Q$.

Therefore, for every $f : I \to Q$, there exists $q \in Q$ such that $f(x) = xq$ for every $x \in I$.

This induces the following theorem, as a replacement of correspondence theorem of injective modules.

Theorem 4.3.8 (Baer)**.** *Let Q be a (left) R-module such that for every left ideal $I \subseteq R$ and every R-module homomorphism $f : I \to Q$, there is an element $q \in Q$ with $f(x) = xq$ for all $x \in I$, then Q is injective.*

Proof. Suppose we have a submodule $M \subseteq S$ for a module S, and we have a homomorphism g from S to Q. We use Zorn's Lemma and consider all possible extensions: the set of pairs $(\bar{M}, \bar{g})$, where $M \subseteq \bar{M} \subseteq S$ and $\bar{g} : \bar{M} \to Q$ is given by $\bar{g} \mid_M = g$. It is non-empty because we can take $\bar{M} = M$.

Observe the ordering on the set, given by $(M_1, g_1) \leq (M_2, g_2)$ when $M_1 \subseteq M_2$ and $g_1 = g_2 \mid_{M_1}$. By Zorn's Lemma, there exists a maximal pair (M', g').

The claim is that $M' = S$. If this is true, then g' is the extension we want, and we are done.

Suppose not, then there is $s \in S \backslash M'$. Define $M'' = M' + Rs \supsetneq M'$. We need to find $g'' : M'' \to Q$ extending g'.

Take $I = \{x \in R : xs \in M'\} \subseteq R$ to be a left ideal in R. There is now a map $f : I \to Q$ given by $x \mapsto g'(xs) \in Q$. This is well-defined because $xs \in M'$.

By assumption, there exists $q \in Q$ such that $f(x) = xq$. Then set$g''(m' + xs) = q'(m'') + xq$, and so $(M'', q'') \supsetneq (M', q')$. This gives a contradiction. □

We now want to characterize the injective modules in principal ideal domains.

Definition 4.3.9 (Divisible)**.** *Let R be a PID, and let M be a R-module. We say M is divisible if $\forall m \in M$, $\forall 0 \neq a \in R$, there exists $m' \in M$ such that $m = a \cdot m'$.*

Proposition 4.3.10. *A module M over a PID R is injective if and only if M is divisible.*

Proof. Take arbitrary ideal I in R and take arbitrary homomorphism $f : I \to M$. Then M is injective if and only if the following extension exists.

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[d, "f"] & R \arrow[dl, dashed] \\
& M &
\end{tikzcd}$$

Since R is a PID, then $I = aR$ for some $a \in R$. Obviously we can assume $a \neq 0$. Now the map f is easy to understand becasue I is free with a basis given by $\{a\}$. Now, the mapping is determined by the single element a. Consider $f(a) = m \in M$ to be arbitrary, then we have $f(ax) = am$.

Now, this f can be extended: there exists $m' \in M$ such that $f(y) = ym'$. By substituting $y = a$, we have $m = f(a) = am'$. Therefore, $m = am'$, which implies divisibility.

Similarly we can see the other side of the proof. □

Example 4.3.11. *Consider $R = \mathbb{Z}$ (which is a PID), then $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Q}$ are divisible.*

In general, the factor module of divisible module is divisible, and so the factor module of injective module is injective.

Recall that every module is a factor module of a free module, and so it is a factor module of a projective module. The dual statement is that every module is a submodule of an injective module.

Proposition 4.3.12. *Consider $R = \mathbb{Z}$. Every group is a subgroup of a divisible group, so every group is a subgroup of an injective $\mathbb{Z}$-module.*

Proof. Take M to be an Abelian group. We want to embed M into a divisible group. We write M as a factor module of a free module, then $M = \mathbb{Z}^{(X)}/N$ for a set X, and $N \subseteq \mathbb{Z}^{(X)}$ is a submodule.

Therefore, we have $N \subseteq \mathbb{Z}^{(X)} \hookrightarrow \mathbb{Q}^{(X)}$, where $\mathbb{Q}^{(X)}$ is divisible. By factoring out the N, we have $M = \mathbb{Z}^{(X)}/N \hookrightarrow \mathbb{Q}^{(X)}/N$, where $\mathbb{Q}^{(X)}/N$ is divisible, so injective. □

4.4 Tensor Product

Let R be an arbitrary ring, let M be a right R-module and let N be a left R-module. We denote them M_R and ${}_RN$ respectively.

Definition 4.4.1 (Bilinear Form, Tensor Product)**.** *Let A be an Abelian group written additively. A bilinear form on $M \times N$ with values in A is a map $B : M \to N \to A$ such that*

1. $B(m_1 + m_2, n) = B(m_1, n) + B(m_2, n)$,
2. $B(m, n_1 + n_2) = B(m, n_1) + B(m, n_2)$,
3. $B(ma, n) = B(m, an)$ *for* $a \in R$.

Then Bil$(M, N; A)$ is the Abelian group of all bilinear forms $M \times N \to A$. For a homomorphism $A \to A$", this induces Bil$(M, N; A) \to$ Bil$(M, N; A')$.

When $(M_R,{}_R N)$ is fixed, there is a functor $F : \mathbf{Ab} \to \mathbf{Ab}$ that sends A to Bil$(M, N; A)$.

The tensor product $M \otimes_R N$ is an Abelian group representing this functor:

$$\mathit{Bil}(M, N; A) \xrightarrow{\sim} \mathbf{Hom}(M \otimes_R N, A)$$

which gives an isomorphism. This functor is natural in A.

A tensor product, if exists, is unique up to canonical isomorphism.

Example 4.4.2. *Consider $M = R$, i.e. the ring as a left and right module over itself. The bilinear form is $B : R \times N \to A$ given by $B(x, n) = B(1, xn)$. Moreover, if $f : N \to A$ takes $n \mapsto B(1, n)$, then it is a group homomorphism.*

Therefore, $f(xn) = B(1, xn) = B(x, n)$.

Hence, Bil$(R, N; A) = \mathbf{Hom}(N, A)$. In particular, $R \otimes_R N \cong N$ and $M \otimes_R R \cong M$.

We now show that a tensor product always exists.

Theorem 4.4.3. *$M \otimes_R N$ exists for every $(M_R,{}_R N)$.*

Proof. It suffices to find a construction: then all tensor products should be related by the canonical isomorphism.

Let $X = M \times N$ as the product of sets. Consider $C = \mathbb{Z}^{(X)}/G$, the factorization of free Abelian group of basis X and a subgroup G, where G is generated by elements of the form:

1. $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$,
2. $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$,
3. $(ma, n) - (m, an)$ for all $a \in R$.

To give a homomorphism $C \to A$ is just to give $B : \mathbb{Z}^{(X)} \to A$ such that

1. $B(m_1 + m_2, n) = B(m_1, n) + B(m_2, n)$.
2. $B(m, n_1 n_2) = B(m, n_1) + B(m, n_2)$,
3. $B(ma, n) = B(m, an)$.

This is to give a map $f : M \times N = X \to A$.
Therefore, we would have an isomorphism $\mathbf{Hom}(C, A) \cong \mathrm{Bil}(M, N; A)$.
Therefore, C is the representing object, and denoted $C = M \otimes_R N$.

□

Remark 4.4.4. *An element $m \otimes n$ in $M \otimes N$ is the coset of (m, n). Then $M \otimes_R N$ is generated by $m \otimes_R n$ for $m \in M$, $n \in N$.*

Remark 4.4.5. *Therefore, given by the isomorphism $\mathbf{Hom}(C, A) \cong Bil(M, N; A)$, we have $Bil(M, N; M \otimes_R N \cong \mathbf{Hom}(M \otimes_R N, M \otimes_R N$. The identity in the hom set is corresponding to a universal element B_{univ} in $Bil(M, N; M \otimes_R N)$, which gives $B_{univ} : M \times N \to M \otimes_R N$.*

Suppose we have some other bilinear form $B : M \times N \to A$, then B corresponds to some homomorphism f, with

$$\begin{tikzcd} M \times N \arrow[r, "B_{univ}"] \arrow[dr, "B"'] & M \otimes_R N \arrow[d, "f"] \\ & A \end{tikzcd}$$

Therefore, every bilinear form B is the composition of a homomorphism f and the universal bilinear form.

The universal bilinear form is now given by $B_{univ}(m, n) = m \otimes_R n = m \otimes n$ for $m \in M$ and $n \in N$. Therefore, the universal property can be rewritten as the following: for every bilinear form $B : M \times N \to A$, there exists a unique homomorphism $f : M \otimes_R N \to A$ such that $B(m, n) = f(m \otimes n)$.

The universal property itself may also define the tensor product.

Property 4.4.6. *1.* $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$,

2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$,

3. $ma \otimes n = m \otimes an$.

Remark 4.4.7. *Recall that* $R \otimes_R N \cong N$*. Indeed,* $1 \otimes n$ *corresponds to* n *and* $a \otimes n$ *corresponds to* an*.*

Remark 4.4.8. *We can also consider the functoriality. Suppose* $f : M \to M'$ *and* $g : N \to N'$ *are two* R*-module homomorphisms. Then we can look at the following composition* B*:*

$$M \times N \xrightarrow{f \times g} M' \times N' \longrightarrow M' \otimes_R N'$$

Then B *is a bilinear form. Indeed, for example we have*

$$\begin{aligned} B(m_1 + m_2, n) &= f(m_1 + m_2) \otimes g(n) \\ &= f(m_1) \otimes g(n) + f(m_2) \otimes g(n) \\ &= B(m_1, n) + B(m_2, n) \end{aligned}$$

Therefore, there exists a unique homomorphism $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ *such that* $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$*.*

This induces a functor Mod-$R \times R$*-Mod* $\to$ **Ab** *given by* $(M, N) \mapsto M \otimes_R N$ *and* $(f, g) \mapsto f \otimes g$*.*

If we fix ${}_R N$*, then Mod-*$R \to$ **Ab** *is an additive functor that sends* $M \mapsto M \otimes_R N$*. In particular, we have the formula* $(f_1 + f_2) \otimes g = f_1 \otimes g + f_2 \otimes g$*.*

We now would like to know the properties of this additive functor.

Similarly, fix M_R*, then we have*

$$0 \longrightarrow N' \xrightarrow{h} N \xrightarrow{k} N'' \longrightarrow 0$$

exact in the category of R*-modules.*

By functoriality, we have an induced sequence

$$0 \longrightarrow \mathit{Bil}(M, N''; A) \longrightarrow \mathit{Bil}(M, N; A) \longrightarrow \mathit{Bil}(M, N'; A)$$

which is also exact:

$$\begin{tikzcd}
M \times N'' \arrow[dr, "B''"] & \\
M \times N \arrow[u] \arrow[r, "B"] & A \\
M \times N' \arrow[u] \arrow[ur, "0"'] &
\end{tikzcd}$$

Then $B''(m, n'') = B(m, n)$ by definition, where $n \in N$ is given by $k(n) = n''$. Therefore, this is independent of the choice on such maps.

When it comes to the definition of tensor product, equivalently, we have

$$0 \longrightarrow \boldsymbol{Hom}(M \otimes N'', A) \longrightarrow \boldsymbol{Hom}(M \otimes N, A) \longrightarrow \boldsymbol{Hom}(M \otimes N', A)$$

as exact sequence for arbitrary A.

This exactness on A is equivalent to the exactness of the following sequence on the right (because of contravariant properties):

$$M \otimes_R N' \xrightarrow{1_M \otimes h} M \otimes_R N \xrightarrow{1_M \otimes k} M \otimes_R N'' \longrightarrow 0$$

Therefore, $M \otimes_R -$ and $- \otimes_R N$ are both right exact.

Remark 4.4.9. *We now show that the tensor product is an additive functor by fixing one of the slots, i.e. commute with arbitrary direct sums.*

Let $(M_i)_{i \in I}$ be a family of right modules, and an arbitrary left R-module ${}_RN$. We want to show there is an canonical isomorphism $(\coprod_{i \in I} M_i) \otimes_R N \cong \coprod_{i \in I} M_i \otimes_R N$. The proof should be element-free.

The left-hand-side represents the functor of bilinear forms $Bil(\coprod_{i \in I} M_i, N; A)$. The right-hand-side represents the product $\prod_{i \in I} Bil(M_i, N; A)$. To see the two modules are isomorphic, it suffices to show that the two functors are isomorphic.

Consider the bilinear forms $B_i : M_i \times N \to A$. We can construct the bilinear form $B : \coprod_{i \in I} M_i \times N \to A$ by writing $B(\sum_{i \in I} m_i, n) = \sum_{i \in I} B_i(m_i, n)$. This induces an isomorphism of functors, with naturality in both slots.

Remark 4.4.10. *The tensor product is generated by the tensor product of elements. In particular, we have the following.*

Suppose $X \subseteq M_R$ and $Y \subseteq_R N$ are generating sets of modules.

We have homomorphisms $R^{(X)} \hookrightarrow M$ by sending $x \mapsto x$, and $R^{(Y)} \hookrightarrow N$ by sending $y \mapsto y$. ($R^{(X)}$ is viewed as a right R-module and $R^{(Y)}$ is viewed as a left R-module.)

Since the tensor product is left exact, we have surjections $R^{(X,Y)} = \coprod_{X \times Y} (R \otimes R)^{(X,Y)} = R^{(X)} \otimes R^{(Y)} \hookrightarrow M \otimes R^{(Y)} \hookrightarrow M \otimes N$*. Therefore the map takes the generating element* (x, y) *to the tensor product* $x \otimes y$*.*

Since this is a surjection, then $M \otimes_R N$ *is generated by elements of the form* $x \otimes y$ *for* $x \in X$ *and* $y \in Y$*.*

Example 4.4.11. *Suppose* $I \subseteq R$ *is a right ideal and let* M *be a left* R*-module. Then the short exact sequence*

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

is right exact when tensored with M*:*

$$I \otimes_R M \longrightarrow R \otimes_R M \longrightarrow R/I \otimes_R M \longrightarrow 0$$

Note that $R \otimes_R M$ *is just canonically isomorphic to* M*. For* $x \in I$*, the first map* α *takes* $x \otimes m \mapsto xm$*, then the image of* α *is* IM *, which is an Abelian group generated by* xm *for* $x \in I$ *and* $m \in M$*, left submodule generated by these elements.*

By exactness, we see that $R/I \otimes_R M$ *is canonically factor to the group* M/IM*.*

In particular, for integer n*, the group* A/nA *is isomorphic to* $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} A$*.*

Remark 4.4.12. *Suppose we have a bimodule* ${}_SM_R$ *where* R *and* S *are rings. We assume the two module structures are related as follows:* $(sm)t = s(mt)$*.*

We can rewrite as follows: for $l_s : M \to M$ *by* $m \mapsto sm$ *and* $t_x : N \to N$ *by* $n \mapsto nx$*. This says that* $l_s \circ t_x = t_x \circ l_s$*.*

In particular, consider ${}_SM_R$ *and* ${}_RN)$*. We can form Abelian group* $M \otimes_R N$*. We now have left multiplication by* s*, which we can tensor along with the identity:* $l_s \otimes 1_N : M \otimes_R N \to M \otimes_R N$*. This is a group endomorphism, and it makes the tensor product* $M \otimes_R N$ *a left* S *-module. Therefore, we can write* ${}_S(M \otimes_R N)$ *where* $s(m \otimes n) = sm \otimes n$*.*

Note that if R *is commutative, then left and right* R*-modules coincide, i.e.* ${}_RM_R$*. Recall that we define* $rm = mr$*. This is now a bimodule over* R*. Therefore, if* M, N *are* R*-modules for commutative ring* R*, then so is the tensor product* $M \otimes_R N$*.*

Remark 4.4.13. *Suppose we have* M_S*,* ${}_SN_R$ *and* P_R*. Then then tensor product* $(M \otimes_S N)_R$ *is a right* R*-module, and* $(\mathbf{Hom}_R(N, P))_S$ *is a group of homomorphisms of right* R*-modules, and has the right* S*-module structure.*

Having this in mind, we can write down the two Abelian groups through canonical isomorphisms, natural in all slots: Bil$(M, N; P) = \mathbf{Hom}_R(M \otimes_S N, P) \cong \mathbf{Hom}_S(M, \mathbf{Hom}_R(N, P))$*.*

The first equation is not so precise: for the definition of tensor product, we view them as Abelian groups now.

For any bilinear form $M \times N \to P$ in this group, or more precisely, $M \otimes_S N \to P$, we can define the hom on the right by $m \mapsto (n \mapsto B(m,n))$. Conversely, we ca take a map in hom φ to the bilinear map $B(m,n) = \varphi(m)(n)$. One can check easily they are inverses to each other as isomorphisms.

There is a similar situation when we have left modules. Consider $({}_SM, {}_RN_S, {}_RP)$. The corresponding isomorphisms are given by $\mathbf{Hom}_R(N \otimes_S M, P) \cong \mathbf{Hom}_S(M, \mathbf{Hom}_R(N, P)$.

Remark 4.4.14 (Construction of Change of Ring)**.** *Suppose we have $f : R \to S$ as a ring homomorphism, with ${}_RN, {}_SS_R$, this is by pulling elements back with $s \cdot t = s \cdot f(t)$.*

In this situation, we can form $S \otimes_R N$. But S is also a left module over itself, so it is a bimodule. Therefore, this is a left module, operates on the tensor of the form $s(x \otimes n) = sx \otimes n$.

In fact, we can get a functor of R-Mod $\to$ S-Mod by sending $M \mapsto S \otimes_R M$. Similarly, we can do the same on right modules.

Recall that we have a functor S-Mod $\to$ R-Mod given by the pullback construction with respect to f. It is not surprising that the two functors are adjoint to each other. In particular, for ${}_RN$ and ${}_SM$, we have $\mathbf{Hom}_S(S \otimes_R N, M) \cong \mathbf{Hom}_R(N, \mathbf{Hom}_S(S, M))$. Here $\mathbf{Hom}_S(S, M) \cong M$, but viewed as left R-module via the pullback. We get that the pullback functor $\mathbf{Hom}_S(S, -)$ is the right adjoint to the tensor product functor $S \otimes_R -$, i.e. extension of scalars.

We can now complete the proof that every module is a submodule of some injective module. We proved this for Abelian groups only. We now prove it for arbitrary modules.

Proposition 4.4.15. *Every module is a submodule of some injective module.*

Proof. Let M be an Abelian group. We use the only R-homomorphism $\mathbb{Z} \to R$ to view R as a $\mathbb{Z}$ module, and consider $\tilde{M} = \mathbf{Hom}_{\mathbb{Z}}(R, M)$, which is a left R-module.

Here we have ${}_{\mathbb{Z}}R_R$ and ${}_{\mathbb{Z}}M$.

Take any left R-module X. We can write the following formula: $\mathbf{Hom}_{\mathbb{Z}}(R \otimes_R X, M) \cong \mathbf{Hom}_R(X, \mathbf{Hom}_{\mathbb{Z}}(R, M))$. Note $R \otimes_R X$ is just X. We see that $\mathbf{Hom}_{\mathbb{Z}}(X, M) = \mathbf{Hom}_R(X, \tilde{M})$. Note that $\tilde{M}$ is the functor left adjoint to the pullback functor applied to X with respect to the homomorphism $\mathbb{Z} \to R$.

Suppose M is a divisible (therefore injective) Abelian group, then $\mathbf{Hom}_{\mathbb{Z}}(X, M)$ is an exact functor as a functor on X. Therefore, the functor $X \mapsto \mathbf{Hom}_R(X, \tilde{M})$ is also exact, now as functor R-Mod $\to$ $\mathbf{Ab}$.

Therefore, $\tilde{M}$ is an injective R-module.

So we have proven that the functor $\mathbf{Ab} \to R$-Mod that takes $M \mapsto \mathbf{Hom}_{\mathbb{Z}}(R, M) = \tilde{M}$ takes injectives to injectives.

Now we can prove that every left module can be embedded in some injective module.

Consider ${}_RM$, then $M \hookrightarrow Q$ is an embedding into a divisible (injective) Abelian group.

Therefore, applying the tilde construction to both, then since the hom functor is left exact, and the tilde is given by the hom functor, we still have an injection $\tilde{M} \hookrightarrow \tilde{Q}$. But now $\tilde{Q}$ is an injective R-module. We have $\tilde{M} = \mathbf{Hom}_{\mathbb{Z}}(R, M)$ is embedded in $\tilde{Q}$. So it suffices to embed $M \hookrightarrow \mathbf{Hom}_{\mathbb{Z}}(R, M)$ by $m \mapsto (\tau \mapsto \tau m)$. Therefore, in total we have an embedding $M \hookrightarrow \tilde{Q}$. □

4.5 Modules over a Principal Ideal Domain

This is almost the simpliest situation to classify modules, only after the situation of field. Over PID, we can classify the finitely generated ones.

Definition 4.5.1 (Torsion). *Let R be a domain and M be a R-module. An element $m \in M$ is called torsion if $\exists 0 \neq a \in R$ such that $am = 0$.*

All torsion modules form a submodule, called $M_{\text{tors}} \subseteq M$.

Definition 4.5.2 (Torsion, Torsion-free). *M is a torsion module if all elements are torsions, $M_{tors} = M$.*

M is a torsion-free module if $M_{tors} = 0$.

Lemma 4.5.3. *M/M_{tors} is torsion free.*

Example 4.5.4. *R is torsion-free because it is a domain. Free modules are torsion-free as well.*

Note that for $R = \mathbb{Z}$,$\mathbb{Q}$ is torsion-free but not free. In particular, for $x, y \in \mathbb{Z}$, there exists $a, b \in \mathbb{Z}$ such that $ax + by = 0$. $\mathbb{Q}$ is an infinitely-generated Abelian group.

Remark 4.5.5. *Notice that a factor module of an injective module over a PID is injective, because injective means divisble over PID, and factor module of divisible module is still divisible.*

There is a dual module for projectives, every submodule of projective modules is projective.

Also, every submodule of a free module is free. We will only show this statement for finitely-generated modules, but this is true in general.

Definition 4.5.6 (Rank)**.** *Note that for $R^m \cong R^n$, we have $n = m$. We call this the rank of R^n.*

Remark 4.5.7. *For a free R-module F, we say F is finitely generated if and only if the rank is finite.*

Proposition 4.5.8. *Let M be a submodule of a free finitely-generated module F over a PID R. Then M is free and rank$(M) \leq$ rank(F).*

Remark 4.5.9. *Note that this holds only on PID. Consider $I \subseteq R$ be an ideal, then I is free if and only if I is principal, i.e. for $x, y \in I$ we have $y \cdot x + (-x) \cdot y = 0$.*

Proof. Let $x_1, \cdots, x_n$ be a basis for F, we prove by performing induction on n.

When $n = 1$, I is an ideal of R, so it is principal and so free.

Suppose the statement is true for $n - 1$, we now show the case for n. Consider the projection of free module $f : F \to R$ given by $f(\sum(a_i x_i) = a_n$. Then the kernel $\ker(f)$ is just the free module with basis $x_1, \cdots, x_{n-1}$.

We have $M \subseteq F$ as a submodule, and the image $f(M) = I \subseteq R$ is still an ideal.

Let us take the kernel of this particular (restricted) surjective map to be M', then we have the exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M \longrightarrow 0$$

Note $M' = M \cap \ker(f) \subseteq \ker(f)$. Therefore, by induction, M' is free of rank at most $n - 1$.

Now I is free because it is principal, and so it is projective. In particular, the sequence above splits. Therefore, $M \cong M' \oplus I$. Both modules are free, where M' has rank at most $n - 1$ and I has rank at most 1, so M has rank at most n. This concludes the proof. □

Let R be a PID and M be a R-module. Recall that if we let $S = R \backslash \{0\}$, then the localization $S^{-1}R = F$ is the quotient field, or field of fractions. We know that R is a subring of F.

We can also localize the module, so $S^{-1}M$ is a vector space over F, which contains all fractions $\{\frac{m}{a}, a \neq 0\}$. Recall that $\frac{m}{a} = 0$ if and only if there exists $0 \neq b \in R$ such that $bm = 0$.

We also have the canonical map $M \to S^{-1}M$ that takes $m \in M$ to $\frac{m}{1}$. The kernel of this map is $\{m \in M : \exists 0 \neq b \in R : bm = 0\} = M_{\text{tors}}$.

Therefore, M is torsion-free if and only if $M \hookrightarrow S^{-1}M$ is an embedding.

Theorem 4.5.10. *A finitely generated torion-free module over a PID R is free.*

Proof. Since M is a torsion-free R-module, then $M \hookrightarrow S^{-1}M$, considered as a vector space over F of finite dimensions.

Let $x_1, \cdots, x_n$ be a basis for $S^{-1}M$. Let $N = Rx_1 + \cdots + Rx_n$. Then N is a free R-module with basis $x_1, \cdots, x_n$.

Now module M is finitely generated, by picking finitely many generators $m_1, \cdots, m_k$ where $m_i \in M \subseteq S^{-1}M$. Therefore, $m_i \in Fx_1 + \cdots + Fx_n$.

There exists $0 \neq a_i \in R$ such that $a_i m_i \in N$. If we take the product of all the a_i's, then let $a = a_1 \cdots a_k \neq 0$, so $am_i \in N$. Therefore, $a \cdot M \subseteq N$. But N is free, then aM is free.

However, there is an isomorphism $a \xrightarrow{\sim} aM$, so M is free. □

Remark 4.5.11. *Suppose M is a finitely generated R-module over a PID R. There is a short exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & M_{tors} \arrow[r] & M \arrow[r] & M/M_{tors} \arrow[r] & 0 \end{tikzcd}$$

Note that M/M_{tors} is torsion-free, and is finitely generated, then it is free. In particular, it is projective, so the short exact sequence splits.

Therefore, $M \cong M_{tors} \oplus M/M_{tors} \cong M_{tors} \oplus R^n$ where n is the rank of M.

Now, $S^{-1}M \cong S^{-1}M_{tors} \oplus F^n$ where n is the rank of M. Note that $S^{-1}M_{tors} = 0$, killed by the localization. Therefore, this is nothing but $\dim_F(S^{-1}M)$.

The study of finitely generated modules can then be focused on torsion finitely generated modules.

Definition 4.5.12 (Primary)**.** *Let M be a torsion, finitely generated R-module. Take $0 \neq P \subseteq R$ as a non-zero prime ideal of R. Therefore, $P = p \cdot R = R \cdot p$ for some prime p.*

We say that $m \in M$ is P-primary if $P^n \cdot m = 0$, which is equivalent to $p^n m = 0$ for some $n > 0$.

We denote $M(P)$ as the set of all P-primary elements in M, also called the P-primary part of M.

Claim 4.5.13. *$M(P)$ is a submodule.*

Proof. A lot of things need to be checked. We only check that the sum is still in $M(P)$.

For $m_1, m_2 \in M(P)$, then $p^{k_1} \cdot m_1 = 0 = p^{k_2} m_2$ for some k_1, k_2. Let $k = \max(k_1, k_2)$, then $p^k \cdot m_i = 0$ for all $i = 1, 2$. Therefore, $p^k(m_1 + m_2) = 0$, which means $m_1 + m_2 \in <(P)$. □

Lemma 4.5.14. *Let $a_1, \cdots, a_n$ be relatively prime elements in a PID R. Then there exists $b_1, \cdots, b_n \in R$ such that $\sum_{i=1}^{n} b_i a_i = 1$.*

Proof. Take the ideal generated by relatively prime elements $I = Ra_1 + \cdots + Ra_n = cR$ is principal for some $0 \neq c \in R$.

Therefore, $c \mid a_i$ for all i, and so $c \in R^\times$ because elements are relatively prime. Therefore, $I = cR = R$. The ideal is just the unit ideal, so $1 \in I$. Therefore, one can find the desired linear combination. □

Remark 4.5.15. *The notion of relatively prime elements not only make sense in PID, but also in UFD. However, the statement is not true over UFD. For example, consider $R = F[x_1, x_2]$ where x_1, x_2 are relatively prime. Here we have $Rx_1 + Rx_2 \neq R$.*

Corollary 4.5.16. *Let M be a module over a PID R, and let $a_1, \cdots, a_n \in R$ be relatively prime and $m \in M$. If $a_i m = 0$ for all i, then $m = 0$.*

Proof. By lemma, we can find b_i's such that $\sum b_i a_i = 1$, then $m = 1 \cdot m = \sum b_i a_i m = 0$. □

Theorem 4.5.17. *Let M be a torsion, finitely generated module over a PID R. Then:*

1. *$M(P) = 0$ for almost all prime ideals $P \neq 0$.*
2. *$M = M(P_1) \oplus M(P_2) \oplus \cdots \oplus M(P_n)$ for some prime ideal P_i. In other words, M is the direct sum of finitely many primary submodules.*

Proof. Since M is finitely generated and torsion, then it can be killed by one element in the ring. In particular, $\exists 0 \neq a \in R$ such that $a \cdot M = 0$.

Claim 4.5.18. *If P is a prime ideal such that $a \notin P$, then $M(P) = 0$.*

Subproof. We write the ideal as $P = R \cdot p$. Since $a \notin P$, then $p \nmid a$. Then because every element $m \in M(P)$ is killed by a power of p, i.e. $p^n \cdot m = 0$, and killed by a, i.e. $a \cdot m = 0$. By corollary, this means $m = 0$, since a and p^n are relatively prime. Therefore, $M(P) = 0$. ■

If we factor a as a product of prime elements, i.e. $a = up_1^{t_1} \cdots p_s^{t_s}$ where p_i's are distinct primes, u is a unit, then $a \in P_i = Rp_i$ and $a \notin P \neq P_i$. (Note that the prime ideals P_i's are distinct.) This proves the first part.

Claim 4.5.19. $M = \coprod M(P_i)$.

Subproof. Take arbitrary $m \in M$ and write $a_i = \frac{a}{p_i^{t_i}}$ where $a_1, \cdots, a_s$ are relatively prime.

By lemma, $\exists b_i \in R$ such that $\sum\limits_{1 \leq i \leq s} b_i a_i = 1$, and so $m = \sum\limits_{1 \leq i \leq s} b_i a_i m$. In particular, $p^{t_i} b_i a_i m = b_i a m = 0$. Therefore, $am = 0$.

Now, $b_i a_i m \in M(P_i)$. ■

Therefore, $M = \sum M(P_i)$. We need to show that this is a direct sum, i.e. for $m_i \in M(P_i)$ such that $m_1 + \cdots + m_s = 0$. We need to show that all $m_i = 0$.

One can choose a power t such that $p_i^t \cdot m_i = 0$ for all i. Now we take integer k from $1, \cdots, s$, then it suffices to show that $m_k = 0$.

Now $q = \frac{p_1^t p_2^t \cdots p_s^t}{p_k^t}$. In particular, since p_i^t kills all m_i, then $qm_i = 0$ for all $i \neq k$. However, this means $q \cdot m_k = 0$ as well. On the other hand, $p_k^t \cdot m_k = 0$. However, q and p_k^t are relatively prime, so we have $q \cdot m_k = 0$ and $p_k^t \cdot m_k = 0$. By the corollary, we know $m_k = 0$.

□

This statement shows that every torsion-free finitely generated module is a direct sum of some primary modules, therefore this reduces our study to the study of primary modules.

Definition 4.5.20 (Cyclic)**.** *An R-module N is cyclic if N is generated by one element.*

Remark 4.5.21. *From homework, we know that every cyclic module N is isomorphic to the factor module R/I for some ideal $I \subseteq R$. Obviously R is generated by one element, and I is also generated by one element. Therefore, all cyclic modules are of this form.*

In particular, since $I = aR$ for some a, we should have $N \cong R/aR$, which is torsion-free if and only if $a \neq 0$.

Claim 4.5.22. *The module $N = R/aR$ is P-primary if and only if $aR = P^n$ for some n.*

Proof. The $\Leftarrow$ direction is clear. On the other hand, suppose N is P-primary, then write $P = Rp$, and we see that $p^n N = 0$ for some power n. Therefore, $p^n R \subseteq aR$. Therefore,

$a \mid p^n$, but an element that divides p^n is also some power of p (up to units), so $a = up^m$. Therefore, $aR = p^m R = P^m$. □

Remark 4.5.23. *Therefore, cyclic P-primary modules all have the form R/P^n for some n.*

Definition 4.5.24 (Residual Field)**.** *Suppose $0 \neq P \subseteq R$ is a prime ideal, and consider P-primary R-modules. First of all, note that $K = R/P$ is a field, called the residue field of P.*

Remark 4.5.25. *Let R be a PID and $P = pR$ is a prime ideal in R. Let M be a P-primary finitely generated R-module over R. We have a sequence of submodules that form the filtration. More precisely, $M \supseteq P \cdot M \supseteq P^2 \cdot M \supseteq \cdots \supseteq P^n M = 0$. (Here we write $P = pR$ and $P \cdot M = pM$.) We can take the subsequence factor $P^i M / P^{i+1} M$. This is an R-module for sure. Now $P(P^i M/P^{i+1}M) = 0$, so the factor module is killed by P. In particular, $P^i M/P^{i+1}M$ is an R/P-module, but R/P is the residual K, so this is a vector space over K of finite dimension. Therefore, it makes sense to talk about the dimensions of each of these factor modules.*

Definition 4.5.26 (Length)**.** *We define the length of the module M to be $l(M) = \sum\limits_{i=0}^{n-1} \dim_K(p^i M/p^{i+1}M) \geq 0$.*

Property 4.5.27.

1. *The length of a cyclic module $l(R/p^n R) = n$. This is because those factors $p^i M/p^{i+1}M \cong p^i R/p^{i+1} R \cong R/P = K$. This is a one-dimensional vector space, so when summing the dimension up for $i = 0, \cdots, n-1$, we have n. Why does the last isomorphism hold? Observe that*

$$P \longrightarrow R \xrightarrow{\cdot p^i} p^i R/p^{i+1R} \longrightarrow 0$$

   is an exact sequence as P is a kernel of $\cdot p^i$. The result follows from the first isomorphism theorem.

2. *If M, N are P-primary finitely generated modules, then $l(M \oplus N) = l(M) + l(N)$.*

3. *If $0 \neq N \subseteq M$ is a submodule, and both are P-primary finitely generated modules, then $l(M/N) < l(M)$. We can denote $M' = M/N$. Then there is a natural surjection $\varphi_i : p^i M/p^{i+1}M \twoheadrightarrow p^i M'/p^{i+1}M'$, given by the surjection $M \twoheadrightarrow M'$. We need strict equality.*

Note that there exists some unique i such that $N \subseteq p^iM$ but $N \not\subseteq P^{i+1}M$. The image of N in $p^iM/p^{i+1}M$ is nonzero (because $N \not\subseteq P^{i+1}M$), but the image of N in $p^iM'/p^{i+1}M'$ is zero, so the kernel of φ_i is non-zero.

We now write ${}_pM = \{m \in M : pm = 0\} = \ker(M \xrightarrow{p} M)$. Note that this is a submodule, and the ideal P acts on ${}_pM$ trivially, i.e. $P \cdot_p M = 0$. Therefore, ${}_pM$ is a vector space over $K = R/P$.

Lemma 4.5.28. *Given by the setting above, assume that $p^nM = 0$ but $p^{n-1}M \neq 0$. If $\dim_P(M) = 1$, then $M = R/P^n = R/p^nR$.*

Proof. By assumption, there exists an element $x \in M$ such that $p^{n-1}x \neq 0$.

Claim 4.5.29. *If $ax = 0$ for some $a \in R$, then $p^n \mid a$.*

Subproof. We write $a = p^m \cdot b$ for $\gcd(p, b) = 1$. We need to show that $m \geq n$. Suppose, towards contradiction, that $m < n$. Therefore, $b(p^mx) = ax = 0$, and $p^{n-m}p^mx = p^nx = 0$. However, p^{n-m} and b are relatively prime, so by lemma we conclude $p^mx = 0$. However, $p^{n-1}x \neq 0$, contradiction. ■

Consider the homomorphism $R \to M$ given by $a \mapsto ax$. Since $P^n \cdot x = 0$, then P^n is contained in the kernel.

Consider $f : R/P^n = R/p^n \cdot R \to M$ given by $a + P^n \mapsto ax$.

Suppose $f(a + P^n) = ax = 0$. Then by claim $a \in P^n$. Therefore, f is injective. Also, we can show that every $y \in M$ is contained in Rx. We can pick smallest k such that $p^ky = 0$. We now do induction on k.

If $k = 1$, $py = 0$, with $y \in_p M \ni p^{n-1}x \neq 0$. Since $\dim_P(M) = 1$, there exists $b \in R$ such that $y = b \cdot p^{n-1}x \in Rx$.

Suppose the case is true for $k - 1$, we prove the case for k. Take $p^{k-1}(py) = 0$, by induction, $py \in Rx$, $py = ax$ for some $a \in R$. Now $0 = p^ny = p^{n-1}ax$. By the claim, $p^n \mid p^{n-1}a$, so $p \mid a$, and we can write $a = pb$ for some $b \in R$. Therefore, $py = pbx$, so $p(y - bx) = 0$. Therefore, $y - bx \in_P M \subseteq Rx$. So $y \in Rx$. Therefore, the map is surjective. In particular, we have an isomorphism as desired. □

Proposition 4.5.30. *Let $p^nM = 0$ but $p^{n-1}M \neq 0$. Then there is a surjective R-module homomorphism $M \twoheadrightarrow R/p^nR$.*

Proof. We perform induction on $l(M)$. We pick $x \in M$ such that $p^{n-1}x \neq 0$. However, $p^nx = 0$ would indicate $0 \neq p^{n-1}x \in_P M$, and so the dimension $\dim_K({}_PM) > 0$.

If $\dim({}_P M) = 1$, by lemma, $M \cong R/p^n R$.

If $\dim({}_P M) > 1$, then there exists a nonzero subspace (submodule) $N \subseteq_p M$ such that $Rp^{n-1}x \nsubseteq N$. Consider the factor module $M' = M/N$, then $l(M') < l(M)$. Then $p^{n-1}(x+N)$ as an element of M' is not equal to N. Therefore, $p^{n-1}M' \neq 0$, as it contains some $x + N \in p^{n-1}M'$, but $p^n M' = 0$. By the induction step, there exists a surjective homomorphism composed by $M \twoheadrightarrow M' \twoheadrightarrow R/p^n R$. □

Theorem 4.5.31. *Every finitely generated P-primary R-module M is isomorphic to a direct sum of cyclic modules R/P^k.*

Proof. We prove by performing induction on $l(M)$. As usual, we choose n such that $p^n M = 0$ but $p^{n-1}M \neq 0$. In particular, M is a R/P^n-module because P^n kills the module. By proposition, there is a surjective R-module homomorphism $M \twoheadrightarrow R/P^n$, and can be embedded in the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & M \arrow[r, two heads] & R/P^n \arrow[r] & 0 \end{tikzcd}$$

Note that this is a short exact sequence of R/P^n modules. The last module R/P^n is free and so projective, then the sequence splits. We consider this as a splitting on R-modules. So $M \cong N \oplus (R/P^n)$ as R-modules.

In particular, $l(N) = l(M) - n < l(M)$. By induction, N is a direct sum of cyclic modules. □

Therefore, collecting the results we saw above, if we let M be a finitely generated R-module over a PID R, then R is a direct sum of modules of the form R and R/P^n for prime ideal P's. Note that every module here is cyclic, so every finitely generated R-module over PID is a direct sum of cyclic modules.

We just saw such decomposition holds, but we still need to check uniqueness.

Remark 4.5.32. *Recall that $M = R^n \oplus M_{tors}$, where $n = \dim_F(S^{-1}M)$ and is the rank of M. Here $S = R\backslash\{0\}$. It sufficient to prove that the torsion part has unique decomposition, up to permutation of terms.*

Therefore, consider $M = M_{tors}$, so M is a finite direct sum of $M(P)$'s. To prove uniqueness, we consider $M = M(P)$ as some P-primary ideal. We write $M = \coprod_{i=1}^{\infty} (R/P^i R)^{\oplus s_i}$. It suffices to express the integer s_i in terms of the module M in a unique way.

We use the following computations: suppose $N = R/p^n R$ is a cyclic module. Then $p^{k-1}N = p^{k-1}R/p^n R$ and $p^k N = p^k R/p^n R$, and $p^{k-1}N/p^k N \cong R/pR$ for $k \leq n$. However, if $k > n$, $p^{k-1}N = 0$ because p^{k-1} kills the module.

To remember, $\dim_K(p^{k-1}N/p^kN) = \begin{cases} 1, & \textit{if } k = 1, \cdots, n \\ 0, 7 \textit{ if } k > n \end{cases}$.

Now $l_K = \dim_K(p^{k-1}M/p^kM) = s_k + s_{k+1} + \cdots$. *Therefore,* $s_k = l_k - l_{k+1}$.

Let M be a torsion module over a PID R. Then there exists distinct prime ideals $P_1, \cdots, P_k$ such that $M \cong R/P_1^{\alpha_{11}} \oplus R/P_1^{\alpha_{12}} \oplus \cdots \oplus R/P_1^{\alpha_{1t_1}} \oplus R/P_2^{\alpha_{21}} \oplus \cdots \oplus R/P_2^{\alpha_{2t_2}} \oplus \cdots \oplus R/P_k^{\alpha_{k1}} \oplus \cdots \oplus R/P_k^{\alpha_{kt_k}}$, and without loss of generality we have $\alpha_{11} \geq \alpha_{12} \geq \cdots$, $\alpha_{21} \geq \alpha_{22} \geq \cdots, \cdots, \alpha_{k1} \geq \alpha_{k2} \geq \cdots$.

The family $\{P_i^{\alpha_{ij}}\}$ is called the set of elementary divisors of M, also known as $ED(M)$. This family of elementary divisors is unique up to permutation of terms.

In particular, if M is a finitely generated module, then $M = R^n \oplus M_{\text{tors}}$. If N is finitely generated as well, then $M \cong N$ if and only if they have the same rank and the same elementary divisor, i.e. $\text{rank}(M) = \text{rank}(N)$, $ED(M) = ED(N)$.

Theorem 4.5.33 (Elementary Divisor Form). *Two finitely generated R-modules over a PID are isomorphic if and only if they have the same rank and the same families of elementary divisors.*

Given by the structure above, by applying the Chinese Remainder Theorem, we have $R/P_1^{\alpha_{1j}} \oplus R/P_2^{\alpha_{2j}} \oplus \cdots \oplus R/P_k^{\alpha_{kj}} = R/I_j$ where $I_j = \prod_{i=1}^{k} P_{i,j}^{\alpha_{i,j}}$. Now $M \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s$ for some $s = \max_{1 \leq i \leq k}(t_i)$. In particular, $I_1 \subset I_2 \subset \cdots I_s$. We can write every ideal here as a principal ideal, e.g. $I_j = a_jR$ for some $a_j \in R$. Equivalently, we have $a_s \mid a_{s-1} \mid \cdots \mid a_2 \mid a_1$.

Conversely, if we know the ideals, we can write down the matrices, by factoring the ideals into the powers of prime ideals. The family of those ideals $\{I_s, I_{s-1}, \cdots, I_1\}$ is called the family of invariant factors of M, denoted $IF(M)$, and are determined uniquely. Sometimes we just write it in terms of $\{a_s, a_{s-1}, \cdots, a_1\}$ and call them the invariant factors (but those are not uniquely determined, since there can be multiple generators for an ideal).

In particular, the two forms are equivalent, and so we have the following theorem:

Theorem 4.5.34 (Invariant Factor Form). *Two finitely generated R-modules are isomorphic if and only if they have the same rank and the same invariant factors.*

Remark 4.5.35 (How to compute the two forms?). *Take M to be a finitely generated R-module, then it is a factor module of a finitely generated free R-module F, and there is* *a submodule $N \subseteq F$ such that $M \cong F/N$. Moreover, N is free because it is a submodule of the free module.*

We get to choose a basis $\{x_1, x_2, \cdots, x_n\}$ for F, and let $\{y_1, y_2, \cdots, y_n\}$ be a set that generates N, where $m \leq n$. Because $N \subseteq F$, then $y_1 = a_{11}x_1 + a_{21}x_2 + \cdots + a_{n1}x_n$, $y_2 = a_{12}x_2 + \cdots + a_{n2}x_n$, up until $y_m = a_{1m}x_1 + a_{2m}x_2 + \cdots + a_{nm}x_n$. We then construct a matrix $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix}$, as the transpose of the system of equations above.

Suppose A is of the form $\begin{pmatrix} t_1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & t_2 & 0 & \cdots & \cdots & \cdots & \vdots \\ 0 & \cdots & \ddots & \cdots & \cdots & \cdots & \vdots \\ 0 & \cdots & \cdots & t_k & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$, such that $t_i \neq 0$ and $t_1 \mid t_2 \mid \cdots \mid t_k$, then we have $y_i = \tau_i x_i$ for $i \leq k$, and $y_i = 0$ for $i > k$. Now, $M = R/t_1R \oplus R/t_2R \oplus \cdots \oplus R/t_kR \oplus R \oplus R \cdots \oplus R$, where there are $m - k$ terms of R-summands.

Recall that $t_1 \mid t_2 \mid \cdots \mid t_k$. Therefore, the invariant factors of M are just the invariant factors of M_{tors}, which is $(t_1R, \cdots, t_kR)$.

Although the matrix A we considered is very preliminary, we can introduce the following operations so that we get to consider an arbitrary matrix:

1. *Transposition of two rows/columns. Such operations don't change M, N or F.*

2. *Subtraction from a row (respectively, column) a multiple of another row (respectively, column). This operation changes the basis elements, but doesn't change the modules M, N or F.*

3. *Multiplication of a row/column by a unit of R. Again, this does not change the modules.*

Note that by applying the three operations, we can get to a simplified form as denoted above.

Example 4.5.36. *Consider $R = \mathbb{Z}$, so the R-modules are the Abelian groups. Consider $M = \mathbb{Z}^2 / \left\langle \begin{pmatrix} 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \end{pmatrix} \right\rangle$. We take the standard basis of $\mathbb{Z}^2$, i.e. $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, with*

$y_1 = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$ *and* $\begin{pmatrix} 2 \\ 4 \end{pmatrix}$*. Therefore,* $A = \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}$*. We then have*

$$\begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix} \to \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 4 \\ 0 & -6 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 0 & -6 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$$

Therefore, the invariant factor form of M *is* $\{2, 6\} = \{2\mathbb{Z}, 6\mathbb{Z}\}$*. Therefore,* $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$*. Now,* $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$*, so* $M \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$*. Hence, the elementary divisor form of* M *is given by* $\{2, 2, 3\}$*.*

We now want to apply our results to PIDs. In particular, for the ring $R = \mathbb{Z}$, the R-modules are exactly the Abelian groups. This would help us classify the finitely-generated Abelian groups.

4.6 Finitely-generated Abelian Groups

Let $R = \mathbb{Z}$. Corresponding to the results above, we have two forms of the main theorem:

Theorem 4.6.1 (Elementary Divisor Form)**.** *Every finitely generated Abelian group is isomorphic to a direct sum of cyclic groups, i.e.* $\mathbb{Z}$ *or* $\mathbb{Z}/p^n\mathbb{Z}$ *for some prime* p*. Two groups are isomorphic if and only if they have the same rank and the same elementary divisors.*

Theorem 4.6.2 (Invariant Factor Form)**.** *Every finitely generated Abelian group is isomorphic to a direct sum of the form* $\mathbb{Z}^m \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z}$ *with* $a_1 \mid a_2 \mid \cdots \mid a_s$*. The ideals* $a_1\mathbb{Z}, \cdots a_s\mathbb{Z}$ *are uniquely determined.*

Moreover, if we assume the integers are positive, then the integers are uniquely determined. Two groups are isomorphic if and only if they have the same rank and the same invariant factors.

Although it is very obvious in this case, the result is not very obvious in general.

4.7 Canonical Form of a Linear Operator

Let F be a field, and V is a vector space of finite dimension over F. Let $S : V \to V$ be a linear operator. Of course, V can be viewed as a module over the field, and then S is just an endomorphism over the module V. We try to classify these linear operators.

Let $R = F[x]$, then it is a Euclidean domain and then a PID. We now get to define an R-module structure on V: let $a_i \in F$, then the scalar multiplication is defined by $(a_nx^n_+ \cdots a_1x + a_0) \cdot v = a_nS^n(v) + \cdots + a_1S(v) + a_0v$. Conversely, suppose M be a R-module, then because F is a subring of R, then M becomes a F-module, and therefore is a vector space over F. Define $T : M \to M$ by $T(m) = x \cdot m$. Then T is a linear operator over the vector space M.

Moreover, if M is a finitely generated module (not necessarily of finite dimension), then $M \cong R^k \oplus M_{\text{tors}}$ for some k. Note that R^k is infinite-dimensional if k is positive. We will see later that M_{tors} always has a finite dimension. Therefore, $\dim(M) < \infty$ if and only if M is torsion as an R-module.

We now can translate between the language of R-modules (where R is a polynomial ring), Linear Operators and Matrices.

(Torsion Finitely-generated) R-modules	Linear Operators	Matrices
Module V	$S : V \to V$, $S(v) = x \cdot v$	$[S]_{\mathcal{B}}$ as $n \times n$ matrix
Direct sum operation $V_1 \oplus V_2$	$S_1 \oplus S_2 : V_1 \oplus V_2 \to V_1 \oplus V_2$ for $(S_1 \oplus S_2) * v_1, v_2) = (S_1(v_1), S_2(v_2))$	$[S_1 \oplus S_2]_{\mathcal{B}_1 \cup \mathcal{B}_2} = \begin{pmatrix} [S_1]_{\mathcal{B}_1} & 0 \\ 0 & [S_2]_{\mathcal{B}_2} \end{pmatrix}$
Isomorphism $\alpha : V_1 \xrightarrow{\cong} V_2$ for $\alpha(f \cdot v) = f \cdot \alpha(v)$, $f \in R, v \in V_1$	For $S_i : V_i \to V_i$, $S_i(v) = xv$, $S_2 \circ \alpha = \alpha \circ S_1$ commutes: $S_1 \cong S_2$ iff $\exists \alpha : V_1 \to V_2 : \alpha \circ S_1 = S_2 \circ \alpha$	$[S_1]_{\mathcal{B}_1}$ and $[S_2]_{\mathcal{B}_2}$ are similar: $[S_2]_{\mathcal{B}_2} = A \cdot [S_1]_{\mathcal{B}_1} \cdot A^{-1}$ where A is the matrix of α
Cyclic R-module R/fR	$S : V \to V$ is cyclic	Companion Matrix $C(f)$

Figure 4.1: Relationship between (Torsion Finitely-generated) R-modules, Linear Operators and Matrices

Remark 4.7.1 (Cyclic Correspondence). *Without loss of generality, we can write f as a monic polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 + a_0 \in F[x]$. There is a canonical map $R = F[x] \to M = R/fR$ by sending $g \mapsto g\bar{g}$.*

We claim that $\{\bar{1}, \bar{x}, \bar{x}^2, \cdots, \bar{x}^{n-1}\}$ is a basis for M. In particular, $\dim_F(M) = n = \deg(f) < \infty$.

For $\bar{g} \in M$, $g = f \cdot q + t$ where $\deg(t) < n$. So $t = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$, hence $\bar{g} = \bar{f}\bar{q} + \bar{t} = \bar{t} = b_0 \cdot \bar{1} + b_1\bar{x} + \cdots + b_{n-1}\bar{x}^{n-1}$. Moreover, suppose $c_0 \cdot \bar{1} + c_1 \cdot \bar{x} + \cdots + c_{n-1}\bar{x}^{n-1} = 0$. We want to show that $c_i = 0$ for all i. Let $h = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in fR$, then $f \mid h$, so $\deg(f) = n > \deg(h)$. Hence, $h = 0$, and so $c_i = 0$ for all i.

Therefore, $\{\bar{1}, \bar{x}, \bar{x}^2, \cdots, \bar{x}^{n-1}\}$ is a basis for $M = R/fR$. Let $S : M \to M$ be the operator $S(\bar{g}) = x\bar{g}$. Therefore, $S(\bar{x}^i = x \cdot \bar{x}^i = \bar{x}^{i+1}$ for $i < n-1$, and $S(\bar{x}^{n-1}) = \bar{x}^n = -a_0 \cdot \bar{1} - a_1 \cdot \bar{x} - \cdots - a_{n-1}\bar{x}^{n-1}$. Moreover, we get the matrix $[S]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$.

This is exactly the companion matrix of f, denoted $C(f)$.

Theorem 4.7.2 (Invariant Factors and Elementary Divisors for Operators)**.** *Let V be a finite-dimensional vector space over F, and $S : V \to V$ is a linear operator. Then*

1. *(Invariant Factor Form) there exists unique monic polynomials $f_1 \mid f_2 \mid \cdots \mid f_r$ such that the matrix of S in some basis is the block diagonal matrix of the form diag$(C(f_1), C(f_2), \cdots, C(f_r))$. This matrix is then unique. This is called the canonical form of S.*

2. *(Elementary Divisor Form) there exists polynomials $p_1^{k_1}, p_2^{k_2}, \cdots, p_s^{k_s}$ (unique up to permutation) where p_i's are monic irreducible polynomials, such that the matrix of S in some basis is of the form diag$(C(p_1^{k_1}), C(p_2^{k_2}), \cdots, C(p_s^{k_s}))$.*

Theorem 4.7.3. *Let A be an $n \times n$ matrix over a field F. Then*

1. *(Invariant Factor Form) there are unique monic polynomials $f_1 \mid f_2 \mid \cdots \mid f_r$ such that A is similar to diag$(C(f_1), C(f_2), \cdots, C(f_r))$, which is called the canonical form of A.*

2. *(Elementary Divisor Form) there are $p_1^{k_1}, p_2^{k_2}, \cdots, p_s^{k_s}$ unique up to permutation such that AA is similar to the block diagonal matrix diag$(C(p_1^{k_1}), C(p_2^{k_2}), \cdots, C(p_s^{k_s}))$.*

Remark 4.7.4. *Let A be an $n \times n$ matrix over the field. How to find its canonical form?*

Correspondingly, there is a matrix $x \cdot I_n - A = \begin{pmatrix} x - a_{11} & a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}$ *over $R = F[x]$. The determinant* $\det(xI_n - A) = p_A(x)$ *is called the characteristic polynomial of A, and is monic of degree n. It is also equivalent to the product of all invariant factors.*

Consider the submodule $N \subseteq R^n$, generated by the columns of $xI_n - A$.

Lemma 4.7.5. $\dim_F(R^n/N) = n$.

Proof. Denote $F = R^n \supseteq N$. Let y_i be the i-th column of $xI_n - A$. We want to find the invariant factors of the factor module R^n/N.

By elementary transformations, we can transform $xI_n - A$ to $\operatorname{diag}(f_1, f_2, \cdots, f_n)$. (Indeed, elementary transformations only change the determinant by a scalar.) Then $p_A(x) = f_1 f_2 \cdots f_n$ and $n = \deg(p_A) = \sum \deg(f_i) = \sum \dim(R/f_iR) = \dim_F(R^n/N)$ since $R^n/N \cong R/f_1R \oplus R/f_2R \oplus \cdots \oplus R/f_nR$. Thus, the invariant factors of R^n/N are exactly $\{f_1, f_2, \cdots, f_n\}$, where $f_1 \mid f_2 \mid \cdots \mid f_n$. □

Now, suppose $S : V \to V$ is a linear operator on vector space V, and choose a basis $\{v_1, \cdots, v_n\}$ for V. Let $A = [S]_{\mathcal{B}}$. We define $g : R^n \to V$ such that $g(f_1, f_2, \cdots, f_n) = f_1(S)(v_1) + f_2(S)(v_2) + \cdots + f_n(S)(v_n)$. This is a R-module homomorphism.

Now, if we apply the first column of $xI_n - A$, we get $g(x - a_{11}, -a_{21}m \cdots, -a_{n1}) = S(v_1) - a_{11} - a_{21}v_1 - \cdots - a_{n1}v_n = 0$. This is true for any column of $xI_n - A$. Therefore, $g(N) = 0$ where N is the submodule generated by the columns. Hence, $N \subseteq \ker(g)$, and so g factors as $g : R^n \to R^n/N \twoheadrightarrow V$. By lemma, R^n/N is n-dimensional, and V is also n-dimensional. Therefore, $h : R^n/N \to V$ is an isomorphism between R-modules.

The goal now is to find the invariant factors of this module V, which is the same as looking for the invariant factors of R^n/N. We can do some by performing elementary transformations on $xI_n - A$, and get a diagonal matrix of the form diag$(f_1, f_2, \cdots, f_n)$ where $f_1 \mid f_2 \mid \cdots \mid f_n$ are monic polynomials, and $V \cong R/f_1R \oplus R/f_2R \oplus \cdots \oplus R/f_nR$. However, note that some of the f_i's are units. WLOG say $f_1 = f_2 = \cdots = f_k = 1$ and $\deg(f_m) > 0$ for all $m > k$. Therefore, the invariant factors of S (or invariant factors of A, or invariant factors of V) are just $\{f_{k+1}, \cdots, f_n\}$.

Example 4.7.6. 1. *Let $A = \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}$. Then $xI_2 - A = \begin{pmatrix} x & 2 \\ 1 & x-3 \end{pmatrix}$. By elementary operations, this matrix can be transformed into the form $\begin{pmatrix} 1 & 0 \\ 0 & x^2 - 3x + 2 \end{pmatrix}$. Therefore, the invariant factors of A is $\{x^2 - 3x + 2\}$ as 1 is a unit.*

The canonical form of the matrix is just the companion matrix $C(x^2 - 3x + 2) = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$. Note that this is similar to matrix A.

2. *Find representatives of conjugacy classes in $G = GL_2(\mathbb{Z}/p\mathbb{Z})$ where p is a prime. Let $F = \mathbb{Z}/p\mathbb{Z}$, and note that $G = (p^2 - 1)(p^2 - p)$. Take a 2×2 matrix $A \in G$, then*

the matrix is invertible with determinant nonzero. We take the invariant factors of A. We know that up to conjugacy, matrix A is uniquely determined by the factors $f_1, f_2, \cdots, f_s$ (non-constant monic polynomials such that $f_1 \mid f_2 \mid \cdots \mid f_s$.

Recall that $p_A(x)$ is the product of invariant factors, so n is the sum of degrees of the invariant factors. Therefore, the sum of degrees $f_1, \cdots, f_s$ is 2. Also, given that $\det(A) \neq 0$ and $\det(A) = \pm p_A(0)$, so $p_A(0) \neq 0$, i.e. $f_i(0) \neq 0$ for all i. There are two cases. Either 1) there is only one invariant factor $f_1 = x^2 + ax + b$ for $b \neq 0$, or 2) there are two invariant factors f_1, f_2, so $f_1 = f_2 = x + c$ for $c \neq 0$. The first case has $p(p-1)$ classes and the second case has $p-1$ classes. Therefore, there are $p^2 - 1$ conjugacy classes in G.

In the first case, the representation is given by $\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$, where $a \in F$ and $0 \neq b \in F$. In the second case, the representation is given by $\begin{pmatrix} -c & 0 \\ 0 & -c \end{pmatrix}$ where $0 \neq c \in F$.

Remark 4.7.7. *Let V be a vector space as an R-module with operator $S : V \to V$. Consider $\{f \in R : f \cdot V = 0\}$, i.e. having $f(S)(V) = 0$. This set is called the annihilators of V, denoted* ***Ann***$(V) \subseteq R$ *as an ideal. Hence, it can be generated by one element $0 \neq f_{min} \cdot R$ which is monic. This is called the minimal polynomial.*

Note that $f_{min} \cdot V = 0$, and if $g \cdot V = 0$ is annihilator, then $f_{min} \mid g$.

Now, the invariant factors of V are $f_1, f_2, \cdots, f_s$ and $V = \coprod_{i=1}^{s} R/f_iR$ and $Ann(R/f_iR) = f_iR$, where $f_1 \mid f_2 \mid \cdots \mid f_s$. In particular, $f_{min} = f_s$.

Example 4.7.8. *Classify 4×4 matrices over $\mathbb{R}$ such that $(A - 3I)^2 = 0$.*

The invariant factors of V should look like $f_1, \cdots, f_s$. Now, $f_s = f_{min} \mid (x-3)^2$. Moreover, the sum of degrees of invariant factors are just 4.

If $f_s = (x-3)^2$, then the collection can be $\{(x-3)^2, (x-3)^2\}$ or $\{x-3, x-3, (x-3)^2\}$. If $f_s = x - 3$, then the collection should be $\{x-3, x-3, x-3, x-3\}$.

For $\{(x-3)^2, (x-3)^2\}$, the corresponding matrix is given by $\begin{pmatrix} 0 & -9 & 0 & 0 \\ 1 & 6 & 0 & 0 \\ 0 & 0 & 0 & -9 \\ 0 & 0 & 1 & 6 \end{pmatrix}$. For $\{x-3, x-3, (x-3)^2\}$, the corresponding matrix is given by $\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & -9 \\ 0 & 0 & 1 & 6 \end{pmatrix}$. For

$\{x-3, x-3, x-3, x-3\}$, *the corresponding matrix is given by* $\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$.

Therefore, every matrix satisfying the conditions in the example is similar (conjugate) to one of these three matrices.

Remark 4.7.9. *Suppose A has invariant factors $f_1, f_2, \cdots, f_s$. Then*

1. $f_1 \mid f_2 \mid \cdots \mid f_s$.

2. $\prod f_i = p_A$.

3. $f_s = f_{min}$.

4. p_A *and* f_s *has the same irreducible factors. It follows that* $f_{min} \mid p_A$.

5. *The invariant factors of A does not depend on the base field. In particular, if $L \supseteq F$ are fields, then the invariant factors of A over F should be the same as the invariant factors of A over L.*

Example 4.7.10. *Let A and B be matrices of F, with $L \supseteq F$. Then $A \sim B$ over F if and only if $A \sim B$ over L.*

4.8 Jordan Canonical Form

Even though we haven't really talked about elementary divisors, they are particularly useful in Jordan canonical form.

Recall that for $A : V \to V$, $\lambda \in F$ is an eigenvalue of A if $Av = \lambda v$ for some $0 \neq v \in V$. (They are exactly the roots of the characteristic polynomial p_A.) Every $v \in V$ such that $Av = \lambda v$ is called an eigenvector of A for the eigenvalue λ. We then have $E_\lambda = \{\text{eigenvalues of } A\} \subseteq V$ called the eigenspace of A with respect to λ.

Proposition 4.8.1. *The following are equivalent:*

1. *A is diagonalizable.*

2. *There exists a basis of eigenvectors.*

3. *V is a direct sum of all eigenspaces, i.e. $V = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$.*

4. *All elementary divisors of A are linear.*

5. *All invariant factors of A are products of distinct linear polynomials;*

6. *f_{min} is a product of distinct linear polynomials.*

In this case, the characteristic polynomial is split, i.e. it is a product of linear factors.

Proof. Linear Algebra. □

Example 4.8.2. *The following are equivalent:*

1. *V is cyclic.*

2. *The set of invariant factors is a singleton $\{f\}$. In particular, $p_A = f$.*

3. *$f_{min} = p_A$.*

4. *All elementary divisors are pairwise relatively prime.*

Let $S : V \to V$ be a linear operator. Assume that p_S is split, so $p_S(x) = \prod_{i=1}^{n}(x - \lambda_i)$ where $n = \dim(V)$. As the product of elementary divisors is p_S, then every elementary divisor is of the form $(x-\lambda)^k$, where $\lambda = \lambda_i$ for some i. Then we examine the cyclic summand $M = R/(x-\lambda)^k R$ where R is the polynomial ring. We would like to find a basis of the vector space. An obvious basis is $\bar{1}, \bar{x}, \bar{x}^2, \cdots, \bar{x}^{k-1}$ for M. Another basis is $\bar{1}, \overline{x-\lambda}, \cdots, \overline{(x-\lambda)^{k-1}}$, where we consider $y = x - \lambda$. In particular, $x \cdot \overline{(x-\lambda)^i} = (x-\lambda)\overline{(x-\lambda)^i} + \lambda\overline{(x-\lambda)^i} = \overline{(x-\lambda)^{i+1}} + \lambda(x \bar{-} \lambda)^i$, and $\overline{(x-\lambda)^k} = 0$, so $x\overline{(x-\lambda)^{k-1}} = \lambda \cdot \overline{(x-\lambda)^{k-1}}$. Now the matrix S in the new basis is given by
$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & \lambda \end{pmatrix}.$$
This matrix is denoted $J(\lambda, k)$, which is a $j \times j$ with respect to eigenvalue λ, and is called a Jordan block.

Theorem 4.8.3 (Jordan Canonical Form)**.** *Let $S : V \to V$ be a linear operator in a finite-dimensional vector space V. Assume that the characteristic polynomial p_S is split. Then there is a basis $\mathcal{C}$ for V such that $[S]_{\mathcal{C}} = diag(J(\lambda_1, k_1), J(\lambda_2, k_2), \cdots, J(\lambda_s, k_s))$. The Jordan blocks $J(\lambda_i, k_i)$ are uniquely determined up to permutation. The matrix is called the Jordan canonical form of S.*

5 Field Theory

5.1 Field Extensions

Proposition 5.1.1. *Every field homomorphism is injective.*

Proof. Suppose $\alpha : F \to K$ is a field homomorphism, then $\ker(\alpha) \subset F$ is a non-trivial ideal. Therefore, α is injective. □

Remark 5.1.2. *In particular, F is isomorphic to the subfield $\alpha(F) \subseteq K$.*

Definition 5.1.3 (Field Extension)**.** *Let $F \subseteq K$ be a subfield. We say that K is an extension of F and write K/F.*

If K/F is a field extension, then $F \hookrightarrow K$ is an embedding, i.e. an injective field homomorphism. Conversely, if $\alpha : F \to K$ is a field homomorphism, then we can identify F as a subfield of K. Specifically, we have $F \cong \alpha(F) \subseteq K$, and $K/\alpha(F)$ is a field extension, i.e. K/F is a field extension.

There is an obvious category of fields, which is a subcategory of the category of rings. However, we can get a different taste of a category on fields.

Definition 5.1.4 (Category of Field Extensions)**.** *Let F be a field. The category of field extensions of F has objects as field extensions K/F and morphisms from K/F to L/F is a field homomorphism $\alpha : K \to L$ that is the identity homomorphism on subfield F, i.e. $\alpha(x) = x$ for all $x \in F$.*

Equivalently, the objects are field homomorphisms $F \to K$ for fixed F, and morphisms between two field homomorphisms $F \to K$ and $F \to L$ are field homomorphisms $K \to L$ such that the related diagrams commute:

$$\begin{tikzcd}
 & F \arrow[dl] \arrow[dr] & \\
K \arrow[rr, "\alpha"'] & & L
\end{tikzcd}$$

We denote this category as Fields/F.

Suppose K/F is a field extension, then K is a module over itself, and is then a module over F (as a vector space). We denote $[K : F] = \dim_F(K)$ as the degree of K over F.

Example 5.1.5. 1. *$[K : F] = 1$ if and only if $K = F$, and we call F/F as the trivial extension.*

2. *$\mathbb{C}/\mathbb{R}$ has a basis $\{1, i\}$ for $\mathbb{C}$ over $\mathbb{R}$, so $[\mathbb{C} : \mathbb{R}] = 2$.*

3. *Note $[\mathbb{R} : \mathbb{Q}] = \infty$ because the extension does not have a finite basis.*

Proposition 5.1.6. *Let $L/K/F$ be field extensions. Then $L : K] = [L : K] \cdot [K : F]$. We can read this even if some terms are ∞. In particular, the extension L/F is finite if and only if L/K and K/F are finite.*

Proof. Let us choose a basis $\{x_i\}_{i\in I}$ for K/F, so $x_i \in K$, and another basis $\{y_j\}_{j\in J}$ for L/K, so $x_j \in L$.

Claim 5.1.7. *$\{x_i y_j\}_{i\in I, j\in J}$ is a basis for L/F.*

Subproof. Suppose $\sum\limits_{x\in I, j\in J} a_{ij}x_i y_j = 0$ for $a_{ij} \in F$. Now $\sum\limits_{y\in J}(\sum\limits_{i\in I} a_{ij}x_i)y_j = 0$ where $\sum\limits_{i\in I} a_{ij}x_i \in K$. However, since y_j's are linearly independent over K, then $\sum\limits_{i\in I} a_{ij}x_i = 0$ for all j, and since x_i's are linearly independent over F, then $a_{ij} = 0$ for all i, j. Hence, they are linearly independent. We now have to show that they generate the whole space.

Let $v \in L$, because y_j's generate L over K, then $v = \sum\limits_{j\in J} u_j y_j$ for some $u_j \in K$. Now since x_i's generate K over F, then every $u_j = \sum\limits_{x\in I} a_{ij}x_i$ for some $a_{ij} \in F$. Now $v = \sum\limits_{i,j} a_{ij}x_i y_j$. This concludes the proof of the claim. ■

The statement automatically follows from the claim.

□

Corollary 5.1.8. *If $L/K/F$ are finite, then $[K : F] \mid [L : F]$ and $[L : K] \mid [L : F]$.*

Example 5.1.9. *For $L/K/F$, suppose $[L : F] = p$ is prime, so either $[K : F] = 1$ or $[L : K] = 1$, so either $K = F$ or $L = K$.*

Corollary 5.1.10. *If $F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$ is a tower of field extensions, then $[F_n : F_1] = \prod\limits_{i=1}^{n-1} [F_{i+1} : F_i]$.*

Lemma 5.1.11. *Let K be a field and $S \subseteq K$ is a subset. Then there is a unique smallest subfield of K containing S.*

Proof. Take the intersection of all subfields of K containing S. Note that this is still a field. □

Definition 5.1.12. *Let K/F be a field extension and $T \subseteq K$ is a subset. Denote set $S = T \cup F$. We can denote $F(T)$ as the smallest subfield of K containing S. Note that $F \subseteq F(T) \subseteq K$, then $F(T)$ is the smallest subfield of K containing F and T, and called the field generated by T over K.*

Suppose T is finite, i.e. $T = \{\alpha_1, \cdots, \alpha_n\}$. Then we can write $F(T) = F(\alpha_1, \cdots, \alpha_n)$.

Lemma 5.1.13. *Let K/F be a field extension, and let $\alpha_1, \cdots, \alpha_n \in K$. Then*

$$F(\alpha_1, \cdots, \alpha_n) = \{\frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)} : f(\alpha_1, \cdots, \alpha_n), g(\alpha_1, \cdots, \alpha_n) \in F[x_1, \cdots, x_n], g(\alpha_1, \cdots, \alpha_n) \neq 0\}.$$

Proof. Let L denote the set on the right hand side. Note that L is a field containing F. By definition, $F(\alpha_1, \cdots, \alpha_n) \subseteq L$.

On the other hand, note $\alpha_i = \frac{\alpha_i}{1} \in F(\alpha_1, \cdots, \alpha_n)$, then $\frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)} \in F(\alpha_1, \cdots, \alpha_n)$, and so $L \subseteq F(\alpha_1, \cdots, \alpha_n)$. □

We can now define a similar structure.

Definition 5.1.14. *For K/F field extension, let $\alpha_1, \cdots, \alpha_n \in K$, then $F[\alpha_1, \cdots, \alpha_n] = \{f(\alpha_1, \cdots, \alpha_n : f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]\}$ is a ring (and may not be a field).*

Note that $F \subseteq F[\alpha_1, \cdots, \alpha_n] \subseteq F(\alpha_1, \cdots, \alpha_n)$.

Remark 5.1.15. *$F[\alpha_1, \cdots, \alpha_n] = F(\alpha_1, \cdots, \alpha_n)$ if and only if $F[\alpha_1, \cdots, \alpha_n]$ is a field.*

Example 5.1.16.

1. *Let x be a variable over F. So $F \subseteq F[x] \subseteq F(X) = K$, so $F[x]$ is the polynomial ring (but not a field), and $K = F(x)$ is the ring of rational functions, which is a field. Here $T = \{x\}$.*

2. *Consider $\mathbb{C}/\mathbb{R}$. Take $T = \{i\}$. Then $\mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}$ is a field, and so $\mathbb{R}[i] = \mathbb{C} = \mathbb{R}(i)$.*

Definition 5.1.17 (Algebraic, Transcendental)**.** *Suppose K/F is a field extension, then $\alpha \in K$ is called algebraic over F if there exists a nonzero polynomial $f \in F[x]$ such that $f(\alpha) = 0$.*

If α is not algebraic, then α is called transcendental over F.

A field extension K/F is algebraic if every element $\alpha \in K$ is algebraic over F.

Example 5.1.18. *1. $\alpha \in F$ is algebraic over F, because $x - \alpha \in F[x]$.*

2. Suppose $\alpha \in L/K/F$. If α is algebraic over F, then α is algebraic over K: $f \in F[x] \subseteq K[x]$.

3. If $\alpha \in K$ is transcendental over F, then $F[\alpha] \cong F[x]$. More precisely, $F[x] \to F[\alpha]$ sending $g \mapsto g(\alpha)$ is an isomorphism. Moreover, $F(x) \cong F(\alpha)$, and α plays the role of a variable.

4. $x \in F(x)$ is transcendental over F.

Theorem 5.1.19. *Let $\alpha \in K/F$ be algebraic over F. Then*

1. *There is a unique monic irreducible polynomial $m_\alpha \in F[x]$ such that $m_\alpha(\alpha) = 0$.*

2. *If $f(\alpha) = 0$ for $f \in F[x]$, then $m_\alpha \mid f$.*

3. *The elements $1, \alpha, \alpha_2, \cdots, \alpha^{n-1}$, where $n = \deg(m_\alpha)$ form a basis for the extension $F(\alpha)$ over F. In particular, $[F(\alpha) : F] = \deg(m_\alpha)$.*

4. *$F(\alpha) = F[\alpha]$. In particular, this holds if and only if α is algebraic.*

Proof. Consider $\varphi : F[x] \to K$ given by $\varphi(g) = g(\alpha)$. Then $\mathrm{im}(\varphi) = F[\alpha]$. Now $\ker(\varphi) \subseteq F[x]$ is a nonzero ideal, and is generated by one element, i.e. $\ker(\varphi) = m_\alpha \cdot F[x]$, where m_α is monic. Now every $f \in F[x]$ such that $f(\alpha) = 0$ is contained in $f \in \ker(\varphi)$, and so $m_\alpha \mid f$. This proves 2). Now, the factor ring $F[x]/m_\alpha \cdot F[x] \cong \mathrm{im}(\varphi) \subseteq K$ as a subring. Since K is a field, then it is a domain, and so $\mathrm{im}(\varphi)$ is a domain, so the factor ring is a domain, and so the ideal is prime, hence m_α is irreducible. This proves 1). For the map $F[x]/m_\alpha \cdot F[x] \to \mathrm{im}(\varphi) \subseteq K$, we have that $\bar{x} \mapsto \alpha$. We know that $\bar{1}, \bar{x}, \cdots, \bar{x}^{n-1}$ is a basis of the factor ring, and so it is a basis for the image of φ. In particular, $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ forms a basis for $F[\alpha]$ over F. Because $m_\alpha \cdot F[x]$ is a nonzero prime ideal, so it is maximal. Hence, the factor ring is a field, and so the image $F(\alpha) = \mathrm{im}(\varphi)$ is a field. Therefore, $F[\alpha] = F(\alpha)$. □

Remark 5.1.20. *This unique monic irreducible polynomial m_α is called the minimal polynomial of α over F. The degree of the extension is then determined by the degree of the minimal polynomial. The degree of this element α is just the degree of the polynomial, i.e.* $\deg(\alpha) = \deg(m_\alpha)$.

Remark 5.1.21. *Given $\alpha \in K/F$, we want to know how to find the minimal polynomial. In particular, we want to find some polynomial $f \in F[x]$ such that $f(\alpha) = 0$. Moreover, if f is not irreducible, i.e. $f = gh$ as monic non-constant polynomials, then either $g(\alpha) = 0$ or $h(\alpha) = 0$, and by continuing the factorization, we can find the minimal polynomial.*

We saw before that $F(\alpha) \cong F[x]/m_\alpha \cdot F[x]$. We can reverse the procedure as follows: suppose $m \in F[x]$ is a monic irreducible polynomial, then it generates prime (and therefore maximal) ideal. Therefore, the residual ring $F[x]/m \cdot F[x]$ is a field because the ideal is maximal. Moreover, consider $F \hookrightarrow F[x]/m \cdot F[x]$ which is an embedding. If we denote $K = F[x]/m \cdot F[x]$, then K/F is a field extension. Take $\alpha = \bar{x} \in K$. Then $m(\alpha) = 0$, and m is monic irreducible, therefore $m = m_\alpha$ is the minimal polynomial of α. Moreover, α generates the field: $F[\alpha] = K = F(\alpha)$. The extension degree is thus given by $[K : F] = \deg(m)$.

Example 5.1.22.

1. *$\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i)$ where $i^2 + 1 = 0$. The polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, therefore, this is isomorphic to the factor ring $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$. The degree of i is the degree of the polynomial, which is 2.*

2. *What is $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$? Note that $\sqrt{3}$ is a root of $x^2 - 3$ over $\mathbb{Q}$, which is a irreducible polynomial, so the degree of extension is 2, with $\deg(\sqrt{3}) = 2$. Degree 2 extensions are also called quadratic extensions.*

3. *Let p be a prime integer. Denote $\xi_p = \cos(\frac{2\pi}{p}) + i \cdot \sin(\frac{2\pi}{p})$ where $(\xi_p)^p = 1$ and $\xi_p \neq 1$. In particular, ξ_p is a root of $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, and therefore it is a root of $x^{p-1} + \cdots + x + 1$. By Eisenstein's criterion, this polynomial is irreducible over $\mathbb{Q}$, so it is the minimal polynomial of ξ_p, i.e. $m_{\xi_p} = x^{p-1} + \cdots + x + 1$, and $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.*

Corollary 5.1.23. *Let $\alpha \in K/F$. Then α is algebraic over F if and only if $[F(\alpha) : F]$ is finite.*

Proof. $(\Rightarrow)$ is true by the theorem.

$(\Leftarrow)$: consider the elements $1, \alpha, \alpha^2, \cdots, \alpha^n$ which are linearly dependent for large enough n, i.e. $n \geq [F(\alpha) : F]$. Therefore, $\sum_{i=0}^{n} a_i \alpha^i = 0$ for some nontrivial combination $a_i \in F$. Therefore, α is algebraic over F. □

Corollary 5.1.24. *A finite field extension is algebraic, i.e. all elements in this extension are algebraic over the base field.*

Proof. Take $\alpha \in K/F$. The extension generated is $F(\alpha) \subseteq K$ and with $[K : F] < \infty$. Therefore, $[F(\alpha) : F] < \infty$. By the previous corollary, α is algebraic over F. □

Corollary 5.1.25. *Let $\alpha_1, \cdots, \alpha_n \in K/F$ be algebraic over F. Then $F(\alpha_1, \cdots, \alpha_n) = F[\alpha_1, \cdots, \alpha_n]$, and this is a finite field extension of F. In particular, $F(\alpha_1, \cdots, \alpha_n)/F$ is algebraic.*

Proof. The last statement simply follows the first two statements. We now prove by induction on n.

Case $n = 1$: this is true by the theorem.

Suppose this is true for case $n-1$, we now show the case at n. Now α_n is algebraic over F, and so it is algebraic over $F(\alpha_1, \cdots, \alpha_{n-1})$, which is equivalent to $F[\alpha_1, \cdots, \alpha_{n-1}]$ by induction hypothesis. Therefore, we know that $F(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n) = F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1, \cdots, \alpha_{n-1})[\alpha_n] = F[\alpha_1, \cdots, \alpha_{n-1}][\alpha_n] = F[\alpha_1, \cdots, \alpha_n]$ by induction.

Therefore, we obtain the extension $F(\alpha_1, \cdots, \alpha_n)/F(\alpha_1, \cdots, \alpha_{n-1})/F$, which are both finite, and so the tower of finite extension is finite. □

Theorem 5.1.26. *Let K/F be a field extension. Then the set $E \subseteq K$ of all algebraic over F elements is a subfield of K containing F.*

Proof. Suppose $\alpha, \beta \in E$, then $F(\alpha, \beta)/F$ is an algebraic extension. Note that $\alpha + \beta, \alpha\beta, \alpha^{-1} \in F(\alpha, \beta)/F$, and so E is generated as a field. □

Theorem 5.1.27. *Let L/K and K/F be field extensions. Then L/F is algebraic if and only if L/K and K/F are algebraic.*

Proof. ($\Rightarrow$): since $K \subseteq L$, then K/F is algebraic. Take $\alpha \in L/F$, then it is algebraic, so $\alpha \in L/K$ is also algebraic.

($\Leftarrow$): take $\alpha \in L$. By assumption, it is algebraic over K. Now there exists nonzero polynomial $f = \sum\limits_{i=0}^{n} \beta_i x^i \in K[x]$ such that $f(\alpha) = 0$. Take $E = F(\beta_1, \cdots, \beta_n)$, which is generated by finitely many algebraic elements over F, so it is algebraic over F. In particular, $[E : F] < \infty$. Note that $\alpha \in L$ is algebraic over E since $f \in E[x]$, and so $[E(\alpha) : E] < \infty$. Therefore, $[F(\alpha) : F] \leq [E(\alpha) : F] = [E(\alpha) : E] \times [E : F]$, but both field extension degrees are finite, so α is algebraic over F. □

Property 5.1.28. *A property $\mathcal{P}$ of field extensions is "good" if for field extensions $L/K/F$, $\mathcal{P}(L/F)$ holds if and only if $\mathcal{P}(L/K)$ and $\mathcal{P}(K/F)$ hold.*

In particular, the algebraic property $\mathcal{P} =$ algebraic is good.

Theorem 5.1.29. *Let $f \in F[x]$ be a non-constant polynomial. Then there exists a field extension K/F such that $[K : F] \leq \deg(f)$ and f has a root in K.*

Proof. We proved the case when f is irreducible. For general f, there exists a irreducible polynomial $g \mid f$. Then take $K = F[x]/gF[x]$, then g has a root in K, and hence f has a root in K and the degree of extension $[K : F] = \deg(g) \leq \deg(f)$. □

Corollary 5.1.30. *Let $f \in F[x]$ be a non-constant polynomial. Then there is a field extension K/F such that $[K : F] \leq \deg(f)!$ and f is split over K.*

Proof. This can be done by induction on the degree of f. It is trivial if the degree is 1: take $K = F$. For the induction step, by the theorem, we find a field extension L/F such that $[L : F] \deg(f)$ and f has a root $\alpha \in L$. Then we write $f = (x - \alpha) \cdot g$, so $g \in L[x]$ has degree $\deg(g) = \deg(f) - 1$. By induction, there exists a field extension K/L such that g is split over K and $[K : L] \leq \deg(g)!$. Therefore, f is split over K and $[K : F] = [K : L] \times [L : F] \leq \deg(g)! \times \deg(f) \leq \deg(f)!$. □

Definition 5.1.31 (Splitting Field)**.** *Let $f \in F[x]$ be a non-constant polynomial. A field extension K/F is called a splitting field of f (over F) if*

1. *f is split over K, i.e. $f = a \cdot (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ where $a \in F$ and $\alpha_i \in K$ are all roots of f in K.*

2. *$K = F(\alpha_1, \cdots, \alpha_n)$.*

Example 5.1.32.

1. *If f is split over F, then F/F is a splitting field.*

2. *Suppose $f = x^3 - 1$ over $F = \mathbb{Q}$. Note $x^3 = (x - 1)(x^2 + x + 1)$, where $x^2 + x + 1$ is irreducible over F. The roots are exactly $\frac{-1 \pm \sqrt{-3}}{2}$. Therefore, $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is the splitting field for f.*

Proposition 5.1.33. *A non-constant polynomial $f \in F[x]$ has a splitting field of degree at most* $\deg(f)!$.

Proof. Similar as above, we find a field extension K/F of degree at most $\deg(f)!$ such that f is split over K. Let $\alpha_1, \cdots, \alpha_n$ are roots of f in K. Then $L = F(\alpha_1, \cdots, \alpha_n)$ is a splitting field and $L \subseteq K$. Therefore, $[L : K] \leq \deg(f)!$. □

Remark 5.1.34. *If K/F is a field extension such that f is split over K, then K contains a unique splitting field of F. Indeed, the field is the only splitting field inside K.*

Remark 5.1.35 (Irreducibility of polynomials of small degree)**.** *If* $\deg(f) = 2$ *and* α *is a root of* f*, then* $f = (x - \alpha)(ax + b)$*, so* f *is split. Therefore, a degree* 2 *polynomial* f *is split, if and only if* f *has a root, if and only if* f *is not irreducible. Similar results hold for polynomials of degree* 3*.*

Definition 5.1.36. *Suppose* K/F *and* K_1/F_1 *are two field extensions. Suppose we have a field homomorphism* $\varphi : F \to F_1$*. A field homomorphism* $\psi : K \to K_1$ *is called an extension of* φ *if* $\psi(a) = \varphi(a)$ *for all* $a \in F$*.*

Suppose further that $f = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$*. We can denote* $\varphi(f) = \varphi(a_n) \cdot x^n + \cdots + \varphi(a_1) \cdot x + \varphi(a_0) \in F_1[x]$*.*

Proposition 5.1.37. *Let* $K = F(\alpha)/F$ *be a finite field extension. Let* $f = m_\alpha \in F[x]$ *be the minimal polynomial of* α*. Suppose* $\varphi : F \to F_1$ *is a field homomorphism and* K_1/F_1 *is a field extension as above. Then*

1. *if* $\psi : K \to K_1$ *is an extension of* φ*, then* $\psi(\alpha)$ *is a root of the polynomial* $\varphi(f) \in F_1[x]$*.*
2. *For any root* α_1 *of* $\varphi(f)$ *in* K_1*, there exists a unique extension* $\psi : K \to K_1$ *of* φ *such that the image* $\psi(\alpha) = \alpha_1$*.*

Proof.

1. Since $f(\alpha) = 0$, we denote $f = a_n x^n + \cdots + a_1 x + a_0$ for $a_i \in F$ and apply ψ and get $\varphi(f)(\psi(f)) = 0$, therefore $\psi(\alpha)$ is a root of $\varphi(f)$.
2. Let $\psi' : F[x] \to K_1$ be the evaluation of polynomial at α_1, i.e. $\psi'(g) = \varphi(g)(\alpha_1)$, then $\psi'(f) = \varphi(f)(\alpha_1) = 0$. Therefore, $f \in \ker(\psi')$. Hence, ψ' factors $\psi : F[x]/f \cdot F[x] \to K_1$. Note that $F[x]/f \cdot F(x) \cong K = F(\alpha)$, so $\psi(\alpha) = \psi'(x) = \alpha_1$.

□

Corollary 5.1.38. *Given the setting in the proposition above, the number of extensions of* φ *is at most* $\deg(f) = \deg(\alpha) = [K : F]$*.*

Theorem 5.1.39. *Let* K/F *be a splitting field of a nonconstant polynomial* $f \in F[x]$ *and* $\varphi : F \to F_1$ *is a field isomorphism. Let* K_1/F_1 *be a splitting field of* $\varphi(f) \in F_1[x]$*. Then there exists a field isomorphism* $\psi : K \to K_1$ *that extends* φ*.*

Proof. We prove by induction on $n = \deg(f)$.

If $n = 1$, then the polynomial is linear and thus split, so $K = F$ and $K_1 = F_1 <$ then $\psi = \varphi$.

Suppose the theorem is true for case $n-1$, we want to show the case for n. Let $\alpha \in K$ be a root of f. Therefore, $f = (x-\alpha)\cdot g$ for some $g \in F(\alpha)[x]$. Let m_α be the minimal polynomial of α over F. In particular, $m_\alpha \mid f$. Therefore, $\varphi(n_\alpha) \mid \varphi(f)$. Since $\varphi(f)$ is split over K_1 by assumption, then $\varphi(m_\alpha)$ is also split over K_1. Take a root α_1 of $\varphi(m_\alpha)$ in K_1. By the proposition above, there exists a field homomorphism $\varphi' : F(\alpha) \to F_1(\alpha_1)$ extending φ such that $\varphi(\alpha) = \alpha_1$. The map φ' is clearly surjective because α is mapped to α_1. It is also injective since it is a field homomorphism. Therefore, φ' is a field isomorphism. Now $\varphi(f) = \varphi'((x-\alpha)\cdot g) = \varphi'(g)$, so $\varphi'(g) \in F_1(\alpha_1)[x]$. Observe that $g \mid f$ is split over K because f is split over K. Moreover, the roots of f in K are the same as the roots of $g \cup \{\alpha\}$. Therefore, the field K is generated by all roots of g in K over $F(\alpha)$, since K is generated over F by all roots of f. Therefore, $K/F(\alpha)$ is a splitting field of g. Similarly, $K_1/F_1(\alpha_1)$ is a splitting field of $\psi'(g)$ for $\psi' : F(\alpha \xrightarrow{\cong} F_1(\alpha_1)$. By applying the inductive hypothesis over $\psi' : F(\alpha) \to F_1(\alpha_1)$ with $g \in F(\alpha)[x]$, we conclude that ψ' extends to an isomorphism of splitting fields $\psi : K \xrightarrow{\cong} K_1$. Since ψ extends to ψ' and ψ' extends to φ, then ψ extends to φ. □

Remark 5.1.40. *We can restate the theorem as the following. For a base field F, there is a category of field extensions over F. Two elements of this category are K/F and K_1/F. Then K/F and K_1/F are isomorphic if there exists $\psi : K \to K_1$ such that $\psi(a) = a$ for all $a \in F$. Equivalently, we say that ψ extends the identity isomorphism from F to itself.*

Theorem 5.1.41. *Let $f \in F[x]$ be a non-constant polynomial and K/F and K_1/F are two splitting fields of the polynomial. Then K/F and K_1/F are isomorphic over F.*

Proof. Apply the previous theorem to the case where $\varphi = \mathbf{id}_F$ and $F_1 = F$. □

5.2 Finite Fields

Definition 5.2.1 (characteristic). *The characteristic of a field F is the smallest positive integer n such that the n-term summation of 1_F is 0_F. If this smallest positive integer exists, then the field has characteristic n; if not, then we say the field has characteristic 0.*

Remark 5.2.2. *Let F be an arbitrary field. Note that $\mathbb{Z}$ is an initial object in the category of rings, then there exists a unique morphism $f : \mathbb{Z} \to F$ that maps $1_{\mathbb{Z}} \to 1_F$. We also have $\mathbb{Z}/\ker(f) \cong im(f) \subseteq F$. Note that the image of f is a domain, so $\ker(f)$ is a prime ideal in $\mathbb{Z}$. Therefore, either*

1. $\ker(f) = 0$, *so characteristic of* F *is char*$(F) = 0$, *with* $\mathbb{Z} \subseteq F$. *This means that the summation of* n *terms of* 1_F *is always nonzero for all positive integer* n.

   Note that if we take $0 \neq n \in \mathbb{Z}$, *then* $n^{-1} \in F$, *so we can consider fractions and then extends* $\mathbb{Z}$ *to* $\mathbb{Q}$ *as a field. Hence,* $\mathbb{Q}$ *is the smallest subfield (also called the prime subfield) of any field* F.

2. $\ker(f) = p\mathbb{Z}$ *where* p *is prime. Then we say the characteristic of* F *is char*$(F) = p$ *(with similar reasoning as above), and therefore* $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$ *is the smallest subfield (also called the prime subfield) of any field* F.

Therefore, if a field F *has characteristic* 0, *then it contains* $\mathbb{Q}$ *as the smallest subfield; if a field* F *has characteristic* p, *then it contains* $\mathbb{Z}/p\mathbb{Z}$ *as the smallest subfield.*

In particular, $\mathbb{Z}/p\mathbb{Z}$ *has characteristic* $\mathbb{Z}$. *Therefore, it does not contain a non-trivial subfield.*

Moreover, notice that a field either has characteristic p *for some prime* p, *or has characteristic* 0.

Remark 5.2.3 (Freshman's Dream, Frobenius Homomorphism)**.** *When a field has characteristic* p, *then* $(a+b)^p = a^p + b^p$ *for all* $a, b \in F$.

Therefore, the map $f : F \to F$ *given by* $f(x) = x^p$ *in such field* F *is an injective field homomorphism:* $f(a+b) = (a+b)^p = a^p + b^p = f(a) + f(b)$ *and* $(ab)^p = a^p b^p$. *This is called the Frobenius homomorphism.*

Also note that $(a+b)^{p^k} = a^{p^k} + b^{p^k}$.

Definition 5.2.4 (Multiplicity, Simple Root, Derivative)**.** *Let* $f \in F[x]$ *be a polynomial where* F *is a field of positive characteristic. Suppose* $\alpha \in F$ *is a root of* f, *then* $f(\alpha) = 0$. *Therefore,* $f = (x-\alpha)^k \cdot h$ *for some* $h \in F[x]$ *and some positive integer* k *such that* $h(\alpha) \neq 0$. *This number* k *is called the multiplicity of* α. *In particular, if* $k = 1$, *then* α *is called a simple root of* f.

Suppose we denote $f = a_n x^n + \cdots + a_1 x + a_0$ *for some* $a_i \in F$. *Then the derivative of* f *is denoted* $f' = a_n \cdot n x^{n-1} + \cdots + a_1$. *In particular, note that* $(f+g)' = f' + g'$ *and* $(fg)' = f'g + fg'$.

Lemma 5.2.5. *Let* $f \in F[x]$ *be a polynomial over* F *and* $\alpha \in F$ *is a root of* f. *Then* α *is a simple root of* f *if and only if* $f'(\alpha) \neq 0$.

Proof. We write $f = (x-\alpha) \cdot g$ and compute the derivative. Note that $f' = g + (x-\alpha) \cdot g'$, then $f'(\alpha) = g(\alpha)$. This is nonzero if and only if α is simple. □

Definition 5.2.6 (Greatest Common Divisor)**.** *The greatest common divisor of two polynomials f and g is a monic polynomial h of the highest possible degree such that $h \mid f$ and $h \mid g$. We denote it $\gcd(f,g) = h$. In particular, when considering constant polynomials, this notion is exactly the same one as the conventional definition.*

Corollary 5.2.7. *If $\gcd(f, f') = 1$, then every root of f is simple.*

Proof. If α is a root of f, then $x-\alpha \mid f$, so $x-\alpha \nmid f'$, hence $f'(\alpha) \neq 0$, so α is simple. □

Remark 5.2.8. *If $\gcd(f, f') = 1$, and K/F is a field extension, then f and f' are still relatively prime over K, hence all roots of f over K are simple over a splitting field: $f = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where all α_i are distinct.*

Definition 5.2.9. *A finite field F is a field of finitely many elements.*

Remark 5.2.10. *The characteristic of a finite field F is a positive prime $p > 0$. Then there is a prime subfield $F_0 \subseteq F$, which is $F_0 \cong \mathbb{Z}/p\mathbb{Z}$. Moreover, if we denote $[F : F_0] = n$, then $x_1, x_2, \cdots, x_n$ can form a basis for F/F_0. Therefore, $F = \{\sum_{i=1}^{n} a_i x_i, a_i \in F_0\}$. Hence, $|F| = p^n$. Therefore, a finite field must have order p^n for some p and some n.*

Theorem 5.2.11. *For any prime integer p and integer $n > 0$, there exists a finite field F with exactly p^n elements. Moreover, every two such finite fields are isomorphic.*

Proof. We write $q = p^n$. We first show the existence. Consider the polynomial $f = x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$. Let F be a splitting field of f over $\mathbb{Z}/p\mathbb{Z}$. Let S be the set of all roots of f in F, so $S \subseteq F$. Note $f = qx^{q-1} - 1 = -1$ since $q = 0$ in $\mathbb{Z}/p\mathbb{Z}$, so $\gcd(f, f') = 1$. Therefore, all the roots of f in F are simple. Hence, $|S| = q$. Suppose α, β are roots of f, i.e. $\alpha^q = \alpha$ and $\beta^q = \beta$. Hence, $\alpha+\beta$ and $\alpha\beta$ are also roots. Moreover, for $\alpha \neq 0$, α^{-1} is also a root. Hence, the set of roots $S \subseteq F$ is a subfield of F, consisting of all the roots. Since F is generated by all the roots, then $S = F$. But that means $|F| = q$. Therefore, we always have a field of p^n elements. In fact, $x^q - x = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_q)$ over F, so $F = \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$.

We now show its uniqueness. Denote $|F| = q = p^n$, so $|F^\times| = q-1$, so $x^{q-1} = 1$ for all $x \in F^\times$. Therefore, $x^q = x$ for all $x \in F$. Hence, all elements of F are roots of $f = x^q - x$. This means f is split over F. Moreover, F is generated by all the roots, then this means $F/(\mathbb{Z}/p\mathbb{Z})$ is a splitting field of f. However, the splitting field is unique up to isomorphism. Therefore, every two fields of order q are isomorphic. □

Since finite fields of a certain order are uniquely determined, we denote $\mathbb{F}_q$ to be a field of q elements for $q = p^n$, uniquely up to isomorphism.

Example 5.2.12. *1.* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

2. $\mathbb{F}_{p^2} \neq \mathbb{Z}/p^2\mathbb{Z}$. *For example,* $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)\mathbb{F}_2[x]$*, where* x^2+x+1 *is the only irreducible polynomial of degree* 2 *over* $\mathbb{F}_2$*. Let* $\alpha = \bar{x}$*, then* $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$*. Notice that* $\alpha(\alpha + 1) = \bar{x}(\bar{x} + 1) = \bar{x}^2 + \bar{x} = 1$ *because* $\bar{x}^2 + \bar{x} + 1 = 0$*. Moreover,* $\alpha^2 = \bar{x}^2 = \bar{x} + 1 = \alpha + 1$*. Therefore,* $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$*.*

Theorem 5.2.13. *Let* F *be a field and* $A \subseteq F^\times$ *is a finite subgroup. Then* A *is cyclic.*

Proof. Note that A is a product of primary components, i.e. $A = \prod_{p \text{ prime}} A[p]$, where $A[p]$ is the product of cyclic groups of the form $\mathbb{Z}/p^k\mathbb{Z}$.

Let us take the set $\{x \in A[p] : x^p = 1\}$. Note that the set has p^a elements, where a is the number of cyclic groups. Note that the elements in this set are roots of $x^p - 1$, so $p^a \leq p$, which means the number of cyclic groups is at most 1, so $A[p]$ is cyclic. By Chinese Remainder Theorem, the product of cyclic groups that are pairwise relatively prime is also cyclic. Hence, A is cyclic. □

Corollary 5.2.14. $\mathbb{F}_q^\times$ *is cyclic. In particular,* $(\mathbb{Z}/p\mathbb{Z})^\times$ *is cyclic.*

Definition 5.2.15 (Simple Field Extension)**.** *A field extension* K/F *is simple if* $\exists \alpha \in K$ *such that* $K = F(\alpha)$*.*

Corollary 5.2.16. *Every finite extension of a finite field is simple.*

Proof. Suppose K/F is an extension such that F is a finite field and K/F is a finite extension. Therefore, K is a finite field. Then $K^\times$ is cyclic, so it is generated by $\alpha \in K^\times$. This implies that $K = F(\alpha) = F[\alpha]$. □

Remark 5.2.17. *For* $q = p^n$ *and* $s = p^m$*, then* $\mathbb{F}_q/\mathbb{F}_s$ *is a field extension if and only if* $m \mid n$*.*

5.3 Normal Extensions

Lemma 5.3.1. *Let* E/F *be a finite field extension, and* $\sigma : F \to L$ *is a field homomorphism. Then there is a finite field extension* M/L *and an extension* $\tau : E \to M$ *over* σ*.*

Proof. Note that $E = F(\alpha_1, \cdots, \alpha_n)$ for $\alpha_i \in E$. We prove the statement by induction on n.

Suppose $n = 1$. Then $E = F(\alpha)$, and we take the minimal polynomial $m_\alpha \in F[x]$. Let M/L be a splitting field of $\sigma(m_\alpha) \in L[x]$. Therefore, this is a finite field extension as well. Now $\sigma(\alpha) = \beta \in M$ is a root of $\sigma(m_\alpha)$. Therefore, there exists a unique extension $\tau : E \to M$ such that $\tau(\alpha) = \sigma(\alpha) = \beta$.

$$\begin{tikzcd}
F(\alpha) \arrow[r, dashed, "\exists!\tau"] \arrow[d, dash] & M \arrow[d, dash] \\
F \arrow[r, "\sigma"'] & L
\end{tikzcd}$$

Now, suppose we have proven the case for $n - 1$, we now prove the case for n. In a similar fashion, we have the diagram

$$\begin{tikzcd}
E = E'(\alpha_1, \cdots, \alpha_{n-1}) \arrow[r, "\tau"] \arrow[d, dash] & M \arrow[d, dash] \\
E' = F(\alpha_n) \arrow[r, "\tau'"] \arrow[d, dash] & M' \arrow[d, dash] \\
F \arrow[r, "\sigma"'] & L
\end{tikzcd}$$

where τ extends σ and the extension M/L is finite. □

Proposition 5.3.2. *Let E/F be a finite field extension. The following are equivalent:*

1. *E is the splitting field of some polynomial f over F.*

2. *For every finite extension M/E and every field homomorphism $\sigma : E \to M$ over F, we have $\sigma(E) = E$.*

3. *Every irreducible polynomial $f \in F[x]$ that has a root in E is split over E.*

Definition 5.3.3 (Normal Extension)**.** *We say an extension is normal if it satisfies all of the above.*

Proof. We first prove that (1) ⇒ (2). Since E is a splitting field of $f \in F[x]$, $E = F(\alpha_1, \cdots, \alpha_n)$ where α_i are all roots of f over E and f is split over E. Now $\sigma(\alpha_i)$ is a root of $\sigma(f) = f$. Therefore, $\sigma(\alpha_i) = \alpha_j$ for some j, so $\alpha_j \in E$. Hence, $\sigma(E) \subseteq E$. Consider $\sigma : E \hookrightarrow E$ as a linear map over F with E/F finite, then σ is an isomorphism. Then $\sigma(E) = E$.

We now prove that (2) ⇒ (3). Let α be a root of f in E, let L be a splitting field of f over E, and let β be a root of f in L. Then there exists a unique F-homomorphism $\sigma : F(\alpha) \to L$ with $\sigma(\alpha) = \beta$. By the lemma, there exists a finite extension M/L and $\tau : E \to M$ extending σ:

$$\begin{tikzcd}
 & M \arrow[d, dash] \\
 & L \arrow[d, dash] \\
E \arrow[uur, dashed, "\tau"] \arrow[d, dash] & E \arrow[dd, dash] \\
F(\alpha) \arrow[uur, "\sigma"] \arrow[d, dash] & \\
F \arrow[r, equal] & F
\end{tikzcd}$$

Since $\tau(E) = E$, we have $\beta = \tau(\alpha) \in E$. Therefore, all the roots of f are in E, so f is split over E.

Finally, we prove that (3) ⇒ (1). Let $E = F(\alpha_1, \cdots, \alpha_n)$. Let $f_i = m_{\alpha_i}$ for $i = 1, \cdots, n$, so are irreducible. As α_i is a root of f_i in E, then every f_i splits over E. Now $f = f_1 \cdots f_n \in F[x]$ is split over E. Then E is generated by all roots of f over F. Therefore, E is a splitting field of f. □

Remark 5.3.4 (Normality Test)**.** *If $E = F(\alpha_1, \cdots, \alpha_n)$, then E/F is normal if and only if m_{α_i} splits over E for all i.*

Example 5.3.5.

1. *Extension of degree* 1 *and* 2 *are normal. Therefore, F/F is normal. Suppose E/F such that $[E : F] = 2$, then we have $\alpha \in E \backslash F$, so $E = F(\alpha)$. Let $f = m_\alpha$, then* $\deg(f) = 2$, *so $f = (x - \alpha)(x - \beta)$ is split over E with $\beta \in E$.*

2. *Consider the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ where $\alpha = \sqrt[3]{2}$, then $m_\alpha = x^3 - 2$, which is irreducible by Eisenstein's criterion. Now $m_\alpha = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$, so it is not split because $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ has no roots in $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Therefore, the extension is not normal.*

Corollary 5.3.6. *If $L/E/F$ is a tower of field extensions and L/F is normal, then so is L/E.*

Proof. If L is a splitting field of $f \in F[x] \subseteq E[x]$, then L is a splitting field of f over E. Therefore, L/E is normal. □

Example 5.3.7. *1. Let $F = \mathbb{Q}$ and note that $x^3 - 2 = (x - \sqrt[3]{2})(x - \xi\sqrt[3]{2})(x - \xi^2\sqrt[3]{2})$ where $\xi^3 = 1$ but $\xi \neq 1$ is a root of unity. Therefore $\mathbb{Q}(\sqrt[3]{2}, \xi)$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Therefore, $\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q}$ is a normal extension, but note that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal extension:*

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q} \arrow[d, dash] \arrow[dd, dash, bend right=60, "\textit{normal}"'] \\
\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \arrow[d, dash, "\textit{not normal}"] \\
\mathbb{Q}
\end{tikzcd}$$

Note that $\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q}(\sqrt[3]{2})$ is quadratic, hence normal, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal because the minimal polynomial $x^3 - 2$ of $\sqrt[3]{2}$ does not split in $\mathbb{Q}(\sqrt[3]{2})[x]$. More generally, $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ is not normal for $n \geq 3$.

2. Note that the extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are normal, as both are quadratic, but $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal because $x^4 - 2$ does not split over $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$.

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash, "\textit{normal}"] \arrow[dd, dash, bend right=60, "\textit{not normal}"'] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "\textit{normal}"] \\
\mathbb{Q}
\end{tikzcd}$$

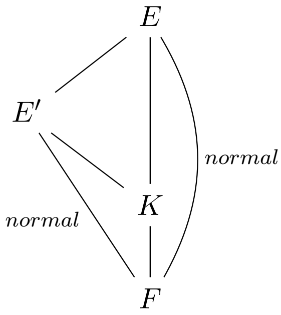
Remark 5.3.8. *Therefore, normality is not a good property.*

Definition 5.3.9 (Normal Closure)**.** *Let K/F be a finite field extension. A normal closure of K/F is a tower $E/K/F$ such that E/F is normal, and if E' is a field such that $K \subseteq E' \subseteq E$ and E'/F is normal, then $E' = E$.*

Theorem 5.3.10. *Let K/F be a finite field extension. Then a normal closure exists and it is unique up to isomorphism over K. (Similarly, over F.)*

Proof. Let $K = F(\alpha_1, \cdots, \alpha_n)$ and $f_i = m_{\alpha_i}$. Now let $f = f_1 \cdots, f_n$. Denote E as the splitting field of f over K. Therefore, E/F is generated by all roots of f as well. Therefore, E/F is a splitting field of f, and thus is normal.

Suppose we have



Since f_i is irreducible and has roots α_i in K (so also in E'), then by definition, f_i is split over E'. Therefore, f splits over E', which means all roots of f in E are already in E'. But E is generated by all the roots, so $E = E'$.

We now show that the normal closure is unique up to isomorphism over K. To prove this, we prove the following claim. This is sufficient because the splitting field of a polynomial is unique up to isomorphism over the ground field.

Claim 5.3.11. *Let $K = F(\alpha_1, \cdots, \alpha_k)$, $f_i = m_{\alpha_i}$ and $f = f_1 f_2 \cdots f_k$. E is then a splitting field of f over K.*

Subproof. We see that f_i is irreducible over F and has root α_i in $K \subseteq E$, so E/F is normal. Therefore, f_i is split over E, and so f is split over E.

Let K' be the field extended from K by the roots of f, so $K \subseteq K' \subseteq E$. Note that f is split over K'. Now K' is also the field extended from F by the roots of f, since K can be extended from F by $\alpha_1, \cdots, \alpha_n$, which are some roots of f. Therefore, K'/F is normal, ans so $K' = E$. Therefore, E is generated by all roots of f. Hence, E/K is a splitting field over f. ■

The statement then follows from the claim. □

Remark 5.3.12.

1. *Suppose K/F to be a finite field extension, and $f = f_1 \cdots f_n$. Take any field extension L/K such that f is split over L. Consider E to be the field extended from K by all roots of f in L. Then E is a normal closure of K/F, with $E \subseteq L$.*

2. *Following the notation above, the normal closure of K/F inside L is unique.*

5.4 Separable Extensions

Lemma 5.4.1. *Let $f \in F[x]$ be a non-constant polynomial. Then the following are equivalent:*

1. *f and f' are relatively prime.*
2. *Over any field extension K/F, f has no multiple roots.*
3. *There is a field extension K/F such that f is split over K and has no multiple roots.*

Proof. We first prove that (1) $\Rightarrow$ (2). Since $\gcd(f, f') = 1$ over K, then f has no multiple roots over K.

We now prove (2) $\Rightarrow$ (3). Take any splitting field K/F of f.

Finally, we prove that (3) $\Rightarrow$ (1). For all roots α of f in K, we have $f'(\alpha) \neq 0$, but $f(\alpha) = 0$. Therefore, $x - \alpha$ does not divide f' for all root α. Hence, $\gcd(f, f') = 1$. □

Definition 5.4.2 (Separable Polynomial)**.** *A non-constant polynomial $f \in F[x]$ is separable if f satisfies all of the above.*

Corollary 5.4.3.

1. *If $f \in F[x]$ is separable, then for all field extensions K/F, $f \in K[x]$ is also separable over K.*
2. *If f is separable and $g \mid f$ is a non-constant divisor, then g is separable.*

Proof.

1. The notion of relatively prime is independent on the fields.
2. Take K/F as in (3) as the above lemma, so f is split over K and has no multiple roots, then so it g. Hence, g is separable.

□

Proposition 5.4.4. *An irreducible polynomial $f \in F[x]$ is separable if and only if $f' \neq 0$.*

Proof. If f is separable, then $\gcd(f, f') = 1$ if and only if $f' \neq 0$. □

Example 5.4.5. *Consider a field F of characteristic $p > 0$, and let $a \in F^\times$. Take the polynomial $f = x^p - a$. The derivative of f is $f' = px^{p-1} = 0$ since $p' = 0$ in F. Therefore, f is not separable.*

In fact, if $a \notin (F^\times)^p$, then f is irreducible. Therefore, there are irreducible polynomials that are not separable.

Let K/F be a splitting field, β be a root of f, so $\beta^p = a$. Then $f = (x-\beta)^p$ over K has multiple roots, i.e. not irreducible.

Definition 5.4.6 (Perfect Field). *A field F is perfect if either it has characteristic 0 or having characteristic $p > 0$ but $F^\times = (F^\times)^p$.*

Proposition 5.4.7. *Every irreducible polynomial over a perfect field is separable.*

Proof. Take $f \in F[x]$ irreducible over perfect field F. If suffices to show that $f' \neq 0$. Notice that having $(ax^n)' = anx^{n-1}$, this equals to 0 if and only if $p \mid n$. This is fine when F has characteristic 0. If the characteristic of F is $p > 0$, then suppose $f' = 0$. Then $f = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_mx^{mp}$. Since F is perfect, then $a_i = b_i^p$ for some $b_i \in F$. Therefore, $f = (b_0 + b_1x + \cdots + b_mx^m)^p$. This is not irreducible, contradiction. □

Example 5.4.8. *1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are perfect.*

2. Finite fields are perfect. Note that we have the Frobinius map $f : F \to F$ as $x \mapsto x^p$ as a field homomorphism. Therefore, this must be injective. Since F is finite, we have a bijection.

3. Consider a field F of characteristic p. Then $F(x)$ is not perfect, since x is not a p-th power of rational functions.

Definition 5.4.9 (Separable Element). *Let K/F be a field extension and $\alpha \in K$ is algebraic over F (so the extension is finite). Then α is separable over F if the minimal polynomial m_α is separable.*

Note that if F is perfect, then every algebraic element α is separable.

Lemma 5.4.10. *Let $L/K/F$ be a tower of field extension, and $\alpha \in L$ is separable over F. Then α is separable over K.*

Proof. Let m_α be the minimal polynomial of α over F, then it is separable. If g is the minimal polynomial of α over K, then $g \mid m_\alpha$. But every divisor of separable polynomial is separable, so α is separable over K. □

Lemma 5.4.11. *Let K/F be a finite field extension, $\sigma : K \to L$ be a field homomorphism. Then there are at most $[K : F]$ extensions $K \to L$ of σ.*

Proof. As usual, write $K = F(\alpha_1, \cdots, \alpha_n$. We prove by induction on n.

When $n = 1$, then $K = F(\alpha)$, so $[K : F] = \deg(m_\alpha)$. Suppose

$$\begin{tikzcd}
K \arrow[dd, dash] \arrow[dr, "\tau"] & \\
& L \\
F \arrow[ur, "\sigma"] &
\end{tikzcd}$$

Then $\tau(\alpha)$ is a root of $\sigma(m_\alpha)$ in L. Therefore, there is a correspondence between extensions of τ and the roots of $\sigma(m_\alpha)$ in L.

Therefore, the number of roots is less than or equal to $\deg(m_\alpha) = [K : F]$.

In general, consider

$$\begin{tikzcd}
K = F'(\alpha_1, \cdots, \alpha_{n-1}) \arrow[d, dash] \arrow[dr, dashed, "\rho"] & \\
F' = F(\alpha_n) \arrow[d, dash] \arrow[r, dashed, "\tau"] & L \\
F \arrow[ur, "\sigma"] &
\end{tikzcd}$$

Then ρ extends τ and τ extends σ. Now the number of choices of τ is at most $[F' : F]$. But now for every τ, the number of extensions ρ of τ is less than or equal to $[K : F']$. Therefore, the number of extensions of σ is at most $[F' : F] \cdot [K : F'] = [K : F]$. □

Definition 5.4.12 (Separable Extension)**.** *A finite field extension K/F is separable if there is a field homomorphism $\sigma : F \to L$ that has exactly $[K : F]$ extensions $K \to L$.*

Proposition 5.4.13. *A finite field extension $F(\alpha)/F$ is separable if and only if α is separable over F.*

Proof. Denote $K = F(\alpha)$.

Suppose K/F is separable, then $\sigma : F \to L$ has exactly $[K : F]$ extensions from K to L. Take $f = m_\alpha$. Now $\sigma(f)$ has exactly $[K : F] = \deg(f)$ roots in l. Then f is split over L and has no multiple roots in L. By definition, f is separable, so α is separable.

Suppose α is separable over F, and let L be the splitting field of f over F. Then f has exactly $[K : F] = \deg(f)$ roots in L. There are exactly $[K : F]$ extensions from K to L. Hence, K/F is separable by definition. □

Lemma 5.4.14. *Let F be an infinite field, and L/F is a field extension, and $g \in L[x_1, x_2, \cdots, x_n]$ is a nonzero polynomial. Then there exists $a_1, a_2, \cdots, a_n$ such that $g(a_1, \cdots, a_n) \neq 0$.*

Proof. We can do induction on n. When $n = 1$, since every polynomial has finitely many roots, but F is infinite, then there is an element of F that is not a root.

Suppose we prove the case for $n-1$, we show the case at n. Let $g = g_0 + g_1 x_n + \cdots + g_m x^m$ where $g_i \in K[x_1, \cdots, x_{n-1}]$. Since g is nonzero, then there exists some i such that $g_i \neq 0$. By induction, there exists $a_1, a_2, \cdots, a_{n-1} \in F$ such that $g_i(a_1, \cdots, a_{n-1}) \neq 0$, so $g(a_1, \cdots, a_{n-1}, x_n)$ is a nonzero polynomial in $L[x_n]$. By case $n = 1$, there exists $a_n \in F$ such that $g(a_1, \cdots, a_n) \neq 0$. □

Remark 5.4.15. *The statement is false when F is finite. Take $F = \mathbb{F}_q$, then every element in F is a root of the polynomial $f = x^q - x$, so $f(a) = 0$ for all $a \in F$ but $f \not\equiv 0$.*

Corollary 5.4.16. *Let $g_1, g_2, \cdots, g)m \in L[x_1, x_2, \cdots, x_n]$ be distinct polynomials. Then there exists $a_1, a_2, \cdots, a_n \in F$ such that $g_i(a_1, \cdots, a_n)$ are distinct.*

Proof. Apply the lemma to the product $\prod\limits_{i<j}(g_i - g_j)$. □

Theorem 5.4.17 (Primitive Element Theorem)**.** *Let K/F be a finite separable extension. Then $K = F(\alpha)$ for some $\alpha \in K$.*

Proof. If F is finite, then so it K. We know that K/F is simple. Therefore, we may assume that F is infinite. Since the extension is separable, then there is a field homomorphism $\sigma : F \to L$ that has $m = [K : F]$ extensions $\tau_1, \cdots, \tau_m : K \to L$. By writing $K = F(\alpha_1, \cdots, \alpha_n)$, we consider $f = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n \in K[x_1, x_2, \cdots, x_n]$.

Now $\tau_i(f) = \tau_i(\alpha_1)x_1 + \cdots + \tau_i(\alpha_n)x_n \in L[x_1, \cdots, x_n]$ for $i = 1, \cdots, m$. Since α_i generates the field K/F and all τ_i's are distinct, so $\forall i \neq j$, there exists α_k such that $\tau_i(\alpha_k) \neq \tau_j(\alpha_k)$, so $g_i \neq g_j$. Therefore, the polynomials are distinct.

By the corollary, there exists $a_1, a_2, \cdots, a_n \in F$ such that the elements $\beta_i = \tau_i(f)(a_1, \cdots, a_n) = \tau_i(\alpha_1)a_1 + \cdots + \tau_i(\alpha_n)a_n \in L$ are distinct.

Let $\beta = \alpha_1 a_1 + \cdots + \alpha_n a_n \in K$. Then $\beta_i = \tau_i(\beta) \in L$ for $i = 1, \cdots, m$ and are pairwise distinct.

Set $K' = F(\beta)$, so it is a subfield of K. Then we have $K/K'/F$. Note that by restricting to $\tau_i |_{K'}: K' \to L$, becuase $\beta \in K'$ and $\tau_i(\beta) = \beta_i$ are distinct, then $\tau_i |_{K'}$ are distinct. Hence, $\tau_i |_{K'}: K' \to L$ are extensions of $\sigma : F \to L$.

$$\begin{tikzcd}
K \arrow[d, dash] \arrow[dr, "\tau_i"] & \\
K' \arrow[r] \arrow[d, dash] & L \\
F \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

Now note that m is bounded above by the number of extensions $K' \to L$ of σ, which is bounded by $[K' : F] \leq [K : F] = m$. Therefore, $K' = K$. Hence, $K = F(\beta)$. □

Example 5.4.18. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(a\sqrt{2} + b\sqrt{3})$.

Example 5.4.19. *Suppose F is a field of characteristic $p > 0$. Then $F(x)/F(x^p)$ is a degree-p extension because $m_x = t^p - x^p$.*

Moreover, $F(x,y)/F(x^p, y^p)$ is an extension of degree p^2 because both $F(x,y)/F(x,y^p)$ and $F(x, y^p/F(x^p, y^p)$ has degree p.

Take a rational function $h \in F(x,y)$, then $h^p \in F(x^p, x^p)$, then $F(x^p, y^p)(h)/F(x^p, y^p)$ has degree at most p. Therefore, $F(x^p, y^p)(h) \neq F(x, y)$. So $F(x,y)/F(x^p, y^p)$ is not simple (and not separable).

Proposition 5.4.20. *Let $E/K/F$ be finite field extensions. Then E/F is finite if and only if E/K and K/F are separable.*

Remark 5.4.21. *Separability is a good property.*

Proof. Suppose E/F is separable. Then there exists $\sigma : F \to L$ having exactly $[E : F]$ extensions $E \to L$:

$$\begin{tikzcd}
E \arrow[d, dash] \arrow[dr, "\tau"] & \\
K \arrow[r, "\rho"] \arrow[d, dash] & L \\
F \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

So σ has at most $[K : F]$ extensions ρ, and each ρ has at most $[E : K]$ extensions τ. Moreover, the total degree $[E : F] = [K : F] \times [E : K]$, so σ has exactly $[K : F]$ extensions, so K/F is separable. Also, every ρ has exactly $[E : K]$ extensions τ, so E/K is separable.

Conversely, suppose both E/K and K/F are separable. We choose $\alpha \in E$ such that $E = K(\alpha)$. Let $\sigma : F \to L$ has exactly $m = [K : F]$ extensions, so $\tau_i : K \to L$:

$$\begin{tikzcd}
E = K(\alpha) \arrow[d, dash] & \\
K \arrow[r, "\tau_i"] \arrow[d, dash] & L \\
F \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

Consider $f = m_\alpha$ over K, with E/K separable, we know α is separable over K, so f is separable over K, with $\deg(f) = [E : K]$. Consider $f_i = \tau_i(f) \in L[x]$. Then $g = f_1 f_2 \cdots f_m \in L[x]$.

Let M be a splitting field of g over L, then all f_i's are split over M. Note that every polynomial f_i is separable. So f_i has exactly $\deg(f_i)$ roots in M. Therefore, for every i, the extension from E to M of τ_i are in one-to-one correspondence with roots of f_i in M. So the number of extensions from E to M of τ_i is equal to $\deg(f_i)$. We then get $\sum \deg(f_i) = \deg(g) = m \times \deg(f) = [E : K] \times [K : F] = [E : F]$ extensions ρ of σ. By definition, this means that E/F is separable. □

Corollary 5.4.22. *Let K/F be a finite field extension. The following are equivalent:*

1. *K/F is separable.*

2. *Every $\alpha \in K$ is separable over F.*

3. *$K = F(\alpha_1, \cdots, \alpha_n)$, where α_i is separable over F.*

4. *$K = F(\alpha)$ where α is separable over F.*

Proof. (1) ⇒ (2): Note that $F \subseteq F(\alpha) \subseteq K$, so $F(\alpha)/K$ is separable, so α is separable.

(2) ⇒ (3): Take any generators $\alpha_1, \alpha_2, \cdots, \alpha_n$.

(3) ⇒ (1): We do mathematical induction on n. The base case is easy. As for the inductive step, consider the extension $K/K'/F$ with $K' = F(\alpha_1, \cdots, \alpha_{n-1})$ and $K = K'(\alpha_n)$. Note that both K/K' and K'/F are separable, so K/F is separable.

(1) ⇒ (4): Theorem.

(4) ⇒ (1): Trivial. □

Corollary 5.4.23. *Every finite field extension over a perfect field is separable.*

Proof. Suppose K/F is a finite field extension over perfect field F. Take an arbitrary element $\alpha \in K$, then m_α is irreducible, and so it is separable. Therefore, α is separable, so K/F is separable. □

5.5 Galois Field Extensions

Definition 5.5.1 (Galois Group). *Let E/F be a finite field extension. Consider the set $\{\alpha : E \to E\text{field isomorphisms over } F\}$. This set forms a group Gal(E/F), called the Galois group of E/F.*

Remark 5.5.2. *If $\sigma \in$ Gal(E/F), then $\sigma(a) = a$ for all $a \in F$. Moreover, for $a \in F$ and $x \in E$, then $\sigma(ax) = \sigma(a)\sigma(x) = a\sigma(x)$. Therefore, σ is F-linear.*

Proposition 5.5.3. *Suppose E/F is a finite field extension. Then*

1. $|\text{Gal}(E/F)| \leq [E : F]$.

2. $|\text{Gal}(E/F)| = [E : F]$ *if and only if E/F is normal and separable.*

Proof.

1. Note that every $\sigma \in \text{Gal}(E/F)$ is an extension of the inclusion of the inclusion $F \hookrightarrow E$ to a field homomorphism $\sigma : E \to E$. Therefore, the order of the Galois group Gal(E/F) is bounded above by the number of extensions, which is bounded above by the degree $[E : F]$.

2. Suppose $|\text{Gal}(E/F)| = [E : F]$, then the inclusion $F \hookrightarrow E$ has at least $|\text{Gal}(E/F)| = [E : F]$ extensions from E to E. Therefore, E/F is separable. Take an arbitrary field extension M over E and let $\sigma : E \to M$ be an extension over the identity of F. Then

$$\begin{tikzcd}
 & M \arrow[d, dash] \\
E \arrow[ur] \arrow[d, dash] & E \arrow[d, dash] \\
F \arrow[r, equal] & F
\end{tikzcd}$$

We need to show that $\sigma(E) = E$. Notice that the number of such σ is bounded above by $[E : F]$. Also, for every $\tau \in \text{Gal}(E/F)$, it satisfies $\tau : E \xrightarrow{\cong} E$, so $E \xrightarrow{\tau} E \hookrightarrow M$. We have $|\text{Gal}(E/F)| = [E : F]$ such compositions $E \hookrightarrow M$, so σ is of this form. Therefore, $\sigma(E) = \tau(E) = E$. hence, we also have normality.

Conversely, suppose E/F is normal and separable. Since the extension is separable, so we get to write $E = F(\alpha)$ for some $\alpha \in E$. Denote $f = m_\alpha \in F[x]$, which is irreducible. Also, $f(\alpha) = 0$. Since the extension E/F is normal, so f is split over E. Since E/F is separable, then f is separable, which means it has no multiple root. Therefore, f has exactly $[E : F]$ roots in E. For every root of β of f in E, there is a unique field homomorphism $\sigma : E \to E$ such that $\sigma(\alpha) = \beta$. This is now an injective linear map of finite-dimensional vector spaces. Therefore, σ is an isomorphism.

Therefore, we have found $[E : F]$ extensions $E \xrightarrow{\cong} E$ over F. Every such extension is an element in the Galois group, so the size of the Galois group is at least $[E : F]$. But the Galois group also has size of at most $[E : F]$, so it has exactly $[E : F]$ elements.

□

Definition 5.5.4 (Galois Extension)**.** *A finite field extension E/F is called Galois if $|Gal(E/F)| = [E : F]$, or equivalently, E/F is normal and separable.*

Example 5.5.5.

1. *$Gal(\mathbb{C}/\mathbb{R}) = \{e, conjugation\}$.*

2. *Consider a field F with characteristic not 2. Take $a \in F^\times$ that is not a square. In this case, $f = x^2 - a$ is irreducible and separable because the derivative is nonzero. Hence, the splitting field E of the polynomial f is separable. Note that $f = (x - \sqrt{a})(x + \sqrt{a})$ so $E = F(\sqrt{a})$, with $[E : F] = 2$. Therefore, E/F is normal and so Galois. The Galois has two elements, one is the identity, the other is σ, with $\sigma(\sqrt{a}) = -\sqrt{a}$. Denote $\alpha = x + y\sqrt{a}$ to be an arbitrary element with $x, y \in F$, then $\sigma(\alpha) = x - y\sqrt{a}$.*

3. *Consider a field F with characteristic 2. Consider $a \in F$ with $f = x^2 + x + a \in F[a]$. Then $f' = 2x + 1 = 1$, so f is separable. Assume f has no root in F, then f is irreducible. Again, take E to be the splitting field of the polynomial f over F. Let $\alpha, \beta \in E$ be a root of f, so $\alpha + \beta = 1$, so $\beta = 1 - \alpha = 1 + \alpha$. Therefore, $f = (x - \alpha)(x - 1 - \alpha)$ over E. We see that $[E : F] = 2$ and the extension is separable, so it is Galois. The Galois group then has two elements, one is the identity, the other element is σ with $\sigma(\alpha) = 1 + \alpha$. Hence, $x + y\alpha \in E$ is sent to $x + y(1 + \alpha)$.*

4. *Let q be a power of a prime. Consider the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of degree n. Note that the Frobenius homomorphism $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ defined by $\sigma(x) = x^q$ satisfies $\sigma(x) = x^q = x$ for $x \in \mathbb{F}_q$. Therefore, $\sigma \in Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Consider σ^i such that the map becomes the identity, then $\sigma^i(x) = x^{q^i} = x$ should hold for all x. However, the multiplication group of $\mathbb{F}_{q^n}$ should be cyclic, so $x^{q^i-1} = 1$, hence the order of*

the multiplication group $q^n - 1$ divides $q^i - 1$. In particular, $n \leq i$. In fact, the smallest i is just n. Therefore, n is the order of σ in the Galois group, so the Galois group has at least n elements, but n is also the upper bound because it is the degree of extension. Hence, the Galois group has order n, and is exactly the cyclic group generated by the Frobenius map.

5. Suppose E/F is Galois, then let $G = Gal(E/F)$. Since it is separable, then $E = F(\alpha)$ for some $\alpha \in E$. Take $f = m_\alpha$, then it is irreducible over F and has $f(\alpha) = 0$. Since E/F is normal, then f is split over E. Because f is separable, f has exactly $[E : F]$ roots in E. Say the roots of f are $X = \{\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n\} \subseteq E$. Pick $\sigma \in G$, then it takes a root to another root, so $\sigma(\alpha_i) = \alpha_j$ for some j.

   Consider G acting on the set X of all roots of f in E.

   Claim 5.5.6. G acts simply transitively.

   Proof. Take any $\beta \in X$, then there exists $\sigma \in G$ such that $\sigma(\alpha) = \beta$. Then G acts transitively. Moreover, this choice is unique, so G acts simply transitively. □

   Note that every set's group action is simply transitive if it is isomorphic to the group acting on itself by left translation, so $X \cong G$ as finite G-sets.

   Consider $E = \mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$. This is an extension of degree 4: suppose $\alpha = \sqrt{2+\sqrt{2}}$, then the minimal polynomial is $f = (x-\alpha)(x+\alpha)(x-\sqrt{2-\sqrt{2}})(x+\sqrt{2-\sqrt{2}}) = x^4 - 4x^2 + 2$, which is irreducible by Eisenstein criterion. Since $f(\alpha) = 0$ and f is irreducible, then $f = m_\alpha$, and so $[E : \mathbb{Q}] = 4$.

   We see that $\beta = \sqrt{2-\sqrt{2}}$ is another root of f, and $\alpha^2 = 2 + \sqrt{2}$, then $\sqrt{2} = \alpha^2 - 2 \in E$. Moreover, $\alpha \cdot \sqrt{2-\sqrt{2}} = \sqrt{2} \in E$. Therefore, $\beta \in E$. Therefore, there exists $\sigma : E \to E$ over $\mathbb{Q}$ such that $\sigma(\alpha) = \beta$. hence, $\sigma(\sqrt{2+\sqrt{2}} = \sqrt{2-\sqrt{2}}$. Therefore, $\sigma \in G = Gal(E/\mathbb{Q})$.

   Note that $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\beta) = \sigma(\sqrt{2-\sqrt{2}} = \sigma(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}) = \frac{\sigma(\sqrt{2}}{\sigma(\alpha)}$. Note $\sqrt{2} = \alpha^2 - 2$, then $\sigma(\sqrt{2}) = \sigma(\alpha)^2 - 2 = \beta^2 - 2 = (2 - \sqrt{2}) - 2 = -\sqrt{2}$. Therefore, $\sigma^2(\alpha) = -\alpha$, so it is not the identity. Moreover, $\sigma^3(\alpha) = \sigma(\sigma^2(\alpha) = \sigma(-\alpha) = -\beta$, so σ^2 is not identity as well. Hence, the Galois group has to be $G = \{e, \sigma, \sigma^2, \sigma^3\}$, which is a cyclic group of order 4. Therefore, $E/\mathbb{Q}$ is Galois.

6. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Note that both $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are extensions of degree 2, so $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ has degree 4, and is the splitting field of $(x^2 - 2)(x^2 - 3)$. Therefore, this is a Galois extension of degree 4, with Galois

group G of order 4. For $\sigma \in G$, $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$, therefore we have at most four possibilities (because the automorphism must send a root to another root of its minimal polynomial, by the example above). Consider σ that takes $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$, and τ that takes $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$. Therefore, $G = \{e, \sigma, \tau, \sigma\tau\}$, so $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

7. *Consider the field extension $\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q}$ where $\xi^3 = 1$ but $\xi \neq 1$. We can just say $\xi = \frac{-1+\sqrt{-3}}{2}$. Note that the extension has degree 6, because $\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q}(\sqrt[3]{2})$ has degree 2 and $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has degree 3. The extension is separable and normal because it is the splitting field of $x^3 - 2$. Therefore, the extension is Galois, and the Galois group G has order 6. For $\sigma \in G$, it should send $\sigma(\sqrt[3]{2}) = \xi^i \cdot \sqrt[3]{2}$ where $i = 0, 1$ or 2, and $\sigma(\xi) = \xi^j$ for $j = 1, 2$. Hence, this is the six choices we want. Consider σ that sends $\sqrt[3]{2}$ to $\xi \cdot \sqrt[3]{2}$ and sends ξ to ξ. Therefore, $\sigma^3 = e$. Also consider τ that sends $\sqrt[3]{2})$ to $\sqrt[3]{2}$ and sends ξ to ξ^2. So $\xi^2 = e$. Therefore, $\tau\sigma\tau = \sigma^2$. The group G is essentially S_3.*

Theorem 5.5.7 (Artin). *Let E be any field and G is a finite subgroup of Aut(E). Set $F = E^G := \{x \in E : \sigma(x) = x \ \forall \sigma \in G\} \subseteq E$, then E/F is a field extension. We claim that E/F is a Galois field extension with Galois group Gal(E/F) $= G$.*

Proof.

Claim 5.5.8. *Every $\alpha \in E$ is algebraic and separable over F and* $\deg(\alpha) = [F(\alpha) : F] \leq |G|$.

Subproof. Denote $S = \{\sigma(\alpha), \sigma \in G\} \subseteq E$. For $\tau \in G$, then $\tau S = S$. Note $|S| \leq |G|$. Consider the polynomial $f = \prod_{\sigma \in S} (x - s) \in E[x]$, with $\deg(f) = |S|$. However, for $\tau \in G$, $\tau f = \prod_{s \in S} (x - \tau s) = f$, so $f \in F[x]$. Note that f is separable and α is a root of f, so α is separable, and is algebraic over F. The degree is then $[F(\alpha) : F] = \deg(m_\alpha) \leq \deg(f) = |S| \leq |G|$. ■

Claim 5.5.9. $[E : F] \leq |G|$.

Subproof. Suppose not, then $[E : F] > |G|$, then there are linearly independent elements $\alpha_1, \cdots, \alpha_n \in E$ over F, and $n > |G|$.

Note that $F(\alpha_1, \cdots, \alpha_n)/F$ is an extension of degree at least $n > |G|$. Note that this is separable over F, so it is generated by one element, i.e. $F(\alpha_1, \cdots, \alpha_n) = F(\alpha)$ for some $\alpha \in E$, then $[F(\alpha) : F] > |G|$, contradiction. ■

Recall that for a finite field extension, we should have $[E : F] \geq |G|$. By the second claim, $[E : F] \leq G$. Therefore, $[E : F] = |G|$. Moreover, we get to write $|G| \geq [E : F] \geq |\mathrm{Gal}(E/F)| \geq |G|$ since $G \subseteq \mathrm{Gal}(E/F)$. Therefore, $[E : F] = |\mathrm{Gal}(E/F)|$, so E/F is Galois. Because G is a subgroup of the Galois group, then $\mathrm{Gal}(E/F) = G$. □

Example 5.5.10. *1. Let K be a field, take $E = K(x_1, x_2, \cdots, x_n)$. We claim that this is the quotient field of $K[x_1, x_2, \cdots, x_n]$. Take $S_n \subseteq Aut(E)$, so it permutes the x_i's. Then $E^{S_n} \subseteq E$ as a subfield of symmetric functions in E. Note that $E^{S_n} = F(s_1, s_2, \cdots, s_n)$ where s_i is the i-th standard symmetric function $\sum x_{j_1} x_{j_2} \cdots x_{j_i}$. From Artin's Theorem, E/E^{S_n} is Galois, and Gal$(E/E^{S_n}) = S_n$.*

2. Let G be a finite group, and we know we get to embed G into some S_n. Note $G \subseteq S_n \subseteq Aut(E)$. Applying Artin's theorem to G, we see that Gal$(E/E^G) = G$. Therefore, every finite group is the Galois group of some field extension.

3. Consider the smallest field of characteristic 0, which is $\mathbb{Q}$. The inverse Galois problem asks whether there is a Galois extension $E/\mathbb{Q}$ with Gal$(E/\mathbb{Q}) \cong G$ for some finite group G. This remains an open question, but it is known that every finite Abelian group and every symmetric group can be realized in such form.

Remark 5.5.11. *There are two maps that give a correspondence: let E/F be a Galois extension and $G =$ Gal(E/F). Given a field L with $F \subseteq L \subseteq E$, we obtain a subgroup of G given by $\{\sigma \in G \mid \sigma(x) = x \ \forall x \in L\} =$ Gal(E/L). Conversely, given $H \subseteq G$, we obtain a subfield L with $F \subseteq L \subseteq E$ by setting $L = E^H$. More precisely, the mappings are given by $K \mapsto$ Gal$(E/K) \subseteq$ Gal$(E/F) = G$ (from intermediate field K to a subgroup of G) and $H \mapsto E^H$ for $H \subseteq G$ and $F \subseteq E^H \subseteq E$ (from a subgroup H of G to an intermediate field E^H of E/F), respectively.*

Theorem 5.5.12. *The two maps are inverses to each other. (In particular, they are bijections.)*

Proof. Take an intermediate field $F \subseteq K \subseteq E$ of E/F. By the first mapping, we get $H = \mathrm{Gal}(E/K)$; by the second mapping, we get E^H. To show that that this is a bijection, we need to show that $E^H = K$.

Note that H is identity on K, so $K \subseteq E^H$. Since E/K is normal and separable, then it is Galois, and so $H = \mathrm{Gal}(E/K)$. In particular, the order of the extension is $[E : K] = |H|$. By Artin's theorem, E/E^H is Galois, and $\mathrm{Gal}(E/E^H) = H$. In particular, the degree $[E : E^H] = |H|$. Therefore, $E^H = K$ because $K \subseteq E^H$.

For the other composition, let H be a subgroup of G, and we get $K = E^H$, then get $\mathrm{Gal}(E/K$. We need to show that the Galois group is just H. By Artin's theorem, we have that $\mathrm{Gal}(E/K) = \mathrm{Gal}(E/E^H) = H$. □

Property 5.5.13. *1. Suppose we have the extension $E/K_2/K_1/F$, then Gal$(E/K_1) \supseteq$ Gal(E/K_2). Similarly, if we have $H_1 \subseteq H_2 \subseteq G$, then $E^{H_1} \supseteq E^{H_2}$. In particular, the largest subgroup (E itself) should correspond to the trivial subgroup, and the smallest subgroup (F itself) should correspond to G, so $F = E^G$. This gives a correspondence between subgroup H and E^H.*

2. Suppose $H \subseteq G$ is a subgroup and $K = E^H$, then Gal$(E/K) = K$, and $[E : K] = |H|$.

3. Take $\sigma \in G$ Galois group and $H \subseteq G$ is a subgroup, then we have the conjugation subgroup $\sigma H \sigma^{-1} \subseteq G$. Note that $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$.

Proof. Note that $x \in E^{\sigma H \sigma^{-1}}$ if and only if $\sigma\tau\sigma^{-1}(x) = x$ for all $\tau \in H$ if and only if $\tau\sigma^{-1}(x) = \sigma^{-1}(x)$ for all $\tau \in H$ if and only if $\sigma^{-1}(x) \in E^H$ if and only if $x \in \sigma(E^H)$. □

4. Let E/F be a Galois field extension with $G =$ Gal(E/F) and $H \subseteq G$ is a subgroup. Then E^H/F is normal if and only if $H \lhd G$.

In this case, Gal$(E^H/F) \cong G/H$.

Proof. Suppose E^H/F is normal. Take $\sigma \in G$ such that

$$\begin{tikzcd}
E \arrow[r, "\sigma", "\sim"'] \arrow[d, dash] & E \arrow[d, dash] \\
E^H \arrow[r, dashed, "\cong"] \arrow[ur] \arrow[d, dash] & E^H \arrow[d, dash] \\
F \arrow[r, equal] & F
\end{tikzcd}$$

Now $\sigma(E^H) = E^H$. We have the restriction res : $G \to \mathrm{Gal}(E^H/F)$ by sending $\sigma \mapsto \sigma\,|_{E^H} \colon E^H \to E^H$, then $\ker(\mathrm{res}) = \mathrm{Gal}(E/E^H) = H \lhd G$.

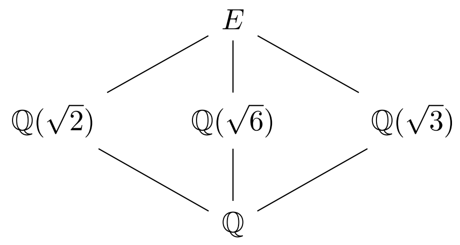
Conversely, suppose $H \lhd G$. Take $\sigma \in G$, then $\sigma H \sigma^{-1} = H$, $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$, so $\sigma(E^H) = E^H$. Then there is a restriction map res : $G \to \mathrm{Gal}(E^H/F)$ given by

$$\begin{tikzcd}
G \arrow[rr] \arrow[dr] & & \mathrm{Gal}(E^H/F) \\
& G/H \arrow[ur, hook, "\sim"'] &
\end{tikzcd}$$

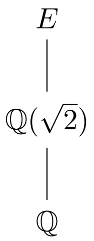
where $H = \ker(\mathrm{res})$.

So $|\mathrm{Gal}|(E^H/F) \geq |G/H| = [G:H] = [E^H : F] \geq |\mathrm{Gal}(E^H/F)|$. Note that the first inequality is equal if and only if we have an isomorphism, and the second inequality is equal if and only if we have E^H/F Galois and normal. Hence, we have an isomorphism $G/H \to \mathrm{Gal}(E^H/F)$ by sending σH to $\sigma \mid_{E^H}$. □

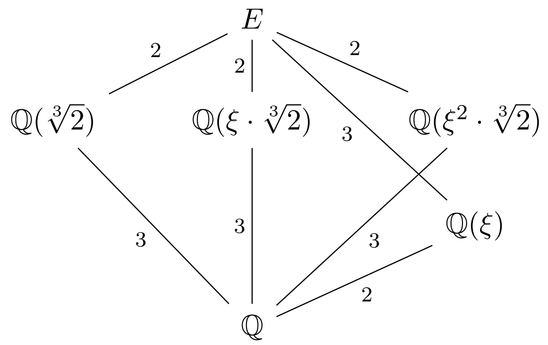
Example 5.5.14. *1. Consider $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*



2. $E = \mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$, and G is the cyclic group of order 4.



3. $E = \mathbb{Q}(\xi, \sqrt[3]{2})$, where $\xi^3 = 1$ but $\xi \neq 1$, and $G = S_3$. There are 3 subgroups of order 2, 1 subgroup (normal) of normal 3.


E
2
2
2
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\xi \cdot \sqrt[3]{2})$
3
$\mathbb{Q}(\xi^2 \cdot \sqrt[3]{2})$
$\mathbb{Q}(\xi)$
3
3
3
2
$\mathbb{Q}$

Proposition 5.5.15. *Let M/F be a field extension, $K \subseteq K \subseteq M$, $F \subseteq L \subseteq M$. KL is the smallest subfield of M containing both K and L.*

Proof. Denote $K = F(\alpha_1, \cdots, \alpha_n)$, then $KL = L(\alpha_1, \cdots, \alpha_n)$.

$$\begin{tikzcd}
 & KL & \\
K \arrow[ur, dash] & & L \arrow[ul, dash] \\
 & F \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

□

Theorem 5.5.16. *Assume that K/F is Galois. Then KL/L is also Galois. The restriction map res : Gal$(KL/L) \to$ Gal(K/F) is well-defined and it yields an isomorphism*

$$\textit{Gal}(KL/L) \xrightarrow{\cong} \textit{Gal}(K/K \cap L).$$

Proof. Note that we can write $K = F(\alpha_1, \cdots, \alpha_n)$. Since K/F is separable, then α_i are separable over F, then they are separable over L, so KL/L is separable. Note that K is the splitting field of $f \in F[x]$ where $f = \prod m_{\alpha_i}$. Then KL/L is a splitting field of $f \in L[x]$. Therefore, KL/L is Galois.

Take $\sigma \in \mathrm{Gal}(KL/L)$. Then $\sigma \mid_K (K) = K$.

$$\begin{tikzcd}
KL \arrow[r, "\sigma", "\sim"'] \arrow[d, dash] & KL \arrow[d, dash] \\
K \arrow[ur, "\sigma|_K"'] \arrow[r, dashed] \arrow[d, dash] & K \arrow[d, dash] \\
F \arrow[r, equal] & F
\end{tikzcd}$$

Therefore, the restriction is well-defined: $\mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$, and gives $\sigma \in \mathrm{Gal}(K/F)$. Suppose σ acts as the identity on K, i.e. $\sigma \mid_K = \mathbf{id}_K$, then $\sigma(\alpha_i) = \alpha_i$ for each α_i, so σ acts as the identity on L. However, now $KL = L(\alpha_1, \cdots, \alpha_n)$, so $\sigma = \mathbf{id}_{KL}$. Therefore, the restriction is injective.

Now $\sigma \in \mathrm{Gal}(KL/L)$, $\sigma \mid_L = \mathbf{id}_L$, so $\sigma \mid_{K \cap L} = \mathbf{id}_{K \cap L}$. Therefore, $\mathrm{res}(\sigma) = \sigma \mid_K \in \mathrm{Gal}(K/K \cap L)$, so $\mathrm{im(res)} \subseteq \mathrm{Gal}(K/K \cap L)$.

Denote $H = \mathrm{im(res)}$. Now $K^H = \{x \in K : \sigma \mid_K (x) = \sigma(x) = x \ \forall \sigma \in \mathrm{Gal}(KL/L)\} \subseteq L$. Now $K^H \subseteq K \cap L$, so $\mathrm{Gal}(K/K^H) = \mathrm{Gal}(K/K \cap L)$. Therefore, $\mathrm{im(res)} = \mathrm{Gal}(K/K \cap L)$. □

Corollary 5.5.17. *If $K \cap L = F$, i.e. K and L are linearly disjoint over F, then Gal$(KL/L) \cong$ Gal(K/F).*

Theorem 5.5.18. *Assume that both K/F and L/F are Galois. Then KL/F is Galois and the restriction map res : Gal$(KL/F) \to$ Gal$(K/F) \times$ Gal(L/F) is injective. If $K \cap L = F$, then res is an isomorphism. Moreover, Gal$(KL/F) =$ Gal$(KL/L) \times$ Gal(KL/K) as an internal direct product.*

Proof. If K is a splitting field of $f \in F[x]$, L is a splitting field of $g \in F[x]$, then KL is a splitting field of fg. Therefore, KL/F is normal.

Moreover, since $K = F(\alpha_1, \cdots, \alpha_n)$ is separable, then $KL = L(\alpha_1, \cdots, \alpha_n)$ is also separable. Hence, KL/F is separable, so it is Galois.

Take $\sigma \in \text{Gal}(KL/F)$, then $\sigma\mid_K = \mathbf{id}_K$, $\sigma\mid_L = \mathbf{id}_L$, so it is in $\text{Gal}(K/L)$, then $\sigma = \mathbf{id}$. Hence, res is injective.

Moreover, suppose K and L are linearly disjoint over F, then for $\tau \in \text{Gal}(K/F)$ and $\rho \in \text{Gal}(L/F)$, note that there is $\tau' \in \text{Gal}(KL/L)$ and $\rho' \in \text{Gal}(KL/K)$ that can be restricted to the two maps. Hence, $\tau'\rho'\mid_K = \tau$, $\tau'\rho'\mid_L = \rho$, so $\tau(\tau'\rho') = (\tau, \rho)$, so res is an isomorphism.

In fact, $\text{Gal}(K/F) \cong \text{Gal}(KL/L)$ and $\text{Gal}(L/F) \cong \text{Gal}(KL/K)$, both of which are subgroups of $\text{Gal}(KL/F)$, satisfy $\text{Gal}(KL/F) = \text{Gal}(KL/L) \times \text{Gal}(KL/K)$ as an internal direct product. □

5.6 Cyclotomic Field Extensions

Example 5.6.1. *Take a field F of characteristic $p > 0$, let $x \in F$ that is a root of unity of degree p, i.e. $x^p = 1$. Then $0 = x^p - 1 = (x-1)^p$, so $x - 1 = 0$, then $x = 1$.*

Let F be a field and n is an integer that is prime to char(F) (if the characteristic is 0, then the restriction is empty). The polynomial $f = x^n - 1$ has derivative $f' = nx^{n-1} \neq 0$, then $\gcd(f, f') = 1$, so f is separable. Consider F_n/F as the splitting field of polynomial f. This is a separable field extension and is unique up to isomorphism. Moreover, it is normal, so F_n/F is Galois.

Definition 5.6.2 (Cyclotomic Field Extension)**.** *The extension structure above F_n/F is called the n-cyclotomic field extension of F.*

Remark 5.6.3. *We want to determine the structure of the Galois group of F_n/F. Recall that if we denote $\mu_n = \{x \in F_n : x^n = 1\} \subseteq F_n^\times$ as the field of root of unity, then it is also cyclic of order n. We know that the group is generated by $\varphi(n)$ elements, where φ is the Euler function. Suppose we choose a generator $\xi_n \in \mu_n$ (a primitive n-th root of unity), then $\forall \xi \in \mu_n$, $\xi = (\xi_n)^i$ for some i, where i is unique modulo n. Hence, $i + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$*

is well-defined. We can also conclude that the field F_n is generated by a primitive root, u.e. $F_n = F(\xi_n)$.

Take $\sigma \in Gal(F_n/F)$, then it sends a root of unity to another root of unity, i.e. $\sigma(\xi_n) = (\xi_n)^i$ for some i, where $\gcd(i,n) = 1$. Now suppose the map $\chi : Gal(F_n/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ sends $\sigma \mapsto [i]_n$, then χ is a homomorphism: suppose in addition that $\tau(\xi_n) = (\xi_n)^j$, then $\sigma\tau(\xi_n) = (\xi_n)^{ij}$. Moreover, if we take a root of unity $\xi \in \mu_n$, then $\xi = (\xi_n)^k$, and $\sigma(\xi) = \sigma(\xi_n^k) = \sigma(\xi_n)^k = (\xi_n)^{ij} = \xi^i$. Therefore, the formula $\sigma(\xi_n) = (\xi_n)^i$ should hold for any root. Hence, we see that χ is independent on the choice of ξ_n.

Claim 5.6.4. *χ is injective.*

Proof. Take $\sigma \in \ker(\chi)$, then $\sigma(\xi_n) = \xi_n = (\xi_n)^i$, so $i \equiv 1 \pmod n$. Therefore, $[i]_n = [1]_n$. □

Hence, we can identify canonically the Galois group of an cyclotomic field extension with the group $(\mathbb{Z}/n\mathbb{Z})^\times$, i.e. $Gal(F_n/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. In particular, $Gal(F_n/F)$ is Abelian.

Remark 5.6.5. *Suppose $F = \mathbb{Q}$. Let Φ_n be the minimal polynomial of ξ_n of degree n. Therefore, $\Phi_n \in \mathbb{Q}[x]$ is monic. Note that $\exists \alpha \in \mathbb{Q}$ such that $\tilde{\Phi}_n := \alpha\Phi_n \in \mathbb{Z}[x]$ is primitive. We know that every primitive root of unity ($\xi_n^n - 1 = 0$, so ξ_n is a root of $f = x^n - 1$, then the minimal polynomial $\Phi_n \mid (x^n - 1)$ and $\tilde{\Phi}_n \mid (x^n - 1)$ in $\mathbb{Q}$. Note that both polynomials are primitive. By Gauss' Lemma, then they are also divisible in $\mathbb{Z}[x]$. Hence, $x^n - 1 = \tilde{\Phi}_n \cdot g$ for some $g \in \mathbb{Z}[x]$. Hence, the leading coefficient of $\tilde{\Phi}_n$ must be ± 1. However, Φ_n is monic, so $\alpha = \pm 1$. We deduce that $\Phi_n \in \mathbb{Z}[x]$. Therefore, the minimal polynomial has integer coefficients. The polynomial Φ_n is called the n-th cyclotomic polynomial (over $\mathbb{Q}$).*

Lemma 5.6.6. *Let p be a prime integer such that $p \nmid n$. Then $(\xi_n)^p$ is a root of Φ_n.*

Proof. We write $x^n - 1 = \Phi_n \cdot g$ where $g \in \mathbb{Z}[x]$. Suppose, towards contradiction, that $(\xi_n)^p$ is not a root of Φ_n, then $(\xi_n)^p$ is a root of g. Therefore, $g((\xi_n)^p) = 0$.

Observe that for $g_1(x) = g(x^p)$, then $g_1(\xi_n) = g((\xi_n)^p) = 0$, so ξ_n is a root of g_1. Therefore, the minimal polynomial $\Phi_n \mid g_1$ in $\mathbb{Z}[x]$. Consider the canonical homomorphism $\mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/pmathbbZ$ and correspondingly $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ that sends h to $\bar{h}$.

Note that $\bar{g}(x) = \bar{g}(x^p)$, but for any $a \in \mathbb{F}_p$, then $a^p = a$, so $\bar{g}(x) = \bar{g}(x^p) = \sum a_i x^{pi} = \sum a_i^p x^{pi} = \sum (a_i x^i)^p = \bar{g}^p$. Therefore, $\bar{g}_1 = (\bar{g})^p$ in $\mathbb{F}_p[x]$.

Recall that $\Phi_n \mid g_1$, then $\bar{\Phi}_n \mid \bar{g}_1 = (\bar{g})^p$ over $\mathbb{F}_p$. Let l be an irreducible divisor of $\bar{\Phi}_n$ in $\mathbb{F}_p[x]$. Then $l \mid \bar{\Phi}_n \mid (\bar{g})^p$, so $l \mid \bar{g}$. Recall that $x^n - 1 = \Phi_n \cdot g$, so $x^n - \bar{1} = \bar{\Phi}_n \cdot \bar{g}$, so $l \mid \bar{\Phi}_n$ and $l \mid \bar{g}$, hence $l^2 \mid x^n - 1$ in $\mathbb{F}_p[x]$. This is a contradiction because $x^n - \bar{1}$ is separable polynomial (as $\bar{f}' = nx^{n-1} \neq 0$), so it cannot be divided by a square of a irreducible, contradiction. □

Corollary 5.6.7. *All primitive roots of* 1 *of degree* n *are the roots of* Φ_n. *In particular,* $\deg(\Phi_n) \geq \varphi(n)$.

Proof. Let ξ be a primitive root of degree n of 1. Then $\xi = (\xi_n)^i$, so $\gcd(i, n) = 1$. We write $i = p_1 p_2 \cdots p_k$ as a product of primes, but that means the primes do not divide n. We apply the lemma k times, then $(\xi_n)^{p_1}, (\xi_n)^{p_1 p_2}, \cdots, (\xi_n)^{p_1 \cdots p_k}$ are the roots of Φ_n. □

Theorem 5.6.8. *Gal*$(\mathbb{Q}_n/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$. *Moreover,* $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$, *and* $\Phi_n(x) = \prod\limits_{\xi \textit{ primitive nth root of } 1} (x - \xi)$, *and should be independent on* ξ_n.

Proof. We know that $\varphi(n) \leq \deg(\Phi_n) = [\mathbb{Q}_n : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})| \leq |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. Therefore, $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$ and $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$, and $\Phi_n(x) = \prod\limits_{\xi \text{ primitive } n\text{th root of } 1} (x - \xi)$. □

Remark 5.6.9. $x^n - 1 = \prod\limits_{d|n} \Phi_d$. *Indeed, note that* $x^n - 1 = \prod\limits_{\xi \textit{ primitive nth root of } 1} (x - \xi)$, *but every root of unity is primitive for exactly one integer. Therefore by taking* $\xi \in \mu_n$, *if* d *is the order of* ξ *in* μ_n, *then* $d \mid n$ *and* ξ *is a primitive* d*th root of unity. Hence,* Φ_d *should be a linear term of the form* $\Phi_d = x - \xi$.

When $d = n$, *we have* $\Phi_n = \frac{x^n - 1}{\prod\limits_{d|n, d \neq n} \Phi_d}$.

Example 5.6.10.

1. $\Phi_1 = x - 1$.

2. $\Phi_2 = x + 1$.

3. $\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ *for* p *prime, as* $\varphi(p) = p - 1$.

4. $\Phi_3 = x^2 + x + 1$.

5. $\Phi_4 = \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1 = (x + i)(x - i)$.

6. $\Phi_5 = x^4 + x^3 + x^2 + x + 1$.

7. $\Phi_6 = x^2 - x + 1$, *as* $\varphi(6) = 2$.

8. *All cyclotomic polynomials are irreducible polynomials over $\mathbb{Q}$, because they are minimal polynomials.*

9. *$\forall n < 105$, all coefficients of Φ_n are 0 or ± 1. $\Phi_{105} = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} + \cdots - 2x^7 + \cdots$. Note that $105 = 3 \times 5 \times 7$ is the product of first three odd primes.*

5.7 Galois Group of a Polynomial

Definition 5.7.1 (Galois Group of a Polynomial)**.** *Let $f \in F[x]$ be a separable polynomial (and so it is non-constant) over a field F of characteristic 0. Take E/F as the splitting field of f. We know that E exists and is unique up to isomorphism. Therefore, E/F is normal and separable, so it is Galois.*

Now Gal(E/F) is called the Galois group of f, also denoted Gal(f).

Example 5.7.2. 1. *Gal($x^n - 1$) $= (\mathbb{Z}/n\mathbb{Z})^\times$ over $\mathbb{Q}$.*

2. *Let K be a field and $E = K(x_1, \cdots, x_n)$ be a field. Note that S_n acts on E by permutation of variables, and $E^{S_n} = K(s_1, s_2, \cdots, s_n)$ is generated by standard symmetric functions over K. We denote $F = E^{S_n}$. Consider $f = \prod_{i=1}^{n}(x - x_i) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n \in F[x]$. We call this the generic polynomial. The coefficients $s_1, \cdots, s_n$ are algebraically independent. We can conclude that E is the splitting field of F over F because the polynomial f splits in E, and E is generated by the roots. The Galois group of f is given by Gal(f) $=$ Gal(E/F) $= S_n$.*

Proposition 5.7.3. *Let E/F be a Galois field extension, and $\alpha \in F$. Let $S = \{\sigma(\alpha) : \sigma \in G = \text{Gal}(E/F)\}$. Then $\deg(\alpha) = |S|$ and the minimal polynomial $m_\alpha = \prod_{\beta \in S}(x - \beta)$.*

Proof. Consider the extension $E/F(\alpha)/F$, where we denote $H = \text{Gal}(E/F(\alpha)) \subseteq G$. Here G acts on S transitively such that $H = \text{stab}(\alpha)$ because the action is trivial. By definition, $\deg(\alpha) = [F(\alpha) : F] = [G : H] = |S|$. Also note that $f = \prod_{\beta \in S}(x - \beta)$ is $G-$ stable: $\sigma f = f$ for all $\sigma \in G$. Therefore, $f \in F[x]$. Since $\alpha \in S$, then $f(\alpha) = 0$. Therefore, $m_\alpha \mid f$, but $\deg(m_\alpha) = |S| = \deg(f)$, then since both polynomials are monic, we conclude that $m_\alpha = f$. □

Example 5.7.4. *Let $\alpha = \sqrt{2} + \sqrt[3]{5}$ over $\mathbb{Q}$. For $\xi^3 = 1$ such that $\xi \neq 1$, we know*

$$\begin{tikzcd}
 & \alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}, \xi) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "G"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[3]{5}, \xi) \arrow[dl, dash, "6"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Note that the intermediate fields are linear disjoint, then $G \cong \mathbb{Z}/2\mathbb{Z} \times S_3$. Let ρ be the element from $\mathbb{Z}/2\mathbb{Z}$, and σ and τ are elements of S_3 as the 3-cycle and the 2-cycle, respectively. We then can denote $\rho(\sqrt{2}) = -\sqrt{2}$, $\rho(\sqrt[3]{5}) = \sqrt[3]{5}$ and $\rho(\xi) = \xi$; $\sigma(\sqrt{2}) = \sqrt{2})$, $\sigma(\sqrt[3]{5}) = \xi \cdot \sqrt[3]{5}$ and $\sigma(\xi) = \xi$; $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt[3]{5}) = \sqrt[3]{5}$, and $\tau(\xi) = \xi^{-1} = \xi^2$.

In particular, $\sigma(\alpha) = \pm\sqrt{2} + \xi^i \cdot \sqrt[3]{5}$, where $i = 0, 1, 2$, so there are 6 possibilities, so $|S| = 6 = \deg(\alpha)$. We can write $\alpha - \sqrt{2} = \sqrt[3]{5}$, then $(\alpha - \sqrt{2})^3 = 5$, so $m_\alpha = (x^3 + 6x - 5)^2 - 2(3x^2 + 2)$.

5.8 Algebraically Closed Field

Proposition 5.8.1. *Let F be a field. The following are equivalent:*

1. *F has no non-trivial finite field extensions.*
2. *Every irreducible polynomial in $F[x]$ is linear.*
3. *Every non-constant polynomial in $F[x]$ has a root in F.*
4. *Every non-constant polynomial in $F[x]$ is split.*

Proof. (1) $\Rightarrow$ (2): Let f be irreducible, then $F[x]/f \cdot F[x]$ is a field extension over F of degree $\deg(f)$. However, F has no non-trivial field extensions, so f is linear.

(2) $\Rightarrow$ (3): Take any non-constant polynomials, we write it as the product of linear terms, then there has to be a root in F.

(3) $\Rightarrow$ (4): Since $f(\alpha) = 0$, then $f = (x - \alpha) \cdot g$.

(4) $\Rightarrow$ (2): if every polynomial is split, then every irreducible is linear.

(2) $\Rightarrow$ (1): Suppose K/F is a finite field extension. Consider $\alpha \in K$. We know that $\deg(m_\alpha) = [F(\alpha) : F]$. But m_α is irreducible, so it is linear, then $[F(\alpha) : F] = 1$, which means $\alpha \in F$. Therefore, $K = F$. □

Definition 5.8.2 (Algebraically Closed)**.** *If F is a field satisfying the four conditions above, then F is called algebraically closed.*

Theorem 5.8.3. *$\mathbb{C}$ is algebraically closed.*

Proof.

Claim 5.8.4. *$\mathbb{R}$ has no non-trivial odd-degree extension.*

Subproof. Every finite extension is generated by one element since it is separable. Suppose $[\mathbb{R}(\alpha) : \mathbb{R}] = \deg(m_\alpha)$ is odd, then m_α is irreducible of odd degree, but that means m_α has to have a real root, then $\deg(m_\alpha) = 1$. ■

Claim 5.8.5. *$\mathbb{C}$ has no quadratic extensions.*

Subproof. If $z = \tau \cdot (\cos(\varphi) + i\sin(\varphi))$ is a complex number, then $t = \sqrt{\tau}(\cos(\frac{\varphi}{2}) + i\sin(\frac{\varphi}{2})$ satisfies $t^2 = z$. Therefore, every complex number is a square, so every quadratic polynomial has a root. ■

Let $K/\mathbb{C}$ be a finite extension. We want to show that $K = \mathbb{C}$. We have a tower $K/\mathbb{C}/\mathbb{R}$, then it is a finite extension. Replacing K by a normal closure of K over $\mathbb{R}$ (up to isomorphism), we may assume that $K/\mathbb{R}$ is Galois. Let $G = \mathrm{Gal}(K/\mathbb{R})$, let $P \subseteq G$ be a Sylow 2-subgroup. Therefore, note that $[K^P : \mathbb{R}] = [G : P]$ is odd. Therefore,$K^P = \mathbb{R} = K^G$, then $G = P$, so G is a 2-group.

Let $H = \mathrm{Gal}(K/\mathbb{C}) \subseteq G$ of index 2. We need to show that $H = \{e\}$. Suppose not, then there exists a subgroup $I \subseteq H$ of index 2. Therefore, we have $\mathbb{C} \subseteq K^I \subseteq K$, but $[K^I : \mathbb{C}] = [H : T] = 2$, contradiction. Therefore, H is trivial and $K = \mathbb{C}$. □

Definition 5.8.6 (Algebraic Closure). *Let F be a field. A field extension F_{alg}/F is called an algebraic closure of F if*

1. *F_{alg} is algebraically closed.*
2. *F_{alg}/F is algebraic.*

Example 5.8.7. *$\mathbb{Q}_{alg}$ is the field of algebraic elements in $\mathbb{C}$.*

Theorem 5.8.8. *F_{alg} exists for every field F.*

Proof. Let S be the set of all non-constant polynomials in $F[x]$. For all $f \in S$ we take a variable x_f. Denote $R = F[x_f]_{f\in S}$. Let $I \subseteq R$ be the ideal that is generated by $f(x_f)$ for all $f \in S$.

Claim 5.8.9. *$I \neq R$.*

Subproof. Suppose $I = R$, then $1 = \sum_{f \in T} f(x_f) \cdot g_f$ where $g_f \in R$ and $T \subseteq S$ is a finite subset. Take $h(t) = \prod_{f \in T} f(t) \in F[t]$ to be a non-constant polynomial. Let L/F be a splitting field of h. IN particular, all $f \in T$ are split over L, so $f(a_f) = 0$ for some $a_f \in L$. Take $x_f = a_f$, then $1 = \sum_{f \in T} f(a_f) \cdot g_f(\cdots) = 0$, contradiction. ■

Since $I \neq R$, there exists a maximal ideal M such that $I \subseteq M \subseteq R$. Let $F_1 = R/M$ to be a field extension over F. We have $I = f(x_f) + I \in R/I \twoheadrightarrow R/M = F_1$. Therefore, if $\bar{x}_f$ is the image of x_f in the field F_1, then $f(\bar{x}_f) = 0$ in F_1. In particular, every $f \in S$ has a root in F_1.

Denote $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq$, where we repeat the procedure as above. Then $F_{\text{alg}} = \bigcup_{i=0}^{\infty} F_i$.

Claim 5.8.10. *F_{alg} is an algebraic closure of F.*

Subproof. Let $f \in F_{\text{alg}}[x]$ be a non-constant polynomial. Then $f \in F_i[x]$ for some i. By construction, f has a root in $F_{i+1} \subseteq F_{\text{alg}}$. Therefore, F_{alg} is algebraically closed. ■

Claim 5.8.11. *F_{i+1}/F_i is algebraic.*

Subproof. It suffices to show that F_1/F_0 is algebraic, and the rest are similar.

Note that $F_1 = R/M$ is generated by the images of generators x_f of R, where R is a polynomial ring. Note that $f(\bar{x}_f) = 0$, so $\bar{x}_f$ is algebraic over F, so F_1/F is algebraic. ■

□

Remark 5.8.12. *Suppose we have $F \hookrightarrow F_{alg}$ and a finite field extension E/F. How do we embed E into F_{alg}?*

Note that there exists an embedding $E \hookrightarrow M$, such that M/F_{alg} is finite. However, $M = F_{alg}$ because F_{alg} is algebraically closed, so we get the desired embedding. Note that this embedding is not unique.

5.9 Radical Field Extensions

Definition 5.9.1 (n-Radical)**.** *Let F be a field of characteristic 0. A field extension $K = F(\alpha)$ over F is n-radical if $\alpha^n \in F$.*

Proposition 5.9.2. *Let K/F be a n-radical field extension. If $\xi_n \in F$, then K/F is a cyclic field extension of degree dividing n.*

Proof. Let $K = F(\alpha)$, and denote $a = \alpha^n \in F$. Then K/F is a splitting field of $x^n - a = \prod_{i=0}^{n-1} (x - \xi_n^i \cdot \alpha) \in K[x]$.

Let $G = \text{Gal}(K/F)$ and take $\sigma \in G$, then $\sigma(\alpha)^n = \sigma(\alpha^n) = \sigma(a) = a$, so $\sigma(\alpha)$ is a root of $x^n - a$. Therefore, denote $\sigma(\alpha) = \xi^i \cdot \alpha$ for some i. We have a well-defined map $f : G \to \mathbb{Z}/n\mathbb{Z}$ where $f(\sigma) = i + n\mathbb{Z}$. In particular, if we also take $\tau \in G$ such that $\tau(\alpha) = \xi^j \cdot \alpha$, then $(\sigma\tau)(\alpha) = \sigma(\xi^j \cdot \alpha) = \sigma(\xi^i)\sigma(\alpha) = \xi^j \cdot \xi^i \cdot \alpha = \xi^{i+j}\alpha$. Therefore, $f(\sigma\tau) = i + j + n\mathbb{Z} = f(\sigma) + f(\tau)$. Therefore, f is a homomorphism. Moreover, note that if $f(\sigma) = 0 + n\mathbb{Z}$, then $\sigma(\alpha) = \xi^0 \cdot \alpha = \alpha$, so $\sigma = \textbf{id}$. Therefore, f is injective. In particular, we have an embedding $G \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, so G is cyclic of order dividing n. □

Remark 5.9.3. *Let L/F be Galois with $G = Gal(L/F)$. The vector space $\textbf{End}_F(L)$ is also a vector space over L over, or just a L-module. In particular, every element of G is an endomorphism of L over F, so G is a subset of $\textbf{End}_F(L)$.*

Lemma 5.9.4. *G is a linearly independent subset of $\textbf{End}_F(L)$ over L.*

Proof. Suppose we have $\sum_{i=1}^{n} x_i\sigma_i = 0$ for $x_i \in L, \sigma_i \in G$, where not all $x_i = 0$. In particular, notice that the smallest number of non-zero terms is 2, then we have $x_1 \neq 0 \neq x_2$ without loss of generality, and assume that the number of non-zero coefficients is at its minimum. For all $y \in E$, we have $\sum x_i\sigma_i(y) = 0$, so $\sum x_i\sigma_i(yz) = (\sum_i x_i\sigma_i(y)\sigma_i)(z) = 0$ for any z. Multiplying the initial linear dependence by $\sigma_1(y)$, and choosing $y \in L$ so that $\sigma_1(y) \neq \sigma_y(y)$, we get by subtracting that $\sum_{i=1}^{n} x_i(\sigma_i(y) - \sigma_1(y))\sigma_i = 0$. The number of non-zero coefficients is smaller, but not zero since $x_2(\sigma_2(y) - \sigma_1(y)) \neq 0$, so we have the required contradiction. □

Proposition 5.9.5 (Hilbert Theorem 90)**.** *Let L/F be a cyclic field extension of degree n. If $\xi_n \in F$, then L/F is n-radical.*

Proof. Let σ be the generator of $\text{Gal}(L/F) = \{\textbf{id}, \sigma, \cdots, \sigma^{n-1}\}$, then consider $\sum_{k=0}^{n-1} \xi_n^{-k}\sigma^k \neq 0$. There exists $y \in L$ such that $\alpha = \sum_{k=0}^{n-1} \xi_n^{-k}\sigma^k(y) \neq 0$, and we claim that $L = F(\alpha)$. To see this, note that $\sigma(\alpha) = \sum_{i=0}^{n-1} \xi^{-i} \cdot \sigma^{i+1}(x) = \xi \cdot \sum_{i=0}^{n-1} \xi^{-(i+1)} \cdot \sigma^{i+1}(x) = \xi\alpha$. Therefore, $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n$. Here $\alpha^n \in F$, so $F(\alpha)/F$ is n-radical. Moreover, the values $\sigma^i(\alpha) = \xi_n^i \cdot \alpha$ are distinct, so $\deg(\alpha) = n$. Since $[L : F] = [F(\alpha) : F] = n$, then we have $L = F(\alpha)$. □

Definition 5.9.6 (Radical Extension). *A field extension L/F is radical if there is a tower of field extensions $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = L$ such that F_{i+1}/F_i is n_i -radical for some n_i, $i = 0, 1, \cdots, m-1$.*

Property 5.9.7.

1. *If K/F and L/K are radical, then so is L/F.*

2. *Suppose $L = F(\alpha_1, \cdots, \alpha_m)$ with $\alpha_i^{n_i} \in F$, then L/F is radical.*

3. *If K/F is radical and L/F is any field extension, then KL/L is radical.*

Lemma 5.9.8. *Every radical field extension L/F is contained in a normal radical field extension E/F.*

Proof. Let $L = F(\alpha_1, \cdots, \alpha_m)$ with $\alpha_i^{n_i} \in E_{i-1} = F(\alpha_1, \cdots, \alpha_{i-1})$ for each i, and let $L = E_m$. We induct on m. When $m = 0$, we take $E = L = F$. Suppose the result holds for $m-1$. Then we can embed E_{m-1}/F into a normal radical extension K_{m-1}/F.

$$\begin{tikzcd}
 & K_m \arrow[dd, dash] \\
E_m \arrow[ur, dashed, "\psi"] \arrow[dd, dash] & \\
 & K_{m-1} \\
E_{m-1} \arrow[ur, dash] \arrow[d, dash] & \\
F \arrow[uur, dash] &
\end{tikzcd}$$

Let K_{m-1} be the splitting field of $g \in F[x]$ over F, so K_{m-1}/F is Galois with $G = \text{Gal}(K_{m-1}/F)$. Let $L = E_{m-1}(\alpha)$ with $\alpha^n = a \in E_{m-1}$ for some n and a. Let $H = \prod_{\sigma} \sigma(m_\alpha) \in F$. Define K_m to be the splitting field of H over K_{m-1}. Then gh splits in $K_m[x]$ and $gh \in F[x]$, and K_m is generated over F by all roots of gh, as the roots of g generate K_{m-1} over F and the roots of h generate K_m over K_{m-1}. Hence K_m/F is normal, so it remains to find an embedding of E_m into K_m. Since $f = m_\alpha \mid h$ and h is split over K_m, in particular f has a root in K_m. Using this root, we embed E_m into $K_m>$ To see that K_m/F is radical, we have that K_m is generated over K_{m-1} by the roots of h. If β is a root of h, then $h(\beta) = 0$, so $(\psi f)(\beta) = 0$, hence $f(\psi^{-1}\beta) = 0$. Since $f \mid x^n - a$, we have $\psi^{-1}(\beta)^n = a$, so $\beta^n = \psi(a) \in K_{n-1}$. Thus, $K_m = K_{m-1}(\beta)$ is n-radical. □

Definition 5.9.9 (Solvable)**.** *Let $f \in F[x]$ be a polynomial over a field (of characteristic 0). We say that the equation $f(x) = 0$ is solvable by radicals if f is split in a radical extension of F.*

Theorem 5.9.10. *A non-constant polynomial $f \in F[x]$ in a field of characteristic 0 is solvable by radicals if and only if Gal(f) is solvable.*

Proof. ($\Rightarrow$): Let L/F be a radical field extension such that f is split over L. By the lemma last time, we may assume that L/F is normal, and therefore Galois. Since L/F is radical, then there exists $F_0 = F \subseteq F_1 \subseteq \cdots \subseteq F_m = L$ such that $F_{i+1} = F_i(\alpha_i)$ where $\alpha_i^{n_i} \in F_i$.

Let n be the least common multiple of n_i's. Let $F' = F(\xi_n)$ be the cyclotomic extension of F over nth roots of unity, and similarly $L' = L(\xi_n)$. Note that $L/E/F$ is a field extension where E is the splitting field of f over F.

We now construct $F_0' = F' \subseteq F_1' \subseteq \cdots \subseteq F_m' = L'$ where $F_{i+1}' = F_i'(\alpha_i)$.

Note that L/F is Galois, then L'/F' is also Galois. Let $G = \text{Gal}(L'/F')$ and $H_i = \text{Gal}(L'/F_i')$. Then $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{e\}$. Since $\xi_n \in F'$, each F_{i+1}'/F_i' is Galois cyclic, so $H_{i+1} \lhd H_i$ with $\text{Gal}(F_{i+1}'/F_i') = H_i/H_{i+1}$ cyclic. Hence G is solvable. The extension F'/F is cyclotomic, hence Abelian, so L'/F is solvable as well. Therefore, E/F is solvable because it is a factor group of $\text{Gal}(L'/F)$.

($\Leftarrow$): Suppose E/F is the splitting field of $f \in F$, take $G = \text{Gal}(f) = \text{Gal}(E/F)$ to be solvable. Let $n = |G|$, then we write $F' = F(\xi_n)$ and $E' = E(\xi_n)$. Since $\text{Gal}(E/F)$ is solvable, $\text{Gal}(E'/F') \hookrightarrow \text{Gal}(E/F)$ is solvable. Take a descending sequence of subgroups $\text{Gal}(E'/F') = H_0 \lhd H_1 \lhd \cdots \lhd H_m = \{e\}$ with H_i/H_{i+1} cyclic. Setting $F_i' = (E')^{H_i}$, we obtain a tower of cyclic extensions $F_0' = F' \subseteq F_1' \subseteq \cdots \subseteq F_m' = E'$, and $\text{Gal}(F_{i+1}'/F_i') \cong H_i/H_{i+1}$ is cyclic, so F_{i+1}'/F_i' is n_i-radical, where $n_i = [F_{i+1}'" F_i]$. Therefore, E'/F' is radical. Since $F' = F(\xi_n)$ is radical, then E'/F is radical, but $E \subseteq E'$, then E/F is radical. Hence, f is solvable by radicals. □

Example 5.9.11. *Denote $f = F[x]$ to be a non-constant polynomial. Let E/F be the splitting field so that $G = Gal(E/F) = Gal(f)$. Consider the set of roots of f in E given by $X = \{\alpha_1, \cdots, \alpha_n\}$ where $n \leq \deg(f)$. Take $\sigma \in G$, then $\sigma(\alpha_i) = \alpha_j$ for some j. Consider G acting on the set X, then there is an injective map $G \to S(X) = S_n$ since E is generated by the roots. Therefore, we can consider $G \hookrightarrow S_n$ as a subgroup.*

For example, consider $f = x^n - 1$ over $\mathbb{Q}$, then $G = (\mathbb{Z}/n\mathbb{Z})^\times \hookrightarrow S_n$. Or suppose f is generic, then $G = S_n$. In particular, if $n \leq 4$, S_n is solvable, so G is solvable, then f is *solvable by radicals. If $n \geq 5$, then S_n is not solvable, so the generic f of degree n is not solvable by radicals. Therefore, in this case we cannot write down the roots in radicals.*

Proposition 5.9.12. *Let $f \in \mathbb{Q}[x]$ be irreducible and $\deg(f) = p$ prime. Assume that f has exactly two non-real roots, then $G = Gal(f) = S_p$.*

Proof. By action on the group, we have $G \hookrightarrow S_p$. Because f is irreducible, G acts transitively on the set of p roots of f over the splitting field. Let $H \subseteq G$ be the stabilizer of some root with $[G : H] = |$ orbit of the root $| = p$. Therefore, $p \mid |G|$. By Cauchy Theorem, there exists $\sigma \in G \subseteq S_p$ such that the order is p. Therefore, σ is a p-cycle.

Moreover, note that complex conjugation τ is also in G and in S_p, it is a transposition since f has exactly two non-real complex roots, which are conjugate. However, we know that S_p is generated by a p-cycle and a transposition, so $G = S_p$. □

Example 5.9.13. $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ *is irreducible with two non-real roots, so it is not solvable by radicals over $\mathbb{Q}$.*

Lemma 5.9.14. *For every finite Abelian group G, there exists n such that there is a surjective homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \twoheadrightarrow G$.*

Proof. Write $G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$. Find distinct primes $p_1, \cdots, p_s$ such that $p_i \equiv 1 \pmod{m_i}$. Take $n = p_1 \cdots p_s$. □

Corollary 5.9.15. *For every finite Abelian group G, there is an extension $E/\mathbb{Q}$ with Galois group G.*

5.10 Kummer Theory

Definition 5.10.1 (Kummer Extension). *Let F be a field and $n > 0$ is an integer, and the characteristic of F does not divide n. Also assume that $\xi_n \in F$. Pick $a_1, a_2, \cdots, a_m \in F^\times$ and let L/F be a splitting field of the polynomial $(x^n - a_1)(x^n - a_2) \cdots (x^n - a_m)$, which is separable. Therefore, the extension is Galois. We want to study the Galois group $G = Gal(L/F)$. In particular, denote $L = F(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_m})$.*

In particular, L/F is called a Kummer extension.

Example 5.10.2. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6})$ *is a Kummer extension over $\mathbb{Q}$.*

Remark 5.10.3. *Let $A \subseteq F^\times$ be a subgroup generated by $(F^\times)^n$ and $a_1, a_2, \cdots, a_m$. Therefore $F^{\times n} \subseteq A \subseteq F^\times$, then $A/F^{\times n} \subseteq F^\times/F^{\times n}$, where the latter is a $\mathbb{Z}/n\mathbb{Z}$-module.*

By taking $a \in A$, we have $a = x^n$ for some $x \in L^\times$. Therefore note that $a_i = (\sqrt[n]{a_i})^n$ in L.

Observe that for any $\sigma \in G$, we have $(\frac{\sigma x}{x})^n = \frac{\sigma(x^n)}{x^n} = \frac{\sigma(a)}{a} = \frac{a}{a} = 1$, so $frac\sigma xx \in \mu_n \subseteq F^\times$ is a root of unity.

Suppose $x^n = a = y^n$, then $y = \xi \cdot x$ for some $\xi \in \mu_n \subseteq F^\times$, therefore $\frac{\sigma(y)}{y} = \frac{\sigma(\xi)\cdot\sigma(x)}{\xi\cdot x} = \frac{\sigma(x)}{x}$, which means the $\sigma(x)$ does not depend on choice of x. Therefore, we have $A \to \mu_n$ where $a \mapsto \frac{\sigma x}{x}$ where $x^n = a$ and $x \in L^\times$. Suppose we have $b \mapsto \frac{\sigma y}{y}$ where $y^n = b$ so $(xy)^n = ab$. Then $ab \mapsto \frac{\sigma(xy)}{xy} = \frac{\sigma x}{x} \cdot \frac{\sigma y}{y}$. Hence, the map is a homomorphism.

Also note that for $a \in A$ we have $a^n \mapsto \frac{\sigma(a)}{a} = 1$ and take $x = a \in F^\times$, so A^n is contained in the kernel of the map. Therefore, $A/A^n \to \mu_n$ is a well-defined homomorphism for all $\sigma \in G$, by sending $aA^n \mapsto \frac{\sigma x}{x}$ with $x^n = a$.

We now have a canonical map $G \times (A/A^n) \to \mu_n$ by sending $(\sigma, aA^n) \mapsto \frac{\sigma x}{x}$ where $x^n = a$. This is a homomorphism if we fix the first argument, and is linear if we fix the second argument (so bilinear). Indeed, for $\sigma, \tau \in G$ and $a \in A$, we have $(\sigma\tau, a) \mapsto \frac{\sigma\tau(x)}{x} = \frac{\sigma\tau(x)}{\sigma(x)} \cdot \frac{\sigma(x)}{x} = \sigma(\frac{\tau(x)}{x}) \cdot \frac{\sigma(x)}{x} = \frac{\sigma(x)}{x} \cdot \frac{\tau(x)}{x}$ because $\frac{\tau(x)}{x} \in \mu_n \subseteq F^\times$. This map structure is called a pairing.

We can then construct a homomorphism $\varphi : G \to \mathbf{Hom}(A/(F^\times)^n, \mu_n)$ that sends $\sigma \mapsto (\bar{a} \mapsto \frac{\sigma x}{x})$.

We want to understand $B^* = \mathbf{Hom}(B, \mu_n)$ where $n \cdot B = 0$. This is called the characteristic group of B. If $B = \mathbb{Z}/k\mathbb{Z}$ where $k \mid n$, then $\mathbf{Hom}(\mathbb{Z}/k\mathbb{Z}, \mu_n) = \mu_k$. In particular, B^* is a cyclic group of order k. Therefore, $B^* \cong B$, but not canonically.

In general, if B is finite and Abelian, then $B = \coprod C_i$ where C_i are cyclic groups such that $n \cdot C_i = 0$. Then $B^* \cong \coprod C_i^* \cong \coprod c_i \cong B$ in a non-canonically way.

In particular, observe that $\mathbf{Hom}(A/(F^\times)^n \cong A/(F^{\times n})$.

Claim 5.10.4. *φ is injective.*

Proof. Take $\sigma \in \ker(\varphi)$, with $x_i = \sqrt[n]{a_i} \in K$. Then $\sigma(\bar{a}_i) = \frac{\sigma x_i}{x_i} = 1$ so $\sigma(x_i) = x_i$ for all i. Since $K = F(x_1, \cdots, x_m)$, then $\sigma = \beth$. □

In particular, $G \hookrightarrow A/(F^{\times n})$, and since G is Abelian, then $G^n = e$ and $|G| \leq |A/(F^{\times n})|$.

Denote $\psi : A/(F^\times)^n \to \mathbf{Hom}(G, \mu_m)$.

Claim 5.10.5. *ψ is injective.*

Proof. Let $\bar{a} \in A/(F^\times)^n$ such that $\psi(\bar{a}) = e$.

$\psi(\bar{a})$ takes $\frac{\sigma x}{x}$ where $x^n = a$. But since $\psi(\bar{a}) = e$, then $\frac{\sigma x}{x} = 1$ for all σ, hence $x \in K^G = F$, so $\alpha = x^n \in (F^\times)^n$, so $\bar{a} = e$. □

Note $\mathbf{Hom}(G, \mu_m) = G^* \cong G$*. Then* $|A/(F^\times)^n| \leq |G|$*, so* $|A/(F^\times)^n| = |G|$*. Therefore,* φ *and* ψ *are isomorphisms.*

Theorem 5.10.6 (Kummer)**.** *Let* F *be a field and* $n > 0$ *is an integer, with* $char(F) \nmid n$*. Let* $a_1, \cdots, a_n \in F^\times$*, and* K *is the splitting field of* $(x^n - a_1)(x^n - a_2)\cdots(x^n - a_m)$*. Then* K/F *is Galois and the map* $\varphi : G \to \mathbf{Hom}(A/(F^\times)^n, \mu_n)$ *is an isomorphism, where* $G = Gal(K/F)$*. (*$A \subseteq F^\times$ *is a subgroup generated by* $(F^\times)^n$ *and* a_i*.)*

Example 5.10.7. *Consider* $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15})/\mathbb{Q}$*. We just need to look at* $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \ni \langle \bar{2}, \bar{5}, \bar{6}, \bar{1}0, \bar{1}5 \rangle$*, which is a vector space over* $\mathbb{F}_2$*.*

So we can write $\{\bar{-1}, \bar{2}, \bar{3}, \bar{5}, \cdots\}$ *as a basis of* $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$*, so* $\bar{2} = \bar{2}$*,* $\bar{5} = \bar{5}$*,* $\bar{6} = \bar{2} \cdot \bar{3}$*,* $\bar{1}0 = \bar{2} \cdot \bar{5}$ *and* $\bar{1}5 = \bar{3} \cdot \bar{5}$*, then we can express these elements by basis elements* $\{2, 3, 5\}$*.*

Therefore, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15})/\mathbb{Q} = (\mathbb{Z}/2\mathbb{Z})^3$*.*

Remark 5.10.8. *Suppose* $\sigma \in G$*, then* $\varphi(\sigma) = f : A/(F^\times)^n \to \mu_n$*. By taking* $a_i \in A$*, then* $x_i = \sqrt[n]{a_i}$ *satisfies* $x_i^n = a_i$*. Now* $\sigma(x_i) = \sigma(\sqrt[n]{a_i}) = f(\bar{a}_i)$*. Then* $\sigma(\sqrt[n]{a_i}) = f(\bar{a}_i) \cdot \sqrt[n]{a_i}$ *where* $f(\bar{a}_i) \in \mu_n$*.*

5.11 Infinite Galois Field Extensions

Definition 5.11.1. *Consider* L/F *to be an algebraic extension, but should be an infinite extension. We say* L/F *is separable if every element of* L *is separable over* F*.* L/F *is normal if the following equivalent conditions holds:*

1. L *is a splitting field of a set of polynomials over* F*.*

2. *Every irreducible polynomial in* $F[x]$ *that has a root in* L *is split over* L*.*

3. L *is the union of all subfields* K *such that* $F \subseteq K \subseteq L$ *such that* K/F *is finite and normal.*

We say L/F *is Galois if* L/F *is separable and normal. Denote* $G = Gal(L/F)$ *to be the group of automorphisms* $\sigma : L \to L$ *that is identity over* F*.*

Remark 5.11.2. *Let* L/F *be a Galois field extension with* $G = Gal(L/F)$*. We can write* $L = \bigcup_{i \in I} L_i$ *where* L_i/F *is finite and Galois. Take* $\sigma \in G$*, then* $\sigma(L_i) = L_i$*, so we can* *restrict σ to L_i and get an automorphism $\sigma\mid_{L_i}: L_i \to L_i$ over F. Therefore, we have $G \to Gal(L_i/F)$ that sends $\sigma \mapsto \sigma\mid_{L_i}$.*

Suppose I is ordered, with $i < j$ if $L_i \subseteq L_j$. We can view I as a small preorder category, with $L_j \to L_i$ a morphism in the category if $L_i \subseteq L_j$. Then we have $G \to \prod_{i\in I} Gal(L_i/F)$, with $(\sigma\mid_{L_j}\mid_{L_i} = \sigma\mid_{L_i}$, then we have the map $G \to \lim_{i\in I} Gal(L_i/F)$ and can be expressed explicitly as $\{(\sigma_i)_{i\in I} : \sigma_j \mid_{L_i} = \sigma_i$ when $i < j\}$, expressed as an inverse limit of finite groups. We can show that this map is an isomorphism. Then G is a profinite group.

Moreover, this is a topological group. We observe that the finite group has discrete topology, then the product of those groups gives a product topology. The product of compact spaces is still quasi-compact. The limit is a closed subset in the product, so it is also quasi-compact. Therefore, G is quasi-compact. (Profinite groups are quasi-compact.) For example, $\mathbb{Z}$ cannot be a Galois group because we cannot introduce any non-trivial topology on $\mathbb{Z}$ so that it becomes quasi-compact.

Also, G is Hausdorff.

Definition 5.11.3 (Profinite Group)**.** *A group that is isomorphic to a limit of finite groups is called a profinite group.*

Remark 5.11.4. *Suppose L/F is a Galois field extension, and $G = Gal(L/F)$, and let $L/K/F$ be an intermediate extension. Then L/K is also Galois and $H = Gal(L/K) \subseteq G$ is a subgroup. Therefore, $H = \{\sigma \in G : \sigma\mid_K = \mathbf{id}_K\}$. But K is a union of finite field extensions, so $K = \bigcup_i K_i$, where K_i/F is finite, then $H = \{\sigma \in G : \sigma\mid_K = \mathbf{id}_K\} = \bigcap_i \{\sigma \in G : \sigma\mid_{K_i} = \mathbf{id}_{K_i}\} = \bigcap_i Gal(L/K_i)$. Moreover, note that $H_i = Gal(L/K_i) \subseteq G$ is open in the topology, and $G = \bigcup_i gH_i$ where each coset is open, and there are finitely many of them, so the coset gH_i is closed. Therefore, $H = Gal(L/K)$ is closed in G.*

Theorem 5.11.5. *Suppose $G = Gal(L/F)$, then the set of intermediate fields in L/F and the set of closed subgroups in G are isomorphic: on one hand, we send an intermediate field K to $Gal(L/K)$, and on the other hand, we send a closed subgroup H to L^H. The two maps are bijection inverses of each other.*

Example 5.11.6.

1. *For a field F embedded into the algebraic closure $F \hookrightarrow F_{alg}$, this embedding is not a Galois extension because it is not necessary separable. Instead, we take $F_{sep} \subseteq F_{alg}$ of all separable elements. Then F_{sep}/F is Galois, and F_{sep} is called the separable closure of F. Therefore, $\Gamma_F := Gal(F_{sep}/F)$ is called the absolute Galois group of field F.*

In particular, Gal$(K/F) = \Gamma_F/\Gamma_K$, with $F_{sep} = K_{sep}$. We don't really understand the structure, even for $\Gamma_{\mathbb{Q}}$ at this point.

2. $\Gamma_{\mathbb{R}} = \mathbb{Z}/2\mathbb{Z}$.

3. *Suppose F is a finite field $\mathbb{F}_q$, then there exists exactly one extension of this field of degree n, namely $\mathbb{F}_{q^n}/\mathbb{F}$. The Galois group of this field extension is canonically isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Then $\Gamma_F = \lim \mathbb{Z}/n\mathbb{Z} = \{(a_n \in \mathbb{Z}/n\mathbb{Z}) : \forall k \mid n, a_k \equiv a_n \pmod{k}\mathbb{Z}\}$. This group is known as the completion of $\mathbb{Z}$, namely the group of profinite integers $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, as the product of all p-adic integers with prime p. This group has the cardinality continuum. We then have $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$ as a dense embedding. Note $\mathbb{Z}$ is not a Galois group but $\hat{\mathbb{Z}}$ is an absolute Galois group.*

6 Hilbert's Nullstellensatz

6.1 Hilbert Basis Theorem

Definition 6.1.1 (ACC,DCC)**.** *Let R be a ring and M is a (left) R-module.*

The ascending chain condition (ACC) is that every sequence $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ of submodules of M is stable, i.e. there exists some $m \in \mathbb{N}$ such that $M_k = M_m$ for all $k \geq m$.

The descending chain condition (DCC) is that every sequence $M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \cdots$ of submodules of M is stable, i.e. there exists some $m \in \mathbb{N}$ such that $M_k = M_m$ for all $k \geq m$.

Proposition 6.1.2. *Let R be a ring and M is a (left) R-module. The following are equivalent:*

1. *ACC (respectively, DCC) condition.*

2. *Every non-empty set of submodules of M has a maximal (respectively, minimal) element.*

Definition 6.1.3. *Let R be a ring. Let M be a (left) R-module. We say M is Noetherian (respectively, Artinian) if M satisfies ACC (respectively, DCC).*

R is a (left) Noetherian (respectively, Artinian) if R as a (left) module over R is Noetherian (respectively, Artinian).

Example 6.1.4. *1. Fields are Noetherian and Artinian.*

2. $\mathbb{Z}$ is Noetherian but not Artinian.

Proposition 6.1.5. *Let $0 \to N \to M \xrightarrow{f} P \to 0$ be a short exact sequence of (left) R-modules. Then M is Noetherian (respectively, Artinian) if and only if both N and P are.*

Proof. We only prove the case for Noetherian. The case for Artinian is analogous.

($\Rightarrow$): consider $N_1 \subseteq N_2 \subseteq \cdots \subseteq N \hookrightarrow M$ and $P_1 \subseteq P_2 \subseteq \cdots \subseteq P$, so the sequence is stable and N is Noetherian. Moreover, consider $f^{-1}(P_1) \subseteq f^{-1}(P_2) \subseteq \cdots \subseteq f^{-1}(P) = M$, then it is stable, and so $\{P_i\}_{i\geq 1}$ is stable.

($\Leftarrow$): Take $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$. Then $f(M_1) \subseteq f(M_2) \subseteq \cdots \subseteq P$ is stable. Hence, $M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots \subseteq N$ is stable. Therefore, there exists some n such that $f(M_k) = f(M_n)$ and $M_k \cap N = M_n \cap N$ for all $k \geq n$. Therefore, $M_k = M_n$ for all $k \geq n$, so $\{M_n\}_{n\geq 1}$ is stable. □

Corollary 6.1.6. *If $M_1, \cdots, M_n$ are Noetherian (respectively, Artinian), then so is $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.*

Proposition 6.1.7. *Suppose $f : R \to S$ is a surjective ring homomorphism. Let M be a (left) S-module. Then M is a Noetherian (respectively, Artinian) S-module if and only if M is a Noetherian (respectively, Artinian) R-module.*

Proof. Again, we only prove the case for Noetherian. A similar proof works for the Artinian case.

($\Rightarrow$): Consider $N_1 \subseteq N_2 \subseteq \cdots \subseteq M$ as a chain of R-submodules. These are S-submodules by surjectivity of f. Therefore, we conclude stability.

($\Leftarrow$): Consider $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$ as S-submodules. Then they are also R-submodules, so they are stable as well. □

Corollary 6.1.8. *Suppose $f : R \to S$ is a surjective ring homomorphism. If R is (left) Noetherian (respectively, Artinian), so is S.*

Proof. Because R is Noetherian (respectively, Artinian), then S is also Noetherian (respectively, Artinian) as R-module, then S is Noetherian (respectively, Artinian) as a S-module by proposition. □

Proposition 6.1.9. *Suppose R is a (left) Noetherian (respectively, Artinian). Then every finitely generated (left) R-module is Noetherian (respectively, Artinian).*

Proof. If R is Noetherian (respectively, Artinian), then R^n is also Noetherian (respectively, Artinian). Therefore, the factor module $M = R^n/N$ is Noetherian (respectively, Artinian). □

Proposition 6.1.10. *Every Noetherian R-module is finitely generated.*

Remark 6.1.11. *This proposition acts as the converse of the previous proposition, and it only holds for Noetherian modules.*

Proof. Suppose M is a Noetherian R-module that is not finitely generated, then we consider the following chain: we first take $N_1 = Rm_1$ for $m_1 \in M$. Then $N_1 \neq M$. Take $N_2 = Rm_1 + Rm_2$ for $m_2 \in M \backslash N_1$. Then $N_2 \neq M$. We proceed inductively, and we get a chain of modules $N_1 \subseteq N_2 \subseteq \cdots$ that is not stable and each module is finitely generated. □

Proposition 6.1.12. *Let R be a (left) Noetherian ring. Every submodule of a finitely-generated (left) R-module is finitely generated.*

Proof. Suppose we have a submodule $N \subseteq M$ where M is a finitely-generated module. Then M is Noetherian, so N is Noetherian, then N is finitely generated. □

Proposition 6.1.13. *Let R be a ring. It is a (left) Noetherian ring if and only if every ideal of R is finitely generated.*

Proof. ($\Rightarrow$): Take $I \subseteq R$ as a (left) ideal, then it is a (left) R-module, so it is finitely generated.

($\Leftarrow$): Consider a chain $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$, then $I = \bigcup\limits_{k=1}^{\infty} I_k$ is a (left) ideal, and is finitely generated. Let $I = (x_1, \cdots, x_n)$. Then $\{x_1, \cdots, x_n\} \subseteq I_N$ for some N. Therefore, $I = I_N = I_{N+1} = \cdots$, so the sequence is stable. □

Theorem 6.1.14 (Hilbert Basis Theorem)**.** *Let R be a (left) Noetherian ring. Then so is $R[x_1, \cdots, x_n]$.*

Proof. It suffices to show that $R[x]$ is a Noetherian ring, the rest just follows from induction. We show that every left ideal is finitely generated. Let $I \subseteq R[x]$ be a left ideal. Now for all $f \in I$, we write $f = a_n x^n + \cdots + a_0$. Look at $J = \{$ highest coefficients $a_n \in I\} \subseteq R$. Then J is a (left) ideal, so it is finitely generated by $\{a_1, \cdots, a_n\}$. Let $f_i \in I$ have highest coefficient a_i and degree n_i. Let $n = \max\limits_i n_i$.

Consider $M = R \oplus Rx \oplus \cdots Rx^{n-1}$. It is a free finitely generated R-submodule of $R[x]$ because it is Noetherian.

Therefore, $I \cap M \subseteq M$ is finitely generated by $g_1, \cdots g_s$ as a R-module.

Claim 6.1.15. *I is generated by $f_1, \cdots, f_m, g_1, \cdots, g_s$ as a $R[x]$-module. Take $h \in I$. We induct on* $\deg(h)$*.*

Subproof. Suppose $\deg(h) < n$, then $h \in I \cap M$ and is generated by $g_1, \cdots, g_s$.

Suppose $\deg(h) \geq n$, then we use induction. Let $h = ax^r + \cdot$, then a is generated by $a_1, \cdots, a_n$. Then there is some linear combination $\sum\limits_i b_i x^{r_i} f_i$ with highest term ax^r. Therefore, $h - \sum\limits_i b_i x^{r_i} f_i$ has degree one less. By induction, it is generated by f_i's and g_j's. Therefore, h is generated by f_i's and g_j's. ■

□

6.2 Hilbert's Nullstellensatz

Definition 6.2.1 (Finite, Finite Type)**.** *Suppose there is a commutative ring S with a commutative subring R. We say S is finite overR is S is a finitely generated R-module. So there exists $s_1, \cdots, s_n$ such that for all $s \in S$, $s = \sum\limits_i \tau_i s_i$ where $\tau_i \in R$.*

We say S is of finite type over R if S is finitely generated as a ring over R. Therefore, there exists $s_1, \cdots, s_n \in S$ such that for all $s \in S$, $s = f(s_1, \cdots, s_n)$ for some $f \in R[x_1, \cdots, x_n]$.

Remark 6.2.2. *Finite implies finite type, but not the other way around.*

Hilbert's Nullstellensatz shows when does the two notions become the same.

Corollary 6.2.3 (From Hilbert's Basis Theorem)**.** *Let $R \subseteq S$ be commutative rings, S of finite type over R. If R is Noetherian, then so is S.*

Proof. Let $s_1, \cdots, s_n \in S$ be generators. Then there is a surjective homomorphism given by $R[x_1, \cdots, x_n] \twoheadrightarrow S$ given by $x_i \mapsto s_i$. Note that by Hilbert's Basis theorem, we know $R[x_1, \cdots, x_n]$ is a Noetherian ring. Therefore, S is Noetherian. □

Lemma 6.2.4. *Let $R \subseteq S \subseteq T$ be commutative rings such that*

1. *R is Noetherian.*

2. *T is of finite type over R.*

3. *T is finite over S.*

Then S is of finite type over R.

Proof. Let $T = R[x_1, \cdots, x_n]$ where x_i's are generators of T over R. Moreover, $T = \sum_{j=1}^{m} S \cdot y_j$ for $y_j \in T$. Then $x_i = \sum_j a_{ij} y_j$ where $a_{ij} \in S$ and $y_i y_j = \sum_k b_{ijk} y_k$ where $b_{ijk} \in S$.

Let $S_0 = R[a_{ij}, b_{ijk}]$ be generated by the two sets of coefficients. Then $R \subseteq S_0 \subseteq S \subseteq T$. By the corollary, S_0 is Noetherian.

Claim 6.2.5. *T is finite over S_0. We can show that $T = \sum_j S_0 \cdot y_j$.*

Subproof. Recall that $\sum S_0 y_j$ and $y_i y_j \in \sum S_0 \cdot y_j$. Then $y_i y_j y_k \in \sum_i S_0 y_j y_k \in \sum S_0 y_j$. ■

Now $S \subseteq T$ is a S_0-submodule, and T is a finitely generated S_0-module.

Since S_0 is Noetherian, S is a finitely-generated S_0-module. Therefore, S is finite over S_0, and so it is of finite type over S_0. However, S_0 is finite type over R, so S is of finite type over R. □

Proposition 6.2.6. *Let E/F be a field extension such that E is of finite type (as a ring) over F. Then E is finite over F, i.e. $[E : F] < \infty$.*

Proof. We first prove a special case, that is suppose $E = F(x_1, \cdots, x_n)$ where x_i's are algebraically independent.

Claim 6.2.7. *$E = F$.*

Proof. Since E is of finite type over F, then $E = F[f_1, \cdots, f_m]$ where $f_i = \frac{g_i}{h}$ for $g_i, h \in F[x_1, \cdots, x_n]$. Note that every element in E is of the form $\frac{g}{h^k}$, for $g \in F[x_1, \cdots, x_n]$. Suppose $n > 0$, then there exists an irreducible polynomial $p \in F[x_1, \cdots, x_n]$ such that $p \nmid h$. Therefore, $\frac{1}{p}$ is not of the form $\frac{g}{h^k}$ in E, contradiction. Therefore, $n = 0$. Hence, $E = F$. ■

We now prove the general case, with $E = F[f_1, \cdots, f_m] = F(f_1, \cdots, f_m)$. Choose a maximal algebraically independent subset in $\{f_1, \cdots, f_m\}$, denoted $\{f_1, \cdots, f_k\}$ without loss of generality.

Let $K = F(f_1, \cdots, f_k)$, then $K \cong F(x_1, \cdots, x_k)$. On the other hand, if we add f_i to the set where $i > k$, then the set is algebraically dependent. Therefore, f_i is algebraic over $\{f_1, \cdots, f_k\}$. Hence, f_i is algebraic over K for all $i \in \{1, \cdots, m\}$. Therefore, E/K is algebraic and is finitely-generated. Therefore, E/K is finite.

By lemma, K is of finite type over F. But $K = F(x_1, \cdots, x_k)$ is also purely transcendental. By the special case, $K = F$, so $[E : F] < \infty$. □

Theorem 6.2.8 (Hilbert's Nullstellensatz, Weak Form)**.** *Let F be an algebraically closed field. Let $f_1, \cdots, f_m \in F[x_1, \cdots, x_n] = R$. The following are equivalent:*

1. *There is no $a = (a_1, \cdots, a_n) \in F^n$ such that $f_i(a) = 0$ for all i.*
2. *f_i generates the unit ideal in $R = F[x_1, \cdots, x_n]$.*

Proof. (2) $\Rightarrow$ (1): If we have a linear combination $\sum\limits_i f_i g_i = 1$, then $\sum\limits_i f_i(a)g_i(a) = 1$. Then there exists i such that $f_i(a) \neq 0$.

(1) $\Rightarrow$ (2): Suppose $R \neq \sum\limits_i f_i R \subseteq M$ for some maximal ideal M. Now $F \hookrightarrow R \twoheadrightarrow R/M$ into the field gives a field extension of F and is of finite type over F. By proposition, it is a finite field extension. But F is algebraically closed. Then it is the trivial extension. Hence, $F \xrightarrow{\cong} R/M$ that sends $a_i \mapsto \bar{x}_i$, $f_j \mapsto \overline{f_i(x_1, \cdots, x_n)} = 0$ since f_j's are in M.

Then $f_i(a) = 0$ for all j, contradiction. □

Remark 6.2.9. *If F is not algebraically closed, e.g. $\mathbb{R}$, we have $x^2 + 1$ with no roots, but it does not generate the unit ideal.*

Theorem 6.2.10 (Hilbert's Nullstellensatz, Alternate Weak Form)**.** *Let K be a field and L is a K-algebra such that L is finitely-generated as a K-algebra and is a field, then L is algebraic over K, and L/K is a finite field extension.*

Corollary 6.2.11. *Suppose, in addition to the above alternate form, that K is algebraically closed, then every maximal ideal of $A = K[X_1, \cdots, X_n]$ is of the form*

$$\mathfrak{m} = (X_1 - a_1, \cdots, X_n - a_n)$$

for some $a_1, \cdots, a_n \in K$; the map $K[X_1, \cdots, X_n] \to K[X_1, \cdots, X_n]/\mathfrak{m} = K$ is given by the natural evaluation map. Hence, there is a natural one-to-one correspondence between K^n and ideals A in Spec$(\mathfrak{m})$ given by $(a_1, \cdots, a_n) \leftrightarrow (X_1 - a_1, \cdots, X_n - a_n)$.

Definition 6.2.12 (Variety)**.** *Let K be a field. A variety $V \subseteq K^n$ is a subset of the form*

$$V = V(J) = \{P = (a_1, \cdots, a_n) \in K^n \mid f(P) = 0 \ \forall f \in J\},$$

where $J \subseteq K[X_1, \cdots, X_n]$ is an ideal. Note that $J = (f_1, \cdots, f_m)$ is finitely generated, so that a variety V is defined by

$$f_1(P) = \cdots = f_m(P) = 0,$$

that is, it is a subset $V \subseteq K^n$ defined as the simultaneous solutions of a number of polynomial equations.

Proposition 6.2.13. *Suppose K is an algebraically closed field and that $A = K[x_1, \cdots, x_n]$ is a finitely-generated K-algebra of the form $A = K[X_1, \cdots, X_n]/J$ where J is an ideal of $K[X_1, \cdots, X_n]$, then every maximal ideal of A is of the form $(x_1 - a_1, \cdots, x_n - a_n)$ for some point $(a_1, \cdots, a_n) \in V(J)$. Therefore, there is a one-to-one correspondence between $V(J)$ and maximal ideals of A given by $(a_1, \cdots, a_n) \leftrightarrow (X_1 - a_1, \cdots, X_n - a_n)$.*

Proof. The ideals of A are given by ideals of $K[X_1, \cdots, X_n]$ containing J, so every maximal ideal of A is of the form $(x_1 - a_1, \cdots, x_n - a_n)$ for some $a_1, \cdots, a_n$ such that $J \subseteq (X_1 - a_1, \cdots, X_n - a_n)$. However, since $(X_1 - a_1, \cdots, X_n - a_n)$ is just the kernel of the evaluation map on f, it then follows that $J \subseteq (X_1 - a_1, \cdots, X_n - a_n)$ if and only if $f(a_1, \cdots, a_n) = 0$ for all $f \in J$, i.e. $(a_1, \cdots, a_n) \in V(J)$. □

More formally, we have the following correspondence.

Remark 6.2.14. *A variety $X \subseteq K^n$ is by definition equal to $X = V(J)$ for some ideal J of $K[X_1, \cdots, X_n]$, so V gives a map from the set of ideals of $K[X_1, \cdots, X_n]$ to the subsets of K^n. Conversely, there is a map I from subsets of K^n to ideals of $K[X_1, \cdots, X_n]$, defined by taking a subset $X \subseteq K^n$ into the ideal*

$$I(X) = \{f \in K[X_1, \cdots, X_n] \mid f(P) = 0 \ \forall P \in X\}.$$

One important property is that: if $J \subseteq J'$, then $V(J) \supseteq V(J')$; if $X \subseteq Y$, then $I(X) \supseteq I(Y)$. Moreover, $X \subseteq V(I(X))$ for any subset X, and $X = V(I(X))$ if and only if X is a variety. Conversely, $J \subseteq I(V(J))$ for any ideal J.

Theorem 6.2.15 (Hilbert's Nullstellensatz, Strong Form)**.** *Let F be an algebraically closed field. Let $f_1, \cdots, f_m, f \in F[x_1, \cdots, x_n] = R$. The following are equivalent:*

1. *If $a \in F^n$ is such that $f_i(a) = 0$ for all i, then $f(a) = 0$.*
2. *There exists $k > 0$ such that $f^k \in \sum R \cdot f_i$, so f is in the radical $\sqrt{\sum R \cdot f_i}$.*

Proof. (2) ⇒ (1): For the k as specified, we have $f^k = \sum\limits_i f_i g_i$, so $f(a)^k = 0$, then $f(a) = 0$.

(1) ⇒ (2): Consider $R[t] = F[x_1, \cdots, x_n, t]$. Now let $f_{m+1} = 1 - t \cdot f \in S \ni f_1, \cdots, f_m$. Note $f_1, \cdots, f_{m+1}$ have no common zero: if $f_1(a) = \cdots = f_{m+1}(a) = 0$, then $f(a) = 0$,

so $f_{m+1}(a) = 1$. By the weak form of the Nullstellensatz, $f_1, \cdots, f_{m+1}$ generate the unit ideal in S, so $1 = \sum\limits_{i=1}^{m} f_i g_i + f_{m+1} g_{m+1}$ for $g_1, \cdots, g_{m+1} \in S$.

Let $t = \frac{1}{f}$ in $F(x_1, \cdots, x_n)[t]$, then f_{m+1} vanishes: $1 = \sum\limits_{i=1}^{m} f_i \cdot \tilde{g_i}$ where $\tilde{g_i} = \frac{h_i}{f^k}$ where $h_i \in R$. Therefore, $f^k = \sum\limits_{i=1}^{m} f_i h_i \in \sum R \cdot f_i$. □

Theorem 6.2.16 (Hilbert's Nullstellensatz, Alternate Strong Form)**.** *Let K be an algebraically closed field. Then:*

1. *If $J \subsetneq K[X_1, \cdots, X_n]$, then $V(J) \neq \varnothing$.*

2. *$I(V(J))$ is the radical of J. Therefore, for $f \in K[X_1, \cdots, X_n]$, $f(P) = 0$ for all $P \in V$ if and only if $f^n \in J$ for some n.*

Proposition 6.2.17. *Let F be an algebraically closed field and set $R = F[x_1, \cdots, x_m]$, with $a = (a_1, \cdots, a_n) \in F^n$. We define $M_a = \{f \in R : f(a) = 0\}$ to be an ideal in R. Then*

1. *M_a is a maximal ideal in R.*

2. *Every maximal ideal of R is $M - a$ for $a \in F^n$.*

Proof. 1. Denote $\alpha_a : R \twoheadrightarrow F$ that sends $f \mapsto f(a)$ to be a surjective ring homomorphism. By the first isomorphism theorem, $M_a = \ker(\alpha_a)$, so $R/M_a \cong F$ is a field, then M_a is maximal.

2. Take $M \subseteq R$ as a maximal ideal, so $M = \sum\limits_{i=1}^{m} f_i R_i$ for some $f_i \in R$. By Hilbert's Nullstellsatz, there exists $a \in F^n$ such that $f_i(a) = 0$ for all i. Then for all $g \in M$, $g(a) = 0$, so $M \subseteq M_a$. But M is maximal, so $M = M_a$.

□

Definition 6.2.18 (Irreducible Variety)**.** *A variety $X \subseteq K^n$ is irreducible if it is non-empty and not the union of two proper subvarieties, i.e. $X = X_1 \cup X_2$ as varieties if and only if $X = X_1$ or $X = X_2$.*

Proposition 6.2.19. *A variety X is irreducible if and only if $I(X)$ is prime.*

Proof. Set $I = I(X)$; if I is not prime, take $f, g \in A\backslash I$ such that $fg \in I$; now define ideals $J_1 = (I, f)$ and $J_2 = (I, g)$. Since $f \notin I(X)$, then $V(J_1) \subsetneq X$, and similarly $V(J_2) \subsetneq X$, and so $X = V(J_1) \cup V(J_2)$ must be reducible. We can prove the converse in a similar manner. □

Corollary 6.2.20. *Let K be a algebraically closed field. Then there is a one-to-one correspondence between V and I:*

1. *Radical ideals J of $K[X_1, \cdots, X_n]$ corresponds to varieties $X \subseteq K^n$.*
2. *Considering the subsets of the two structure, we have a second correspondence: prime ideals P of $K[X_1, \cdots, X_n]$ corresponds to the irreducible varieties $X \subseteq K^n$.*

Proposition 6.2.21. *Let $A = K[x_1, \cdots, x_n]$ be a finitely generated K-algebra where K is an algebraically closed field; write J for the ideal of relations holding between $x_1, \cdots, x_n$, so that $A = K[X_1, \cdots, X_n]/J$. Then there is the one-to-one correspondence between the prime ideals of A and irreducible subvarieties $X \subseteq V(J)$.*

Proof. We know that maximal ideals correspond one-to-one with points of $V(J)$. Moreover, because prime ideals of A correspond to prime ideals of $K[X_1, \cdots, X_n]$ containing J, then by the above corollary, every prime ideal P of A is of the form $P = I(X)$ modulo J for an irreducible variety $X \subseteq K^n$ with $J \subseteq P = I(X)$. This condition is equivalent to $V(J) \supseteq V(P) = V(I(X)) = X$. □

The concept of variety is deeply connected with Zariski topology.

7 Dedekind Domain

7.1 Definitions

Definition 7.1.1 (Product Ideal)**.** *Let R be a domain, and $I, J \subseteq R$ are ideals, then the product ideal IJ is the ideal generated by xy for $x \in I$ and $y \in J$. Note $xR \cdot yR = xyR$.*

Example 7.1.2. *Consider $R = \mathbb{Z}[\sqrt{-5}]$, but $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, so R does not have unique factorization. Indeed, note $2R \cdot 3R = (1+\sqrt{-5})R \cdot (1-\sqrt{-5})R$.*

Consider $P_1 = 2R + (1+\sqrt{-5})R = \langle 2, 1+\sqrt{-5}\rangle$. Then

$$2 \in P_1^2 = \langle 4, 2+2\sqrt{-5}, (1+\sqrt{-5})^2 = -4+2\sqrt{-5}\rangle = 2R.$$

Therefore, $P_1 = 2R$ is not a principal ideal domain.

Consider $P_2 = \langle 3, 1+\sqrt{-5}\rangle$ and $P_3 = \langle 3, 1-\sqrt{-5}\rangle$. Now

$$3 \in P_2 \cdot P_3 = \langle 9, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6\rangle = 3R.$$

Also note that $P_1 \cdot P_2 = \langle 6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, (1+\sqrt{-5})^2\rangle = (1+\sqrt{-5})R$ and $P_1 \cdot P_3 = (1-\sqrt{-5})R$ by similar calculations.

In particular, we have $P_1^2 \cdot P_2P_3 = P_1P_2 \cdot P_2P_3$. Notice that we have uniqueness in this case. The ideal is factored into unique prime ideals, which is the point of Dedekind domains.

Definition 7.1.3 (Divisible)**.** *Let $A, B \subseteq R$ be ideals where $B \neq 0$. We say A is divisible by B if there exists an ideal $C \subseteq R$ such that $A = BC \subseteq B$. We denote $B \mid A$. In particular, $A \subseteq B$.*

Remark 7.1.4. *Notice that $bR \mid aR$ if and only if $aR \subseteq bR$ if and only if $b \mid a$, which holds for principal ideals. However, in general, this is false.*

Example 7.1.5. *Consider $R = F[x, y]$, where $A = xR$, $B = xR + yR$, then $A \subseteq B$ but $B \nmid A$.*

Definition 7.1.6 (Dedekind Ring). *A domain R is a Dedekind ring if for every two ideals $A \subseteq B \subseteq R$, there is an ideal $C \subseteq R$ such that $A = BC$. We say C is the quotient in this case.*

Example 7.1.7. *Every PID is Dedekind.*

Property 7.1.8 (Cancellation Law). *Suppose $A, A', B \subseteq R$ are non-zero ideals for Dedekind ring R. If $AB = A'B$, then $A = A'$.*

Proof. Take $0 \neq b \in B$, then $bR \subseteq B$. Therefore, there exists an ideal $C \subseteq R$ such that $bR = BC$. Then $ABC = A'BC$, so $Ab = A'b$, which means $A = A'$. □

Proposition 7.1.9. *Every ideal of a Dedekind ring R is a finitely generated projective R-module.*

Proof. Take $0 \neq A \subseteq R$ as an ideal. Then $\exists 0 \neq a \in A$, so $aR \subseteq A$. Hence, there exists ideal $B \subseteq R$ such that $aR = AB$. In particular, $a = \sum\limits_{i=1}^{n} x_{-}y_i$ where $x_i \in A$ and $y_i \in B$. Define

$$\begin{aligned} f : R^n &\to A \\ (\tau_1, \cdots, \tau_n) &\mapsto \sum_{i=1}^{n} \tau_i x_i \in A \\ g : A &\to R^n \\ x &\mapsto (\frac{xy_1}{a}, \cdots, \frac{xy_n}{a}) \in R^n \end{aligned}$$

Note $x \in A, y \in B$, then $xy \in AB = aR$, so $\frac{xy}{a} \in R$. Then $(f \circ g)(x) = f(g(x)) = \sum\limits_{i=1}^{n} \frac{xy_i}{a} x_i = x$. Therefore, $f \circ g = 1_A$. We then have

$$\begin{tikzcd} 0 \arrow[r] & \ker(f) \arrow[r] & R^n \arrow[r, "f"] & A \arrow[r] \arrow[l, bend left, "g"] & 0 \end{tikzcd}$$

splits.

Therefore, $R^n = \ker(f) \oplus A$, so A is a finitely-generated projective module. □

Corollary 7.1.10. *Every Dedekind ring is Noetherian.*

Definition 7.1.11 (Krull Dimension). *If R is a commutative ring, consider a chain of $n + 1$ prime ideals*

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

where we call this chain of length n. The dimension $\dim(R)$ is the maximal length of chain of prime ideals in R. This is the Krull dimension.

Example 7.1.12.

1. *For a field F, $\dim(F) = 0$.*

2. *For a PID R, $\dim(R) = 1$; $\dim(\mathbb{Z}) = 1$.*

3. *Suppose R is a domain. Note that 0 is prime. Therefore, $\dim(R) \leq 1$ if and only if every non-zero prime ideal is maximal.*

4. $\dim(F[x_1, \cdots, x_n]) = n$.

Proposition 7.1.13. *If R is a Dedekind ring, $\dim(R) \leq 1$.*

Proof. Let $P \subseteq R$ be a non-zero prime ideal. Suppose, towards contradiction, that P is not maximal. Suppose $Q \supseteq P$ a prime ideal, then there exists an ideal $A \subseteq R$ such that $P = Q \cdot A$. Hence, either $Q \subseteq P$ or $A \subseteq P$. If not, then there exists $xinQ \backslash P$ with $y \in A \backslash P$ and $xy \notin P$, contradiction.

Suppose $A \subseteq P$, then $QA \subseteq QP$, but then we know $P = QA \subseteq QP \subseteq P$. Therefore, $QA = QP$, so $A = P$, but $P = QP$, then $RP = P = QP$, which means $R = Q$, contradiction. Therefore, $P = Q$, another contradiction. □

Theorem 7.1.14. *Let R be a Dedekind domain. Then every non-zero ideal $I \subseteq R$ is a product of primes: $I = P_1 P_2 \cdots P_n$. The prime ideals $P_1, \cdots, P_n$ are unique up to permutation.*

Proof. Clearly we know R is Noetherian.

Let $A = \{I \subseteq R \text{ ideal } : I \neq 0, I \neq R, I \text{ is not such product } \}$. Suppose $A \neq \varnothing$, then it has a maximal element I. In particular, $I \neq R$, and there exists a maximal ideal $M \subseteq R$ such that $I \subseteq M \notin A$.

There exists an ideal $Y \subseteq R$ such that $I = M \cdot Y \subsetneq Y = R \cdot Y$. Clearly $Y \neq R$, otherwise $I = M$. Therefore, $y \notin A$, so $Y = P_1 \cdots P_n$ for P_i prime. SO $I = M \cdot P_1 \cdots P_n$, so $I \notin A$, contradiction.

Note $P_1 \cdots P_n \subseteq P_1$. Since P_1 is prime, then $Q_i \subseteq P_1$ for some i. Recall that the dimension of a Dedekind domain is 1, so every non-zero prime ideal is maximal. Therefore, Q_i and P_1 are maximal. Hence, $Q_i = P_1$. Without loss of generality, say $Q_1 = P_1$, then $Q_2 \cdots Q_m = P_2 \cdots P_n$. We proceed by induction. □

7.2 Integral Elements

Definition 7.2.1 (Integral Element)**.** *Let $R \subseteq S$ be commutative rings. An element $x \in S$ is called integral over R if there exists a polynomial $f \in R[x]$ such that $f(s) = 0$.*

Example 7.2.2. *1. If R and S are fields, then integral elements are equivalent to algebraic elements.*

2. Every element $r \in R \subseteq S$ is integral over R: take $f = x - t$.

Definition 7.2.3 (Faithful Module)**.** *Let R be a commutative ring and M is a R-module. We say M is faithful if $\forall 0 \neq r \in R$, $r \cdot M \neq 0$. Equivalently, R as an Abelian group generates the injective homomorphism $R \to \mathbf{End}(M)$.*

Example 7.2.4. *Rings $R \subseteq S$ indicates S is a faithful R-module.*

Proposition 7.2.5. *Let $R \subseteq S$ be rings and $s \in S$. The following are equivalent:*

1. *s is integral over R.*
2. *$R[s]$ is finitely generated as a R-module.*
3. *There is a faithful $R[s]$-module that is finitely generated as a R-module.*

Proof. (1) $\Rightarrow$ (2): Let $f \in R[x]$ be monic, $f(s) = 0$. Let $n = \deg(f)$. By observing $s^n + a_1 s^{n-1} + \cdots + a_{n-1}s + a_0 = 0$ where $a_i \in R$, we have $R[s] = \sum\limits_{i=0}^{n-1} Rs^i$ is finitely generated.

(2) $\Rightarrow$ (3): $R[s]$ is a faithful (as $R[s]$-module) finitely-generated R-module.

(3) $\Rightarrow$ (1): Suppose M is a faithful $R[s]$ -module, finitely generated as a R-module Let M be generated by $m_1, \cdots, m_n$. We write $sm_i = \sum\limits_{j=1}^{n} a_{ij} m_j$ with $a_{ij} \in R$. They form an $n \times n$ matrix A over R.

Let $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ m_n \end{pmatrix}$, then $s \cdot X = A \cdot X$, so $(s \cdot I - A)X = 0>$ This gives a matrix over $R[s]$.

Note that for an $n \times n$ matrix B, there exists an adjoint (cofactor) matrix B' such that $B' \cdot B = \deg(B) \cdot I$ over commutative rings. Then we have $(sI \overset{\sim}{-} A)(sI - A)X = 0$, so $\deg(s \cdot I - A)X = 0$. Hence, $\deg(S \cdot I - A) \cdot m_i = 0$ for all i. Therefore, $\deg(s \cdot I - A) \cdot M = 0$.

Since M is faithful as a $R[s]$-module, then $\deg(s \cdot I - A) = 0$. Consider $f(x) = \deg(xI - A) \in R[x]$, which is monic of degree n. Then $f(s) = 0$, so s is integral over R. □

Corollary 7.2.6. *Let $R \subseteq S$ be rings and $s_1, \cdots, s_n \in S$ are integral over R. Then $R[s_1, \cdots, s_n]$ is finitely generated as an R-module.*

Proof. We proceed by induction.

The base case is trivial. Suppose we know $R' = R[s_1, \cdots, s_{n-1}]$ is finitely generated as R-module, then $R[s_1, \cdots, s_n] = R'[s_n]$ which is a finitely generated R'-module. But since s_n is integral over R, then s_n is integral over R'. We then can conclude the proof easily. □

Proposition 7.2.7. *Let $R \subseteq S$ be rings. Then the set S' of all integral elements in S over R is a subring over S: $R \subseteq S' \subseteq S$.*

Proof. Obviously $R \subseteq S' \subseteq S$. We show that S' is a ring. For $x, y \in S$, we show $x + y, xy \in S$.

Let $z = x + y$. Note that the proof still works if we set $z = xy$. Then we have rings $R[z] \subseteq R[x, y]$. But $R[x, y]$ is faithful as a $R[z]$-module, so by corollary it is integral as a R-module.

By proposition, z is integral over R, so $z \in S'$. □

Definition 7.2.8 (Integral Closure, Integral, Integrally Closed, Normal)**.** *S' is called the integral closure of R in S.*

If $S' = S$, we say that S is integral over R. If $S' = R$, we say that R is integrally closed in S.

Let R be a domain (or commutative ring), we embed $R \subseteq F$, which is the quotient field of R. We say R is normal if R is integrally closed in F.

Proposition 7.2.9. *Let $R \subseteq T \subseteq S$ be rings such that T is integral over R and $s \in S$ is integral over T. Then s is integral over R.*

Proof. Consider $s^n + t_1 s^{n-1} + \cdots + t_{n-1}s + t_n = 0$ for $t_i \in T$. Then $R \subseteq T' = R[t_1, \cdots, t_n] \subseteq T$, and t_i's are integral over R. Hence, T' is finitely generated as a R-module.

Now $s \in S$ is integral over T', then $T'[s]$ is finitely generated as T'-module. By transitivity, $T'[s]$ is finitely generated as an R-mod. But $T'[s]$ is faithful as $R[s]$ module. Therefore, by proposition, s is integral over R. □

Corollary 7.2.10. *Let $R \subseteq S$ be rings. Then the integral closure of R in S is integrally closed in S.*

Example 7.2.11. *Suppose we have a subring R in a field K, and L/K is an algebraic field extension. Then the integral closure of R in L is normal.*

Suppose we have a domain R with a quotient field F, and L/K is an algebraic field extension, with $S \subseteq L$ is the integral closure of R in L. Then S is normal and the quotient field of S is L.

Proof. Let $x \in L$ be algebraic over F. Note that there exists $a_i \in F$ such that

$$x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1}x + \alpha_n = 0.$$

We can then set $ax^n + a_1x^{n-1} + \cdots + a_n = 0$ for $a, a_i \in R$. Then we have $(ax)^n + a_1(ax)^{n-1} + \cdots + a^{n-1}a_n = 0$.

Note $y = ax$ is integral over R, then $y \in S$, and we have $x = \frac{y}{a}$, so $y \in S$, $a \in R \subseteq S$.

Now S is integrally closed in L, which is the quotient field of S then, so S is normal. □

Theorem 7.2.12. *Every Dedekind ring is normal.*

Proof. Let F be the quotient field of R, and take $x \in F$ integral over R. Note that $F \supseteq R[x]$ is finitely generated as a R-module, so $\exists 0 \neq y \in R$, and we get to define $A := y \cdot R[x] \subseteq R$ as a non-zero ideal. Then $x \cdot R[x] \subseteq R[x]$, hence $xA \subseteq A$.

Denote $x = \frac{a}{b}$ where $a, b \in R$, then $\frac{a}{b} \cdot A \subseteq A$, so $aA \subseteq bA$.

Since R is Dedekind, then there exists an ideal $B \subseteq R$ such that $(aR)A = aA = bAB = (bB)A$, so $aR \subseteq bB \subseteq bR$, so $x = \frac{a}{b} \in R$. □

Lemma 7.2.13. *Let R be a Noetherian normal domain with F as its quotient field. Let $x \in A$ and $A \subseteq R$ be a non-zero ideal such that $xA \subseteq A$, then $x \in R$.*

Proof. Note that A is a faithful $R[x]$-module and is finitely generated as an R-module, then x is integral over R. By normality, $x \in R$. □

Theorem 7.2.14. *A domain R is Dedekind if and only if R is Noetherian, normal and* $\dim(R) \leq 1$.

Proof. ($\Rightarrow$): this can be easily concluded from the knowledge we have.

($\Leftarrow$):

Claim 7.2.15. *Every non-zero ideal of R contains the product of finitely many prime ideals.*

Proof. We apply the Noetherian induction.

Let $0 \neq A \subseteq R$ be an ideal with $A \neq R$. (If $A = R$, we take the empty product.) Suppose A is not prime, so $\exists x, y \in R$ such that $xy \in A$ but $x, y \notin A$. Now $(A + xR)(A + yR) \subseteq A$ contains the product of primes, where $A + xR \neq A$ and $A + yR \neq A$. □

Suppose $0 \neq A \subseteq B \subseteq R$ are ideals, then there exists an ideal C such that $A = BC$, which can be proven by Noetherian induction on B.

Claim 7.2.16. *$\exists x \in F \backslash R$ such that $xB \subseteq R$.*

Proof. Take $0 \neq b \in B$. By the previous claim, there exists

$$P_1 \cdots P_n \subseteq bR \subseteq B \subseteq P,$$

where P_i's are primes (also maximals) and P_n is the smallest, and P is also prime (also maximal). Then $P_1 \subseteq P_n \subseteq P$, so there exists some i such that $P_i \subseteq P$. But P and P_i are maximal ideals, then $P_i = P$. Without loss of generality, say $i = 1$, then $P = P_1$. Now $P_2 \cdots P_n \not\subseteq bR$, so there exists $c \in P_2 \cdots P_n$ such that $c \notin bR$ and $x = \frac{c}{b} \notin R$. So $cP_1 \subseteq P_1 \cdots P_n \subseteq bR$, then $\frac{c}{b} P_1 \subseteq R$, then $\frac{c}{b} B \subseteq R$. □

Claim 7.2.17. *$xB \not\subseteq B$.*

Proof. Indeed, otherwise $xB \subseteq B$, then by lemma $x \in R$, contradiction. □

Let $B' = B + xB \subseteq R$, then $B \not\subseteq B'$, and $A \subseteq B \subseteq B'$. By induction, $\exists C' \subseteq R$ such that $A = B'C' = B \cdot (R + xR) \cdot C'$. Take $C = (R + xR) \cdot C'$. It suffices to show that $C \subseteq R$ is an ideal. Indeed, for $c \in C$, $cB \subseteq A \subseteq B$, then by lemma we know $c \in R$, so $C \subseteq R$. □

Definition 7.2.18 (Trace)**.** *Let L/K be a finite field extension, so we can view L as a vector space over K. Take $\alpha \in L$, then there exists a map, namely the left multiplication $m_\alpha : L \to L$ that takes $x \mapsto \alpha x$, which makes it a K-linear transformation. The trace of α, denoted $Tr_{L/K}(\alpha)$, can then be defined as the trace of this linear transformation in the linear algebra sense.*

Alternatively, if L/K is a separable extension, then we can define the trace $Tr_{L/K}(\alpha)$ as $Tr(x) = \sum\limits_{\tau \in Gal(E/L)} \tau(x) \in E$, where E is the normal closure over L, i.e. E/K is Galois.

Theorem 7.2.19. *Let R be a Dedekind ring with quotient field F. Let L/F be a finite field extension and S is the integral closure of R in L. Then S is also Dedekind with quotient field L.*

Proof. For this proof, we assume that L/F is separable, which is reasonable. Denote $G = \mathrm{Gal}(E/F)$ where E is the normal closure over L/F.

Consider the homomorphisms from L to E, then for any $x \in L$, we can consider the trace as the sum of all the Galois conjugates of x, i.e. $\mathrm{Tr}(x) = \sum\limits_{\tau \in \mathrm{Gal}(E/L)} \tau(x) \in E$.

Note that take any $\sigma \in G$, we then have $\sigma\tau : L \xrightarrow{\tau} E \xrightarrow{\sigma} E$. Moreover, $\sigma\mathrm{Tr}(x) = \sum\limits_{\tau} \sigma\tau(x) = \mathrm{Tr}(x)$, so $\mathrm{Tr}(x) \in E^G = F$.

In particular, we can the trace map $\mathrm{Tr}(L \to F)$ is linear, with $\mathrm{Tr}(x+y) = \mathrm{Tr}(x)+\mathrm{Tr}(y)$.

Claim 7.2.20. *$Tr \neq 0$.*

Subproof. $L = F(\alpha)$, then $1, \alpha, \cdots, \alpha^{n-1}$ is a basis for L/F, where $n = [L : F]$.

We have distinct homomorphisms $\tau_1, \cdots, \tau_n : L \to E$, then $\tau_i(\alpha^j) = (\tau_i(\alpha))^j$. This gives an $n \times n$ matrix with non-zero determinant. Then $\mathrm{Tr}(\alpha^i) = \sum\limits_i \tau_i(\alpha^j) \neq 0$ for some j. Hence, $\mathrm{Tr} \neq 0$. ■

Claim 7.2.21. *$Tr(S) \subseteq R$.*

Subproof. Recall that $\mathrm{Tr}(x) = \sum\limits_{\tau : L \to E} \tau x$. For $x \in S$, it is always integral over R, with $f(x) = 0$ for some $f \in R[x]$ monic. Then $f(\tau x) = 0$, so τx is integral over R for all τ. Therefore, $\mathrm{Tr}(x)$ is integral over R. But $\mathrm{Tr}(x) \in F$, and since R is normal, then $\mathrm{Tr}(x) \in R$. ■

We know that L is the quotient field of S, now $\forall x \in L$, $x = \frac{s}{a}$ for $s \in S$, $a \in R$. Let $\{x_1, \cdots, x_n\}$ be a basis for L/F, so every x_i is of the form $\frac{s_i}{a_i}$. Then we may assume that $x_i \in S$ since they are invertible. We define the map

$$\begin{aligned} f : L &\to F \times F \times \cdots \times F = F^n \\ y &\mapsto (\mathrm{Tr}(x_1 y), \cdots, \mathrm{Tr}(x_n y). \end{aligned}$$

Claim 7.2.22. $\ker(f) = 0$.

Subproof. Let $y \in \ker(f)$. Then $\mathrm{Tr}(x_i y) = 0$ for all i. Recall $\mathrm{Tr}(ay) = a \cdot \mathrm{Tr}(y)$ for $a \in F$, $y \in L$. Then $\mathrm{Tr}(zy) = 0$ for all $z \in L$. But $\mathrm{Tr} \neq 0$, then $y = 0$. ■

Therefore, we can easily see that f is an isomorphism.

Consider $f \mid_S$: $S \to R \times \cdots \times R$ which is R-linear and injective: note that $y \in S$ indicates $x_i y \in S$, so $\mathrm{Tr}(x_i y) \in R$.

Therefore, we have an embedding $S \hookrightarrow R^n$ as an R-submodule.

Since R is Noetheriand and Dedekind, then S is finitely generated as an R-module. Therefore, S is of finite type over R, so S is Noetherian.

Since S is integrally closed in L, we can easily conclude that S is normal.

Finally, we show that $\dim(S) \leq 1$. Let $0 \neq P \subseteq S$ be a prime ideal. It suffices to show that P is maximal. Define $Q := P \cap R$, then it is prime in R.

Claim 7.2.23. $Q \neq 0$.

Subproof. Take $0 \neq x \in P$, then it is integral over R. Then we have $x_n + a_1 x^{n-1} + \cdots + a_n = 0$ for some $a_i \in R$. Note $a_n \neq 0$, then $a_n \in Sx \subseteq P$. Since $a_n \in R$, so $0 \neq a_n \in Q$. ■

Therefore, Q is maximal, then R/Q is a field.

Consider the map $R \subseteq S \twoheadrightarrow S/P$, we then have $R/Q \hookrightarrow S/P$, where R/Q is a field and S/P is a ring as a finitely-generated R/Q-vector space, so it is essentially a domain.

Consider $l_u : S/P \to S/P$ as left-multiplication. This map is injective and so an isomorphism. Therefore, $u \in (S/P)^\times >$ Hence, S/P is a field, and so P is maximal. □

Example 7.2.24. *1. Suppose $L/\mathbb{Q}$ is a finite field extension with $R = \mathbb{Z}$. Then S is always Dedekind.*

In particular, suppose L is a quadratic extension over $\mathbb{Q}$, i.e. $L = \mathbb{Q}(\sqrt{d})$ where $d \neq 0$ and is square-free. Now

$$S = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}, & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{if } d \equiv 1 \pmod 4 \end{cases}.$$

In particular, $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind ring, but $\mathbb{Z}[\sqrt{5}]$ is not because it is not integrally closed. Instead, $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is.

2. *Let $R = F[x]$ where F is a field. Then we have*

$$\begin{tikzcd} S \arrow[r, hook, "subset"] \arrow[d, dash] & L \arrow[d, dash, "finite"] \\ F[x] \arrow[r, hook, "subset"'] & F(x) \end{tikzcd}$$

with S Dedekind. Note that S is the ring of regular polynomial functions on a regular affine algebraic curve over F. For example, let $y = \sqrt{1-x^2}$, then $L = F(x)(y)$ satisfies a circle $x^2 + y^2 = 1$. Then $S = F[x,y] = F[X,Y]/(X^2+Y^2-1)$.

Remark 7.2.25. *The intersection of Dedekind domain and UFD is exactly the PIDs.*

It is obvious that PIDs are in the intersection. Then if suffices to show that every prime ideal is principal.

Take $0 \neq P \subseteq R$ prime, then take $0 \neq x \in P$ with $x = p_1 \cdots p_n$ primes in P. Then $P_i \in P$ for some i. Then $P_iR \subseteq R$. But we know that p_iR is prime, then $P = p_iR$ is a maximal ideal.

7.3 Discrete Valuation Ring (DVR)

Definition 7.3.1 (Discrete Valuation)**.** *Let F be a field. $v : F^\times \to \mathbb{Z}$ is called a discrete valuation if*

1. *$v(xy) = v(x) + v(y)$,*

2. *$v(x+y) \geq \min(v(x), v(y))$.*

We also define $v(0) = \infty$.

Example 7.3.2. 1. *Let R be a Dedekind ring. Let F be the quotient field of R, and $0 \neq P \subseteq R$ be prime. We define a discrete valuation $v_P : F^\times \to R$ as for $0 \neq x \in R$, $xR = P^i \cdot$ (product of other ideals) for $i \geq 0$. Then $v_P(x) = i$. For $x \in R^\times$, we write $x = \frac{y}{z}$ for $y, z \in R \backslash \{0\}$. Then $v_P(x) = v_P(y) - v_P(z)$. Here v_P is called the discrete valuation with P, or just p-adic discrete valuation on F.*

2. *Suppose $R = \mathbb{Z}$, $P = p\mathbb{Q}$ and $F = \mathbb{Q}$. Then $v_p(x) = i$ where $x = p^i \frac{a}{b}$ for $p \nmid a, \nmid b$.*

Proposition 7.3.3 (Ostrowsky)**.** *There are the only valuations of $\mathbb{Q}$, i.e. the non=trivial absolute value on $\mathbb{Q}$ is equivalent to either the usual real absolute value or a p-adic absolute value.*

Example 7.3.4. *Let K be a field, $F = K(x)$, $P = pK[x]$ for p monic irreducible. Then $v_p(f) = i$ for $f = p^i \frac{a}{b}$, $p \nmid a, p \nmid b$, and $v_\infty(\frac{g}{h}) = \deg(h) - \deg(g)$.*

Definition 7.3.5 (Valuation Ring, Discrete Valuation Ring)**.** *Let F be a field and $v : F^\times \to \mathbb{Z}$ is a discrete valuation. Set $v(0) = \infty$. $Rv = \{x \in F : v(x) \geq 0\}$ is a subring of F, called the valuation ring.*

A domain R is a discrete valuation ring (DVR) if $R = R_v$ for some valuation on the quotient field F.

Example 7.3.6.

1. *Let F be a field and let $v = 0$ on F, then $Rv = F$, so F is a DVR.*
2. *Let $F = \mathbb{Q}$ and $p \in \mathbb{Z}$ be a prime. Then $R_{v_p} = \{\frac{a}{b} : p \nmid b\} = \mathbb{Z}_p$, namely the localization at $p\mathbb{Z}$.*

Definition 7.3.7 (Local Ring)**.** *We say that a ring R is a local ring if any of the following properties hold:*

1. *R has a unique (left/right) maximal ideal.*
2. *It is a non-trivial ring and the sum of any two non-units in R is a non-unit.*
3. *It is a non-trivial ring such that if x is any element of R, then x or $1-x$ is a unit.*

Proposition 7.3.8. *If R is a Dedekind ring and $P \subsetneq R$ is a nonzero prime ideal, then $R \subseteq R_{v_p} = R_p \subseteq F$, where F is the quotient field of R.*

If R is any commutative ring and $P \subsetneq R$ is a prime ideal, then R_p is a local ring with unique prime/maximal ideal P_p.

In general, if $v : F^\times \to \mathbb{Z}$ is a discrete valuation, then R_v is local with unique maximal ideal $M = \{x \in F : v(x) > 0\}$. Note that every $x \in R_v \backslash M$ is invertible.

Theorem 7.3.9. *The following are equivalent:*

1. *DVR.*
2. *Local PID.*
3. *Local Dedekind ring.*

Proof. (1) $\Rightarrow$ (2): Let R be a DVR. Then R is local with maximal ideal M.

Claim 7.3.10. *Every non-zero ideal $I \subseteq R$ is of the form $\pi^i R$ for $i \geq 0$ and $v(\pi) = 1$. In particular, R is a PID.*

Subproof. Assume $v : F^\times \to \mathbb{Z}$ is nonzero, otherwise $R = F$ is a PID. Now $\text{im}(v) \subseteq \mathbb{Z}$ is an ideal, so $\text{im}(v) = n\mathbb{Z}$. We can divide by n to let $\text{im}(v) = \mathbb{Z}$. Let $i = \min\limits_{x \in I} v(x)$ and fix $\pi \in F$ with $v(\pi) = 1$. Then $v(\frac{x}{\pi^i}) = v(x) - v(\pi^i) = v(x) - iv(\pi) \geq i - i = 0$, so $\frac{x}{\pi^i} \in R$, so $I \subseteq \pi^i R$. Conversely, for all $x \in I$ with $v(x) = i$, $v(\frac{x}{\pi^i} = 0$, then $\frac{x}{\pi} \in R^\times$, so $\pi^i = \frac{\pi^i}{x} \cdot x \in I$, then $I = \pi^i R$. ■

(2) ⇒ (3): trivial.

(3) ⇒ (1): If R is a field then R is clearly a DVR. Let R be a local Dedekind ring with unique maximal ideal $M \neq 0$, then M is the only non-zero prime ideal in R. By factorization, every ideal is of the form M^i, then take $v = v_M : F^\times \to \mathbb{Z}$, which is the only valuation of R.

Claim 7.3.11. *$R = R_v$, then R is a DVR.*

Subproof. Note that every $x \in R\backslash\{0\}$ satisfies $v(x) \geq 0$, so $x \in Rv$, then $R \subseteq R_v$. (By factoring xR into powers of M, we see that $v(x) \geq 0$.) Now for every element $x = \frac{a}{b} \in R_v\backslash\{0\}$, we let $aR = M^i$ and $bR = M^j$. Then $v(x) = i - j \geq 0$, so $M^i \subseteq M_j$, which means $aR \subseteq bR$, then $x \in R$, so $R = R_v$. ■

□

Remark 7.3.12. *If R is a DVR and M is the unique maximal ideal, then all non-zero ideals form a chain $M \supseteq M^2 \supseteq \cdots \supseteq M^i \supseteq \cdots$.*

If $a \in R$ non-zero, we write $aR = M^i$ and then $i = v(a)$, so $aR = M^{v(a)}$.

Remark 7.3.13. *In general, let R be a Dedekind ring and $P \subsetneq R$ a non-zero prime. Pick any $x \in R\backslash\{0\}$. Then R_p is a local Dedekind ring, so it is a DVR with discrete valuation $v = v_p : F^\times \to \mathbb{Z}$. By factorization, we have $xR = P^i \cdot P_1 \cdots P_n$, so $(xR)_p = P_p^i$ since $(P_j)_p = R_p$ when $P_j \not\subseteq P$, also $i = v_p(x)$. Therefore, $xR = \prod\limits_{p \text{ non-zero prime}} P^{v_p(x)}$, which is always finite.*

Definition 7.3.14 (Fractional Ideal)**.** *Let R be a Noetherian domain and F is the quotient field. A fractional ideal of R is a finitely-generated R-submodule of F.*

Example 7.3.15. *1. All ideals are fractional ideals.*

2. If $I \subseteq F$ is any fractional ideal and $x \in F^\times$, then $xI \cong I$ is also a fractional ideal.

Remark 7.3.16. *Let R be a Dedekind ring with F as its quotient field. A fractional ideal A is a finitely-generated R-module by definition. There exists $0 \neq a \in R$ such that $aA \subseteq R$ as an ideal. Conversely, every ideal is a fractional ideal.*

Let $A, B \in$ Frac(R), which is the set of fractional ideals. Then $A = \sum a_i R$, $B = \sum b_j R$. $AB = \sum a_i b_j R$, so $AB \in$ Frac(R).

Proposition 7.3.17. *Frac(R) is an Abelian group.*

Proof. The operation comes for free and the identity is R itself. Take $A \in \text{Frac}(R)$, then there exists $0 \neq a \in R$ such that $I = aR \subseteq R$ is an ideal. Pick any $0 \neq x \in I$, so that $xR \subseteq I$, there exists an ideal $J \subseteq I$ such that $xR = IJ = aA \cdot J$. Then $R = A \cdot \frac{a}{x}J$, so $A^{-1} = \frac{a}{x} \cdot J \in \text{Frac}(x)$. □

Remark 7.3.18. *Let $A \in$ Frac(R). Find $a \in R$ such that $aA = I \subseteq R$ is an ideal. Note $A = P_1 \cdots P_s$ as a product of prime ideals. Also, $aR = Q_1 \cdots , Q_t$ is also a product of prime ideals. Now $A = (a^{-1}R) \cdot I = Q_1^{-1} \cdots Q_t^{-1} P_1 \cdots P_s$. So every fractional ideal is a product of primes and their inverses.*

Therefore, denote $A = S_1^{\alpha_1} \cdots S_r^{\alpha_r}$ where $S_i \subseteq R$ are primes with $\alpha_i \in \mathbb{Z}$. Note that such decomposition is unique. Then Frac(R) is a free Abelian group with a canonical basis of prime ideals.

Note that if we start with ideals only, we only get a monoid or semi-group.

Remark 7.3.19. *A fractional ideal A is principal if $A = xR$ for $x \in F^\times$. Note that $(xR)(yR) = xyR$ is also principal. Therefore, principal fractional ideals form a subgroup PFrac(R) $\subseteq$ Frac(R). There is a surjective homomorphism with kernel as $R^\times \subseteq F^\times$:*

$$F^\times \twoheadrightarrow PFrac(R) x \mapsto xR$$

By the First Isomorphism Theorem, PFrac(R) $\cong F^\times / R^\times$. We also denote Cl($R$) = Frac($R$)/PFrac($R$) to be the class group of R. We then have an exact sequence of Abelian groups

$$\begin{tikzcd} 1 \arrow[r] & R^\times \arrow[r] & F^\times \arrow[r] & Frac(R) \arrow[r] & Cl(R) \arrow[r] & 1 \end{tikzcd}$$

where $A \in$ Frac(R) is sent to $[A] \in$ Cl(R).

Note that Cl(R) $= 1$ if and only if every fractional ideal is principal if and only if every ideal is principal if and only if R is a PID.

Example 7.3.20. *1. Let R be the ring of algebraic integers, then the class group is finite.*

In particular, if $R = \mathbb{Z}[\sqrt{-5}]$, then $Cl(R) = \{[R], [I]\}$, which is a cyclic group generated by $[I]$. Indeed, $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, with $I = 2R + (1+\sqrt{-5})R$, then $I^2 = 2R$.

2. Let K be a field and we have $F/K(x)$ as a finite field extension. Let R be the integral closure of $K[x]$ in F. If K is finite, then $Cl(R)$ is also finite.

In particular, let K be a field of char$(K) \neq 2$. Consider $K(x)(\sqrt{1-x^2})/K(x)$, then $R = K[x, y]$ where $y = \sqrt{1-x^2}$. Hence, $R = K[x, y] = K[X, Y]/(X^2 + Y^2 - 1)$.

Observe that $x^2 + y^2 = 1$, so $x^2 = 1 - y^2 = (1+y)(1-y)$. Let $K = \mathbb{Q}$ or $\mathbb{R}$, then we have the factorization with $I = xR + (1-y)R$ and $J = xR + (1+y)R$, which are both prime but not principal. Moreover, $IJ = xR$ and $I^2 = (1-y)R$, $J^2 = (1+y)R$ with $(IJ)^2 = I^2J^2$. Therefore, $Cl(R) = \{[R], [I] = [J]\}$.

However, if $K = \mathbb{C}$, then $Cl(R) = 1$, so R is a PID in this case.

7.4 Modules over Dedekind Rings

Recall that the PIDs are exactly the intersection of Dedekind rings and the UFDs. We want to find a similar classification of modules over PIDs as the usual modules.

Let R be a Dedekind ring and M is a R-module. Recall that $M_{\text{tors}} = \{m \in M : \exists 0 \neq a \in R \text{ such that } a \cdot m = 0\}$. We say M is torsion if $M = M_{\text{tors}}$ and M is torsion-free if $M_{\text{tors}} = 0$.

Let M be a torsion finitely generated R-module, and let $0 \neq P \subseteq R$ be a prime ideal. We say M is P-primary if $P^n \cdot M = 0$ for some $n > 0$.

We have $M[P] = \{m \in M : P^n \cdot m = 0 \text{ for some } n > 0\}$ as a finitely-generated submodule of M , called the P-primary component of M.

Recall $M = \coprod_{0 \neq P \subseteq R \text{ prime}} M[P]$. Note that the same proof works: every two distinct non-zero prime ideals are coprime, i.e. $P + Q = R$.

Now let M be a P-primary finitely-generated torsion R-module. Take $r \in R \backslash P$. Then $l_r : M \to M$ that sends $m \mapsto rm$ is an automorphism on M. Indeed, $rR + P = R$.

Suppose $S \subseteq R$ is a multiplicative subset and M is a R-module. Then for all $s \in S$, $l_s : M \to M$ is an isomorphism, then M has the structure of a module over $S^{-1}R$: note that $\frac{r}{s} \cdot m = l_s^{-1}(rm)$.

Therefore, we can localize by $S = R\backslash P$. Now $R_p = S^{-1}R$, then M is a finitely-generated R_p-module. Then R_p is a local Dedekind ring, and so it is a PID. Therefore, N is a direct sum of cyclic modules $M = R_p/P_p^n$.

Note that $M = R_p/P_p^n \cong R/P^n$, because $R_p/P_p^n = S^{-1}(R/P^n)$, and the localization acts as an isomorphism towards R/P^n since multiplication by any s is an isomorphism.

Theorem 7.4.1 (Invariant Form)**.** *Let M be a torsion finitely-generated module over a Dedekind ring R, then there are ideals*

$$A_1 \supseteq A_2 \supseteq \cdots \supseteq A_r$$

of R such that $M \cong R/A_1 \oplus \cdots R/A_r$. The ideals A_i are unique and are called the invariant form of M.

Theorem 7.4.2 (Elementary Divisor)**.** *Let M be a torsion finitely-generated module over a Dedekind R, then there are non-zero prime ideals $P_1, \cdots, P_s$ of R and positive integers $k_1, \cdots, k_s$ such that*

$$M \cong R/P_1^{k_1} \oplus \cdots \oplus R/P_s^{k_s}.$$

The ideals P_i and integers k_i are unique up to permutation. The family $\{P_i^{k_i}\}_{i\geq 1}$ is called the elementary divisors of M.

Lemma 7.4.3. *Let M be a torsion-free finitely-generated module over a Dedekind ring R. Then M is isomorphic to a submodule of R^n for some n.*

Proof. We localize with $S = R\backslash\{0\}$, so $S^{-1}R = F$, where F is the quotient field of R. Then $S^{-1}M$ is a vector space over F, so $S^{-1}M \cong F^n$. Here we call this n to be the rank of M.

Consider the map $M \to S^{-1}M$ by sending $m \mapsto \frac{m}{1}$, then the kernel of the map $\ker(M \to S^{-1}M) = M_{\text{tors}} = 0$. Hence, we know $M \hookrightarrow S^{-1}M \cong F$. In particular, there exists $0 \neq a \in R$ such that

$$M \underset{\sim}{\xrightarrow{a}} aM \hookrightarrow R^n$$

because M is torsion-free. □

Corollary 7.4.4. *$M \cong A_1 \oplus \cdots \oplus A_n$ where A_i are ideals in R. In particular, M is projective.*

Proof. We prove by induction on $n = \text{rank}(M)$. The base case is trivial. We now suppose the case is true at $n-1$, we now show the case for n.

By lemma, consider $M \hookrightarrow R^n$. Then

$$\ker(M \subseteq R^n \to R) = N \subseteq R^{n-1}.$$

Now $A = \text{Im}(M \subseteq R^n \to R) \subseteq R$ is an ideal. Then we have

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, hook] & M \arrow[r] & A \arrow[r] & 0 \end{tikzcd}$$

to be a split short exact sequence since A is projective. Then $M \cong N \oplus A$. We use induction to conclude the proof. □

Let M be a finitely-generated R-module, then

$$\begin{tikzcd} 0 \arrow[r] & M_{\text{tors}} \arrow[r] & M \arrow[r] & M/M_{\text{tors}} \arrow[r] & 0 \end{tikzcd}$$

Now torsion-free implies projective, so the short exact sequence splits. Then

$$M \cong M_{\text{tors}} \oplus M/M_{\text{tors}}.$$

Consider fractional ideals A, B of R (which implies they are non-zero, and take $x \in B \cdot A^{-1}$ from the fractional ideal. Consider

$$\begin{aligned} f_x : A &\to B \\ a &\mapsto xa \end{aligned}$$

which is well-defined since $xa \in (BA^{-1}) \cdot A = B$. Then f_x is a R-module homomorphism. Now there is

$$\begin{aligned} BA^{-1} &\to \mathbf{Hom}_R(A, B) \\ x &\mapsto f_x \end{aligned}$$

Lemma 7.4.5. *This is an isomorphism of R-modules.*

Proof. Suppose $f_x = f_y$, then take $0 \neq a \in A$, we have

$$xa = f_x(a) = f_y(a) = ya,$$

so $x = y$. Consider $f : A \to B$. For $0 \neq a_0 \in A$ and $a \in A$,

$$a_0 \cdot f(a) = f(a_0 a) = a \cdot f(a_0).$$

Therefore, $f(a) = xa$, where $x = \frac{f(a_0)}{a_0}$. Now $xa \in B$ for all $a \in A$, so $xA \subseteq B$. Then $x \in xR = xAA^{-1} \subseteq BA^{-1}$, so $f = f_x$. □

Consider the map

$$\begin{aligned} \mathbf{Hom}_R(B,C) \times \mathbf{Hom}_R(A,B) &\to \mathbf{Hom}_R(A,C) \\ (f,g) &\mapsto f \circ g \\ CB^{-1} \times BA^{-1} &\mapsto CA^{-1} \end{aligned}$$

Therefore we can consider the map in two ways, as a composition and as a product operation.

Note that $A_1 \oplus \cdots \oplus A_n \xrightarrow{f} B_1 \oplus \cdots \oplus B_m$ is given by a matrix with entries in $B_j A_i^{-1}$.

Remark 7.4.6. *Let C be a fractional ideal. Observe that $(B_jC)(A_iC)^{-1} = B_jA_i^{-1}$. In other words, f gives a canonical homomorphism*

$$g : A_1C \oplus \cdots \oplus A_nC \to B_1C \oplus \cdots \oplus B_mC,$$

and so if f is an isomorphism, then so is g.

Suppose for fractional ideals A_i, B_j we have

$$M = A_1 \oplus \cdots \oplus A_n \cong B_1 \oplus \cdots \oplus B_m,$$

then $n = m$. Indeed, let $S = R\backslash\{0\}$ and $S^{-1}A_i \cong F \cong S^{-1}B_j$, then $S^{-1}M \cong F^n \cong F^m$, so $n = m$.

Moreover, the isomorphism is given by an $n \times n$ matrix C with entries in $B_iA_j^{-1} \in A$, then C is invertible.

Claim 7.4.7. *Take $a_i \in A_i$ for all i, then*

$$\det(C) \cdot a_1 a_2 \cdots a_n \in B_1 \cdots B_m.$$

Proof. Let $D = C \cdot \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$, then $d_{ij} = c_{ij} \cdot a_j \in B_i A_j^{-1} A_j = B_i$.

Now

$$\deg(C) \cdot a_1 \cdots a_n = \deg(D) \in B_1 \cdots B_n.$$

□

It then follows that

$$\deg(C) \cdot A_1 \cdots A_n \subseteq B_1 \cdots B_m.$$

The same argument works on the inverse of the isomorphism, so

$$\deg(C^{-1}) \cdot B_1 \cdots B_m \subseteq A_1 \cdots A_n.$$

Therefore,

$$\begin{cases} \deg(C) \cdot A_1 \cdots A_n = B_1 \cdots B_m \\ \deg(C^{-1}) \cdot B_1 \cdots B_m = A_1 \cdots A_n \end{cases}.$$

Therefore, $[A_1 \cdots A_n] = [B_1 \cdots B_m]$ in the class group $\mathrm{Cl}(R)$. We define it to be the determinant $\det(M)$, the determinant of M in the class group.

Lemma 7.4.8. *Let A and B be fractional ideals $P \subseteq R$ is a non-zero prime ideal, then $A \oplus BP \cong AP \oplus B$.*

Proof. We first assume that $B = R$. Then it suffices to show that $A \oplus P \cong AP \oplus R$.

Note $A^{-1} \cdot A = R$, so $\exists x_i \in A^{-1}$, $a_i \in A$ such that $\sum x_i a_i = 1$. Therefore, there exists some i such that $x_i a_i \notin P$. Consider

$$\begin{aligned} f : A &\to R \\ a &\mapsto x_i a \in R. \end{aligned}$$

Then $\mathrm{im}(f) \ni x_i a_i \notin P$. Then consider

$$h : A \oplus P \xrightarrow{(f,g)} R$$

for $g : P \hookrightarrow R$, so $\mathrm{im}(h) = \mathrm{im}(f) + \mathrm{im}(g)$. But $\mathrm{im}(f) \not\subseteq P$ and $\mathrm{im}(g) = P$, which is a maximal ideal, then $\mathrm{im}(h) = R$.

Now let $N = \ker(h)$, then

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, hook] & A \oplus P \arrow[r, "h"] & R \arrow[r] & 0 \end{tikzcd}$$

is a split short exact sequence. Then

$$A \oplus P \cong N \oplus R.$$

Therefore, if we denote F as the quotient field of R, then $F \oplus F \cong S^{-1}N \oplus F$, therefore $N \hookrightarrow S^{-1}N \cong F$ where N is a finitely-generated R-submodule of F.

Then N is a fractional ideal, so

$$[A \cdot P] = \deg(A \oplus P) = \det(N \oplus R) = [N \cdot R] = [N]$$

in $\mathrm{Cl}(R)$. Then $A \cdot P \cong xN \cong N$ with $x \in F^\times$.

This proves the special case. In general, we know $AB^{-1} \oplus P \cong AB^{-1}P \oplus R$ by the special case. Therefore, $A \oplus BP \cong AP \oplus B$. □

Theorem 7.4.9. *Let R be a Dedekind domain. Then*

1. *Every torsion-free finitely-generated R-module M is isomorphic to $I \oplus R^{n-1}$ where $n = rank(M)$, and $I \subseteq R$ is an ideal such that $[I] = \det(M)$.*

2. *Two torsion-free finitely-generated R-module M and N are isomorphic if and only if $rank(M) = rank(N)$ and $\det(M) = \det(N)$ in $Cl(R)$.*

Proof. 1. Note $A \oplus BP \cong AP \oplus B$.

Claim 7.4.10. *For every two ideals I and J in R, $I \oplus J \cong IJ \oplus R$.*

Subproof. Let $J = P_1 \cdots P_s$ where P_i are primes, then

$$\begin{aligned}I \oplus J &= I \oplus P_1 \cdots P_s \\ &= IP_1 \oplus RP_2 \cdots P_s \\ &= IP_1 \cdots P_s \oplus R \\ &= IJ \oplus R.\end{aligned}$$

■

Now $M \cong I_1 \oplus \cdots I_n \cong I_1I_2 \oplus R \oplus I_3 \oplus \cdots \oplus I_n = I_1I_2I_3 \oplus R \oplus I_4 \oplus \cdots \oplus I_n$, so $M \cong I \oplus R^{n-1}$, where n is the rank of M, and $I_j \subseteq R$ are ideals such that $I = I_1 \cdots I_n$. Therefore, $[I] = [I_1] \cdots [I_n] = \det(M)$.

2. Denote n as the rank of M and N, then $M \cong I \oplus R^{n-1}$ and $N \cong J \oplus R^{n-1}$, so $[I] = \det(M) = \det(N) = [J]$ in $\mathrm{Cl}(R)$, so there exists $x \in F^\times$ such that $J = xI$, which means $M \cong N$.

□

7.5 Picard Group

Let R be a commutative ring.

Definition 7.5.1 (Spectrum, Jacobson Radical)**.** *The (prime) spectrum of R is the set of all prime ideals in R, denoted Sepc(R). The maximal spectrum of R is the set of maximal ideals of R, denoted Specm(R).*

The Jacobson radical is defined as the intersection of all maximal ideals for commutative rings, i.e. $J(R) = \bigcap_{M \in \mathit{Specm}(R)} M$.

Proposition 7.5.2 (Nakayama Lemma, Statement 1)**.** *Let I be an ideal in R, and M a finitely-generated module over R. If $IM = M$, then there exists $r \in R$ such that $r \equiv 1 \pmod{I}$ such that $rM = 0$.*

Corollary 7.5.3 (Nakayama Lemma, Statement 2)**.** *If $J(R)M = M$, then $M = 0$.*

Lemma 7.5.4. *If R is local, then every finitely-generated projective R-module is free.*

Proof. Suppose $M \subsetneq R$ is the maximal ideal, with $K = R/M$. Let P be a finitely-generated projective R-module. Now $P/MP(= P \otimes_R K)$ as a K-space of finite dimension.

Let $p_1, \cdots, p_n \in P$, then $\{\bar{p}_1, \cdots, \bar{p}_n\}$ is a basis for P/MP over K. Note $\bar{p}_i = p_i + MP \in P/MP$.

Claim 7.5.5. *$\{P_1, \cdots, P_n\}$ is a basis for P over R.*

Subproof. Take $Q = \sum R \cdot p_i \subseteq P$. Now $N = P/Q$, then $N/M \cdot N = (P/MP)/((Q+MP)/MP) = 0$, where $\bar{p}_i$ in $Q + MP$ generates P.

By Nakayama Lemma, $N = 0$. Therefore, $P = Q$, so $p_i's$ generate P.

Consider the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & S \arrow[r] & R^n \arrow[r, "\varphi"] & P \arrow[r] & 0 \end{tikzcd}$$

where $\varphi(e_i) = p_i$. Note that φ is a surjection. To show it is an isomorphism, it suffices to show that $\ker(\varphi) = S = 0$. Also note that the sequence

$$\begin{tikzcd} S/MS \arrow[r] & K^n \arrow[r, "\sim"] & P/MP \arrow[r] & 0 \end{tikzcd}$$

has an isomorphsim where we send $e_i \mapsto \bar{p}_i$. Therefore, both sequence split by projective. Therefore, $S/MS = 0$, then by Nakayama Lemma, $S = 0$, so φ is an isomorphism. ■

□

Remark 7.5.6. *Let $P \subsetneq R$ be a prime ideal. The local ring $R_P = S^{-1}R$, where $S = R \backslash P$.*

Denote M as an R-module, then $M_P = S^{-1}M$ is an R_P-module.

If $M_P = 0$ for all P, then $M = 0$.

If M is a finitely-generated projective module, then by lemma, M_P is a finitely-generated free R_P-module.

Considering rank : Spec$(R) \to \mathbb{Z}^{\geq 0}$ as a map that sends $P \mapsto$ rank(M_P), we have rank$(M_P) \in \mathbb{Z}^{\geq 0}$. Therefore, $M = 0$ if and only if rank $= 0$.

If M and N are finitely-generated projective R-module, then $M \otimes_R N$ is a finitely-generated projective R-module. Therefore, rank$_{M \otimes N}$ = rank$(M) \cdot$ rank(N). If rank$_M$ = rank$_N = 1$, then rank$_{M \otimes_R N} = 1$ (with $M_P \cong R_P \cong N_P$). Therefore, we have a monoid structure on ranks. Moreover, this is a group.

Let M be a finitely-generated rank-1 projective R-module. Then $M^* = Hom_R(M, R)$ is the dual R-module.

Claim 7.5.7. *M^* is a finitely-generated rank-1 projective R-module.*

Proof. $M \oplus N \cong R^n$, so $M^* \oplus N^* \cong (R^*)^n = R^n$. Hence, M^* is a finitely-generated projective R-module. Although localization doesn't usually commute with hom functors, we have

$$(M^*)_P \cong \mathbf{Hom}_{R_P}(R_P \cong M_P, R_P) \cong R_P,$$

so $\operatorname{rank}(M^*) = 1$. □

Let M be a finitely-generated rank-1 projective R-module with map $f : M \to R$, then we have a map

$$\begin{aligned} M^* \otimes_R M &\to R \\ f \otimes m &\mapsto f(m) \end{aligned}$$

Claim 7.5.8. *This map is an isomorphism.*

Proof. It suffices to check this is an isomorphism after localization. (We want to check that the kernel and cokernel are both 0m, but they commute with the localization functor as well.)

Consider $(M_P)^* \otimes_{R_P} M_P \to R_P$. As $M_P \cong R_P$, pick $x \in M_P$, then $\{x\}$ becomes a basis. Hence, $(M_P)^* \cong R_P$. We can pick some $f \in (M_P)^*$, so that $f(x) = 1$, then $\{f\}$ is a basis of $(M_P)^*$.

Therefore, $f \otimes x \mapsto f(x) = 1$ by the mapping, and observe that $\{1\}$ is a basis of R_P. We then have an isomorphism. □

Therefore, $M^* \otimes_R M \cong R$. We can now define the Picard group.

Definition 7.5.9 (Picard Group)**.** *For a commutative ring R, the Picard group $Pic(R)$ is the set of isomorphism classes of finitely-generated rank-1 R-modules, with operation $\otimes$ and unit R.*

Remark 7.5.10. *Let R be a Dedekind ring and I is a fractional ideal, then I is a finitely-generated R-module. Let $P \subseteq R$ be prime, then I_P is a fractional ideal of R_P, which is a PID, so $I_P = xR_P \cong R_P$. Then $rank_I = 1$. Hence, I is a finitely-generated rank-1 projective R-module.*

Now consider the map

$$\begin{aligned} Frac(R) &\to Pic(R) \\ I \cdot J &\mapsto I \cdot J \cong I \otimes J \end{aligned}$$

If $M \in Pic(R)$, then $M \cong I$ is an ideal. We observe that the map is surjective. For any I in the kernel of the map, we have $I \cong R$, so I is a principal ideal of R. Therefore, the kernel is exactly the principal ideals of R.

In particular, we have $Cl(R) \xrightarrow{\cong} Pic(R)$.

8 Representation Theory

8.1 Simple and Semisimple Modules

Remark 8.1.1. *To measure complexity of a ring, we can measure the complexity of category of modules over it.*

Definition 8.1.2 (Simple Module)**.** *Let R be a ring. A non-zero (left) R-module M is simple if M has no proper submodules besides M and 0.*

Lemma 8.1.3. *Let R be a ring and M is a (left) R-module. Then M is simple if and only if $M \cong R/I$ for (left) maximal ideal I.*

Proof. ($\Rightarrow$): Let M be a simple and $m \in M$ be non-zero. Then define $f : R \to M$ by $r \mapsto rm$. Then $\text{im}(f) \neq 0$, so $\text{im}(f) = M$ by simpleness. Therefore, $I = \ker(f) < R$ is a left ideal and $M \cong R/I$. We have the correspondence between submodules of M/I and ideals in R containing I, so I is maximal.

($\Leftarrow$): Use the same correspondence. □

Corollary 8.1.4. *Every non-zero ring has a simple (left) module.*

Proposition 8.1.5 (Simplicity Test)**.** *Let R be a ring and A is a (left) R-module. Then M is simple if and only if $M \neq 0$ and $M = Rm$ for any non-zero $m \in Rm$.*

Proof. ($\Rightarrow$): Let $N < M$ be a non-zero submodule, then for any non-zero $n \in N$, $Rn < N < M$, so $M = N$.

($\Leftarrow$): $Rm < m$ is a non-zero submodule, so $Rm = M$. □

Example 8.1.6.

1. *Suppose F is a field or a division ring, then every (left) module is free according to Zorn's lemma. Therefore, the only simple module is F.*

2. *Let D be a division ring. Take $R = M_n(D)$, then $M = D^n$ (viewed as column vectors) is a left R-module. Hence, for every non-zero $m_1, m_2 \in D$, there exists $r \in End(M) = R$ such that $rm_1 = m_2$, which is similar to the case in vector spaces. Hence, $Rm = M$ for every non-zero $m \in M$, then M is simple.*

3. *Let $R = \mathbb{Z}$. The maximal ideals are $p\mathbb{Z}$ for p prime, so all simple $\mathbb{Z}$-modules are of the form $\mathbb{Z}/p\mathbb{Z}$.*

Theorem 8.1.7 (Schur Lemma)**.** *Let R be a ring, and M, N are simple (left) R-modules. Suppose $f : M \to N$ is an R-linear map, then $f = 0$ or f is an isomorphism.*

Proof. Suppose $f \not\equiv 0$, then $\text{im}(f) \neq 0$ and $\ker(f) \neq M$, so $\text{im}(f) = N$, and $\ker(f) = 0$ by simpleness. □

Corollary 8.1.8. *If M is a simple (left) R-module, then $End(M)$ is a division ring.*

Definition 8.1.9 (Semisimple Module)**.** *A (left) R-module M is semisimple if $M \cong \coprod_{i\in I} M_i$ where all M_i are simple.*

Remark 8.1.10. *Semisimpleness implies simple. Note that 0 is semisimple but not simple.*

Definition 8.1.11 (Semisimple Ring)**.** *A ring R is (left) semisimple if R is semisimple as a (left) R-module, i.e. $R \cong \coprod_{i\in I} L_i$ as an internal product for non-zero minimal (left) ideals.*

Example 8.1.12. 1. *Let D be a division ring and $R = M_n(D)$, then $M = D^n$ viewed as column vectors. For all $1 \leq i \leq n$, let $L_i \subseteq R$ be a left ideal whose only non-zero column is the i-th one. Then $L_i \cong M$ is simple, and $R \cong \coprod_{i=1}^{n} L_i$ is semisimple.*

2. *If $R_1, \cdots, R_n$ are semisimple, so is $R_1 \times R_2 \times \cdots \times R_n$. Therefore, $R = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ as above is semisimple. Actually,every semisimple ring is of this form.*

Remark 8.1.13. *Suppose $R = \coprod_{i\in I} L_i$ where $L_i < R$ are left ideals. Write $1 = \sum_{i\in I} e_i$ for $e_i \in L_i$, where almost all e_i are 0. Let $J = \{i \in I : e_i \neq 0\}$, then for all $a \in R$, $a = \sum_{i\in I} ae_i = \sum_{i\in J} ae_i$. Then $R = \coprod_{i\in J} L_i$ is a finite sum of ideals.*

Also, $e_j = \sum_{i\in J} e_ie_j \in L_i$, so $e_ie_j = e_j$ if $i = j$ and $e_ie_j = 0$ if $i \neq j$.

Consider $(*)$ condition: $\{e_i\}_{i\in J}$ are orthogonal idempotent elements and they partition 1. Note that this condition does not need to distinguish between left and right ones.

Conversely, if $\{e_i\}_{i\in J}$ satisfies $(*)$ then $L_i = Re_i$ are left ideals and $R = \coprod_{i\in J} L_i$.

Proposition 8.1.14. *Left semisimpleness and right semisimpleness are equivalent.*

Proof. Let R be a left semisimple ring so that $R = \coprod_{i \in I} Re_i$ and Re_i are minimal. Then $R = \coprod_{i \in I} e_i R$. For arbitrary i, we show that $e_i R$ is simple by simplicity test.

Let $e = e_i$. Take $0 \neq a \in eR$, then $ea = a$. Therefore, $\sum e_i = 1$, and so $\sum ae_i = a \neq 0$, so there exists j such that $ae_j \neq 0$. Now $0 \neq Rae_j \subseteq Re_j$ is simple, then $Rae_j = Re_j$, so $\exists b \in R$ such that $bae_j = e_j$.

Take $f : Re \to Re_j$ by sending $x \mapsto xae_j$, this is a homomorphism of left R-modules. Now $f(e) = eae_j = ae_j \neq 0$, so $f \not\equiv 0$. By Schur's lemma, f is an isomorphism. Now $f(abe) = abeae_j = abae_j = ae_j = f(e)$, so $abe = e \in aR$. □

Definition 8.1.15 (Minimal Ideal)**.** *The definition of a minimal ideal of ring R is equivalent to the following conditions:*

- *N is nonzero and if K is an ideal of R with $K \subseteq N$, then either K is trivial or $K = N$.*
- *N is a simple R-module.*

Lemma 8.1.16. *A (left) Rmodule M is semi-simple if and only if M is a sum of simple submodules.*

Proof.

- If M is semisimple, then $M = \bigoplus_{j \in J} S_j$, where every S_j is simple. Given a subset $I \subseteq J$, define $S_I = \bigoplus_{j \in I} S_j$. If N is a submodule of M, we see, using Zorn's Lemma, that there exists a subset I of J maximal with $S_I \cap N = \{0\}$. We claim that $M = N \oplus S_I$, which will follow if we prove that $S_j \subseteq N + S_I$ for all $j \in J$. This inclusion holds, obviously, if $j \in I$. If $j \notin I$, then the maximality of I gives $(S_j + S_I) \cap N \neq \{0\}$. Thus, $s_j + s_I = n \neq 0$ for some $s_j \in S_j$, $s_I \in S_I$, and $n \in N$, so that $s_j = n - s_I \in (N + S_I) \cap S_j$. Now $s_j = 0$, lest $s_I \in S_I \cap N = \{0\}$. Since S_j is simple, we have $(N + S_I) \cap S_j = S_j$; that is, $S_j \subseteq N + S_I$.

- Suppose, conversely, that every submodule of M is a direct summand. We begin by showing that each nonzero submodule N contains a simple submodule. Let $x \in N$ be nonzero; by Zorn's Lemma, there is a submodule $Z \subseteq N$ maximal with $x \notin Z$. Now Z is a direct summand of M, by hypothesis, and so Z is a direct summand of N, i.e. $N = Z \oplus Y$. We claim that Y is simple. If Y is a proper nonzero submodule of Y , then $Y = Y \oplus Y$ and $N = Z \oplus Y = Z \oplus Y \oplus Y$. Either $Z \oplus Y$ or $Z \oplus Y$ does not contain x [lest $x \in (Z \oplus Y) \cap (Z \oplus Y) = Z$], contradicting the maximality of Z. Next, we show that M is semisimple. By Zorn's Lemma, there is a family $(S_k)_{k\in K}$ of simple submodules of M maximal with the property that they generate their direct sum $D = \bigoplus_{k\in K} S_k$. By hypothesis, $M = D \oplus E$ for some submodule E. If $E = \{0\}$, we are done. Otherwise, $E = S \oplus E$ for some simple submodule S, by the first part of our argument. But now the family $\{S\} \cup (S_k)_{k\in K}$ violates the maximality of $(S_k)_{k\in K}$, a contradiction.

□

Lemma 8.1.17. *Let R be a semi-simple ring, $R = \coprod L_i$ where L_i's are minimal (left) ideals. Then every simple (left) R-module is isomorphic to L_i for some i.*

Proof. Note that $\mathbf{Hom}_R(R, M) = M$. Apply this to M as simple modules. Therefore, there exists a non-zero $R = \coprod L_i \to M$. Therefore, there exists a non-zero map $L_i \to M$ for some I. By Schur's lemma, $L_i \cong M$. □

Theorem 8.1.18. *Let R be a ring. The following are equivalent.*

1. *R is semi-simple.*
2. *Every (left) R-module is semi-simple.*
3. *Every (left) R-module is projective.*
4. *Every (left) R-module is injective.*
5. *All short exact sequences split.*

Proof. (1) ⇒ (2): Denote $R = \coprod L_i$. Let M be any left R-module. Take $m \in M$ and $L_i m \subseteq M$, then $L_i m \subseteq L_i$ is simple, so $L_i m = \begin{cases} 0 & , \\ L_i & , \text{simple} \end{cases}$. Then $M = R \cdot M = \sum\limits_{m\in M, i} L_i M$ is the sum of simple submodules. By lemma, M is semi-simple.

(2) ⇒ (3): Denote $M = \coprod M_j$ as a direct sum of simple modules. Since (2) ⇒ (1) trivially, R is semi-simple, then $R = \coprod L_i$ simple modules and every M_j is isomorphic to L_i for some i. Then L_i projective implies M_i is projective. Therefore, M is projective.

(3) ⇒ (5): Note that the sequence

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] & N \arrow[r] & P \arrow[r] & 0 \end{tikzcd}$$

is split since P is projective.

(5) $\Rightarrow$ (4): M is injective if for every module Y and a submodule $X \subseteq Y$, every homomorphism $X \to M$ extends to $Y \to M$. Therefore we have

$$\begin{tikzcd}
0 \arrow[r] & X \arrow[r, "g"] \arrow[d, "f"'] & Y \arrow[r] \arrow[l, bend right, "h"'] \arrow[dl, dashed] & Z \arrow[r] & 0 \\
 & M & & &
\end{tikzcd}$$

and induces the map from $Y \to M$ by $f \circ h$, since $(f \circ h) \circ g = f \circ (h \circ g) = f$.

(4) $\Rightarrow$ (1): Prove that R is a sum of minimal left ideals. Let I be the sum of all minimal left ideals. We show that $I = R$. Suppose that $I \neq R$, so $I < R$, then there exists a maximal left ideal $I \subseteq M \subseteq R$. Consider $0 \to M \to R \to R/M \to 0$. This splits because M is injective. Hence, there exists a submodule $N \subseteq R$ such that $N \cong R/M$. Now N is simple because R/M is simple. Because $M \cap N = 0$, we have $I \cap N = 0$. Hence, $I + N \supsetneq I$. But $I + N$ is a sum of simple modules, contradiction. □

Recall that if $D_1, \cdots, D_s$ are division rings, then $R = M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$ is semi-simple. We also have the converse result.

Theorem 8.1.19. *Every semi-simple ring is of the form as above.*

Proof. Let R be the direct sum of minimal let ideals. Then $R \cong \coprod_{i=1}^{s} L_i^{\oplus n_i}$, where $L_1, \cdots, L_s$ are all non-isomorphic minimal left ideals. Now we can write $R = \mathbf{Hom}_R(R, R) = \mathbf{Hom}_R(\coprod L_i^{\oplus n_i}, \coprod L_j^{\oplus n_j}) = \mathbf{Hom}_R(\coprod N_i, \coprod N_j)$ as we denote $N_i = L_i^{\oplus n_i}$. This is just the set of matrices $\left\{ \begin{pmatrix} s_{11} & \cdots s_{1s} & \\ \vdots & \ddots & \vdots \\ s_{s1} & \cdots & s_{ss} \end{pmatrix} : s_{ij} = \mathbf{Hom}_R(N_j, N_i) \right\}$. If $i \neq j$, $\mathbf{Hom}_R(N_j, N_i) = 0$ since $\mathbf{Hom}_R(L_j, L_i) = 0$. Now for $i = j$, $\mathbf{Hom}_R(N_i, N_i) = \mathbf{Hom}_R(L_i^{\oplus n_i}, L_i^{\oplus n_i}) = M_{n_i}(D_i)$, where $D_i = \mathbf{Hom}_R(L_i, L_i) = \mathbf{End}_R(L_i)$, which is a division ring. Note that all matrices in the set above is diagonal, so we can write

$$R = \left\{ \begin{pmatrix} M_{n_1}(D_1) & 0 & \cdots & 0 \\ 0 & M_{n_2}(D_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_{n_s}(D_s) \end{pmatrix} \right\} = M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s).$$

□

Remark 8.1.20. *R has exactly s simple modules $N_1, \cdots, N_s$, up to isomorphism. We have $D_i = End_R(N_i)$ and $\dim_{D_i}(N_i) = n_i$. Therefore, s does not depend on the decomposition.*

From the proof, we have

$$\begin{aligned} R = \mathbf{Hom}_R(R, R) = End_R(R) \\ x \mapsto l_x \end{aligned}$$

should be viewed as a right module, with $l_x \circ l_y = l_{xy}$. Note $D_i = End_R(L_i)$ for L_i minimal right ideal.

Suppose $R = M_n(D) \cong L^{\oplus n}$ where L is a right module. Consider

$$\begin{aligned} D \to End_R(L) \\ x \mapsto l_x \end{aligned}$$

and this is an isomorphism. Indeed, by writing $D \xrightarrow{f} \mathbf{Hom}_R(L, L)$, we have

$$D^n \xrightarrow{f^{\oplus n}} \mathbf{Hom}_R(R = L^{\oplus n}, L) = L \cong D^n$$

so $f^{\oplus n}$ is the identity map, then f is an isomorphism. As $R \cong L^{\oplus n} = L \oplus \cdots \oplus L$, but M is a right simple R-module, so $M \cong L$. Therefore, $D \cong End_R(M)$, $n = \dim_D(M)$, which are both unique for a ring R.

In general, when $R = M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$, let $K_i = (0, \cdots, 0, L_i, 0, \cdots, 0)$, so L_i's are all simple right R-modules up to iomsophism. s is the number of all such modules. Now $D_i = End_R(L_i)$, $n_i = \dim_{D_i}(L_i)$ are both unique.

If we use left module structure instead, we will recover a simple left R-module structure with L_i's as minimal left ideals, then $D_i^{op} \cong End_R(L_i')$. For M a (left) R-module such that $M \cong L^{oplusa_i} \oplus \cdots \oplus L_s^{\oplus a_s}$ the information is essentially the tuple of dimensions, and

$$R\text{-}Mod \cong D_1\text{-}Mod \times \cdots \times D_s\text{-}Mod M_n(D)\text{-}Mod \cong D\text{-}Mod$$

Note that the second isomorphism works for all rings D. This is called the Monta equivalence. Let D be a ring and $R = M_n(D)$, then ${}_RD^n_D$ acts as a bimodule, and the operations commute:

$$\begin{aligned} D\text{-}Mod &\leftrightarrow M\text{-}Mod \\ N &\mapsto D^n \otimes_D N \\ \mathbf{Hom}_R(D^n, M) &\mapsfrom M \end{aligned}$$

8.2 Jacobson Radical

Definition 8.2.1 (Radical). *Let R be a ring and M is a (left) R-module. Recall that the radical of M is the intersection of all submodules of M, denoted Rad(M). If the intersection is empty, then we say Rad$(M) = M$.*

Remark 8.2.2. *Some modules don't have maximal submodules. The proof for maximal ideals on Zorn's lemma does not work here, because the union of the modules is the entire module M: the union contains identity element, unlike the union of ideals, which doesn't contain the identity element.*

A submodule $N \subseteq M$ is maximal if and only if M/N is simple.

Example 8.2.3. 1. *Rad$_{\mathbb{Z}}(\mathbb{Z}) = \bigcap_{p\ prime} p\mathbb{Z} = 0$.*

2. *Rad$_{\mathbb{Z}}(\mathbb{Q}) = \mathbb{Q}$ because it has no maximal submodule. If N is maximal, then $\mathbb{Q}/N$ is simple, so $\mathbb{Q}/N \cong \mathbb{Z}/p\mathbb{Z}$. We then have $Q \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$, but $\mathbb{Q}$ is divisible and $\mathbb{Z}/p\mathbb{Z}$ is not.*

3. *Rad$_R(M/Rad_R(M)) = 0$.*

Proposition 8.2.4. *Let M be a (left) R-module.*

1. *Let M be semisimple, then Rad$(M) = 0$.*

2. *If M is Artinian, and Rad$(M) = 0$, then M is semisimple.*

Proof. 1. Since M is semisimple, we have $M = \coprod_{i \in I} M_i$ of simple modules. Write $N_j = \coprod_{i \neq j} M_j \subseteq M$, then $M/N_j = M_j$ simple, so N_j is maximal. hence, $\bigcap_j N_j = 0$, so Rad$(M) = 0$.

2. Let N be the sum of all simple submodules of M. Assume $N \neq M$, then there exists a minimal submodule $N' \subseteq N$ such that $N + N' = M$.

Claim 8.2.5. *$N \cap N' = 0$.*

Subproof. Note that $N' \neq 0$ since $M \neq N$. Assume that $N \cap N' \neq 0$, since $\mathrm{Rad}(M) = 0$, then there exists a maximal submodule $M' \subseteq M$ such that $N \cap N' \not\subseteq M'$. Now $M' \subsetneq (N \cap N') + M' = M$.

Claim 8.2.6. *$N + (M' \cap N') = M$.*

Subproof. Take $m \in M$, then $m = x + y$ for $x \in N$ and $y \in N'$. Now $y = z + m'$ where $z \in N \cap N'$ and $m' \in M'$. Then $m' = y - z \in N'$. Hence, $m' \in M' \cap N'$. Now $m' = (x + z) + m'$, where $x + z \in N$ and $m' \in M' \cap N'$. ■

Because $N + N' = M$ and $N + (M' \cap N') = M$, then by minimality of N', $M' \cap N' = N'$, so $N' \subseteq M'$. But $N \cap N' \not\subseteq M'$, contradiction. ■

Now $M = N \oplus N'$ with $N' \neq 0$. N' contains a simple submodule P because M is Artinian. But $P \not\subseteq N$ by definition of N, contradiction.

□

Lemma 8.2.7. *Consider a ring R as its own left module. Now $Rad_R(R) = \{a \in R : 1 - xa \text{ has left inverse } \forall x \in R\}$.*

Proof. $\subseteq$: Take $a \in \mathrm{Rad}_R(R)$. Suppose $1 - xa$ has no left inverse, then $R(1 - xa) \neq R$, with $R(1-xa) \subseteq M \subseteq R$ where M is a maximal left ideal. For $a \in \mathrm{Rad}(R)$, $xa \in \mathrm{Rad}(R)$, then $1 = (1 - xa) + xa \in M$ because $1 - xa \in M$ and $xa \in \mathrm{Rad}(R) \subseteq M$, contradiction.

$\supseteq$: Let $M \subseteq R$ be a maximal left ideal, $a \in R>$ Suppose $1 - xa$ has a left inverse for all $x \in R$. Suppose, towards contradiction, that $a \notin M$, then $a \not\subseteq M$, so $M \not\supseteq Ra + M = R$. Then $1 = xa + y$ where $xa \in R$ and $y \in M$, so $y = 1 - xa \in M$ has a left inverse, then $zy = 1$ is in M. However, $1 \notin M$ because it is a maximal ideal, so we reach a contradiction. □

Lemma 8.2.8. *If $1 - ab$ is left invertible, so is $1 - ba$.*

Proof. Suppose $c(1 - ab) = 1$, then $(1 + bca)(1 - ba) = 1$. □

Proposition 8.2.9. *$Rad_R(R) = \{a \in R : 1 - xay \in R^\times, \forall x, y \in R\}$.*

Proof. We know $\mathrm{Rad}_R(R) = \{a \in R : 1 - xy \text{ is left invertible } \forall x \in R\}$, so $\Leftarrow$ direction is clear.

($\Rightarrow$): $a \in \mathrm{Rad}_R(R)$, $x, y \in R$, we have $1 - yxa$ is left invertible. By lemma, $1 - xay$ is left invertible, let $b(1 - xay) = 1$. Then $1 + ybxa$ is left invertible, so by lemma $1 + bxay$ is left invertible. But $1 + bxay = b$, so b (and $1 - xay = b^{-1}$) is invertible. □

Remark 8.2.10. *This characterization is symmetric in left and right. $Rad_R(R)$ is a two-sided ideal in R, called the Jacobina radical of R, or $J(R)$. $Rad_R(R)$ is also the intersection of all maximal right ideals. If $R \neq 0$, then $J(R) \neq R$ (maximal ideal exists).*

Theorem 8.2.11. *Let R be a ring. Then R is semisimple if and only if R is Artinian and $J(R) = 0$.*

Remark 8.2.12. *Sometimes R doesn't have any non-trivial biideals.*

Proof. ($\Rightarrow$): Suppose $R = M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$ for $D_1, \cdots, D_s$ division rings, so $M_{n_i}(D_i)$'s are simple components of R, unique up to isomorphism. When $R = M_n(D)$, $D \hookrightarrow R$ by $d \mapsto \operatorname{diag}(d, \cdots, d)$, so left R-modules are left D-modules. For all $R \supseteq I_1 \supseteq I_2 \supseteq \cdots$, we have $\infty > \dim_D(R) \geq \dim_D(I_1) \geq \cdots \geq 0$, so the sequence stabilizes.

Claim 8.2.13. *$M_n(D)$ has no non-trivial two-sided ideals.*

Subproof. Suppose $I \subseteq M_n(D)$ is and $I \neq 0$, then let $x = \sum\limits_{i,j} d_{ij}e_{ij} \in I$ be non-zero. Suppose $d_{kl} \neq 0$, then for all s, $e_{sk} \times e_{ls} = d_{kl}e_{ss} \in I$, so $e_{ss} \in I$ for all s. Hence, $1 = \sum\limits_s e_{ss} \in I$. ■

Claim 8.2.14. $J(R) = 0$.

Subproof. Note that the set

$$\{\begin{pmatrix} 0 & \cdots & 0 & * & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & * & 0 & \cdots & 0 \end{pmatrix} \in M_n(D)\}$$

is a maximal left ideal, so $J(M_n(D)) = 0$. Therefore, $J(R) = \prod\limits_i J(M_{n_i}(D_i)) = 0$. ■

□

Definition 8.2.15 (Simple). *A ring R is simple if $R \neq 0$ and R has no non-trivial two-sided ideals.*

Example 8.2.16. *$M_n(D)$ is simple for D division ring.*

Theorem 8.2.17. *Every simple Artinian ring is isomorphic to $M_n(D)$ for some D division ring.*

Proof. Let $R \neq 0$ be a simple Artinian ring. $J(R) \neq R$ is a two-sided ideal, so $J(R) = 0$. Therefore, R is semisimple. Write $R = M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$. If $s \geq 2$, then $M_{n_1}(D_1) \times 0 \times \cdots \times 0 \subseteq R$ is a non-trivial two-sided ideal. □

8.3 Algebra

Definition 8.3.1 (R-Algebra). *Let R be a commutative ring and S be a ring. S is an R-algebra if S has a structure of R-module such that*

1. *Two addition structures are the same.*

2. *$\forall a \in R$, $x, y \in S$, there is $a(xy) = (ax)y = x(ay)$.*

Remark 8.3.2. *For all $a \in R$ and $x \in S$, there is $ax = a(1_s \cdot x) = (a1_s) \cdot x$. Therefore, scalar products corresponds with products. Consider $R \to S$ by sending $a \mapsto a1_s$, then this is a ring homomorphism. Also, $\forall a \in R, x \in S$, we have $f(a)x = xf(a)$: $f(a)x = (a1_s) \cdot x) = ax$ and $xf(a) = x(a1_s) = a(x \cdot 1_s) = ax$. Then im$(f) \subseteq Z(S)$.*

Claim 8.3.3. *Conversely, suppose $f : R \to S$ is a ring homomorphism where R is commutative and im$(f) \subseteq Z(S)$, then S can be given an R-algebra structure.*

Proof. Note $ax = f(a) \cdot x$. Check the necessary conditions. □

Definition 8.3.4 (Category, Homomorphism). *Let R be a commutative ring , then* **Alg**(R) *is the category of R-algebras. The morphisms in* **Alg**(R) *are R-algebra homomorphisms that*

1. *respect all structures, or*

2. *by claim, the following diagram commutes by the homomorphism from $S \to T$:*

$$\begin{tikzcd}
 & R \arrow[dl] \arrow[dr] & \\
S \arrow[rr] & & T
\end{tikzcd}$$

Remark 8.3.5. *In particular,* **Alg**$(\mathbb{Z})$ *is the category of rings. In* **Alg**(R)*, the initial object is R, the final object is 0. Products are the same as products in the category of rings, but the coproducts are complicated. However, in* **CAlg**(R)*, category of commutative rings over R, the coproduct of S and T is $S \otimes_R T$ by $(x \otimes y)(x' \otimes y') = xx' \otimes yy'$.*

So for all $f : S \to V$ and $g : T \to V$, we have $S \otimes_R T \to V$ by $x \otimes y \mapsto f(x)g(y)$. Note that V needs to be commutative.

8.4 Representation of Finite Groups

We can use three different languages to describe the groups.

Definition 8.4.1 (First Language: G-space)**.** *Let G be a group and F be a field. A G-space is a vector space over F, together with an G-action by linear operators:*

1. $g(v_1 + v_2) = gv_1 + gv_2)$,
2. $g(\lambda v) = \lambda(gv)$ *for all* $\lambda \in F$,
3. $(gh)v = g(hv)$,
4. $ev = v$.

The first two properties describe linearity, and the last two properties describe the G-action.

Definition 8.4.2 (Second Language: Representation)**.** *A representation of G over F is a group homomorphism $\rho : G \to GL(V)$ for some vector V over F.*

Remark 8.4.3. *G-spaces corresponds with representations by $gv = \rho(g)(v)$.*

Definition 8.4.4 (Third Language: Group Action)**.** *Let G be a group and F be a field. The group algebra is the vector space spanned by G:*

$$F[G] = \{\sum_{g \in G} G_g g : a_g \in F, \textit{ almost all } 0\} = \{f : G \to F : f(g) = 0 \textit{ for almost all } g\}.$$

There is a multiplication operation on $F[G]$ following the multiplication on G, given by

$$\Big(\sum_{g \in G} a_g g\Big)\Big(\sum_{h \in G} b_h h\Big) = \sum_{g \in G}\sum_{h \in G} a_g b_h gh = \sum_{l \in G}\Big(\sum_{gh = l} a_g b_h\Big)l.$$

We can view $G \hookrightarrow F[G]$ with only one non-zero coefficient. Then G is a basis of $F[G]$ and $\dim(F[G]) = |G|$.

Remark 8.4.5. *$F \hookrightarrow F[G]$ is given by $\lambda \mapsto \lambda \cdot e$, then F is a subring of $F[G]$.*

Remark 8.4.6 (Naturality)**.** *If we have a group homomorphism $H \to G$, then there is a F-algebra homomorphism $F[H] \to F[G]$. Therefore, we have a functor* **Grp** $\to$ $F-$**Algebra** *by $G \mapsto F[G]$. This functor also has a right adjoint $S \mapsto S^\times$ such that*

$$\begin{tikzcd}\left(f : G \to S^\times\right) \arrow[r, bend left, "extend"] & \left(h : F[G] \to S\right) \arrow[l, bend left, "restrict"]\end{tikzcd}$$

where G is invertible.

Remark 8.4.7. *Suppose V is a G-space, then it is a left $F[G]$-module with the structure $\left(\sum\limits_{g\in G} a_g g\right) \cdot v = \sum\limits_{g\in G} a_g(gv)$. Moreover, the left $F[G]$-module structure then gives the structure of a G-space by restricting to $G \subseteq F[G]$. Therefore, we have*

	G-spaces	*Representations*	*Left $F[G]$-modules*
Basic Info	V 0 V *with* $\dim(V) = 1$ $V = F$ *, trivial action*	$\rho : G \to GL(V)$ $\rho : G \to \{e\}$ *zero representation* $\rho : G \to F^\times$ *as character* $\rho : G \to F^\times$, $\rho(g) = 1$ *as trivial representation*	V 0 V *with* $\dim(V) = 1$ $V = F$, $(\sum\limits_{g\in G} a_g g)v = \sum\limits_{g\in G} a_g v$
Category (all are Abelian)	*Vector spaces as Objects, Linear mappings $V \to W$ that preserves G-actions as Morphisms*	*Representations as Objects, Linear maps $f : V \to W$ such that $f(\rho(g)(v)) = \rho(g)f(v)$ as Morphisms*	*Category of $F[G]$-modules*
Direct Sum	$V \otimes W$*:* $g(v + w) = gv + gw$	$\rho \oplus \mu : G \to GL(V \oplus W)$	$V \oplus W$ *as $F[G]$-modules*
Isomorphism	*G-equivalent isomorphisms of vector Spaces*	*Isomorphisms of vector spaces $f : V \to W$ such that* $\begin{tikzcd} G \arrow[r, "\rho"] \arrow[dr, "\mu"'] & GL(V) \arrow[d, "\sim"', "conjugate\ by\ f"] \\ & GL(W) \end{tikzcd}$	*Module Isomorphisms*

Figure 8.1: Relationship between G-spaces, Representations and $F[G]$-Modules

When V is finite-dimensional, $GL(V) = GL_n(F)$, so a representation represents G as matrices $\rho : G \to GL_n(F)$, $\mu : G \to GL_m(F)$. This is (almost) another language: for $\rho \oplus \mu : G \to GL_{m+n}(F)$ that sends $g \mapsto \begin{pmatrix} \rho(g) & 0 \\ 0 & \mu(g) \end{pmatrix}$, where $\rho \cong \mu$ if and only if $\exists A \in GL_n(F)$ such that for all $g \in G$, $\mu(g) = A\rho(g)A^{-1}$.

Example 8.4.8. *Let G be a finite group of order n, then $F[G] = F[t]/(t^n - 1)$. When $F = \mathbb{Q}$, $\mathbb{Q}[G] = \prod\limits_{d|n} \mathbb{Q}[t]/\varphi(d) = \prod\limits_{d|n} \mathbb{Q}(\xi_d)$. Moreover, if G is commutative, then the group algebra is also commutative.*

Theorem 8.4.9. *Let G be a finite group and F be a field. Then $F[G]$ is semisimple as a ring if and only if $char(F) \nmid |G|$. In particular, if $char(F) = 0$, then every $F[G]$ structure is semisimple.*

Proof. ($\Rightarrow$): For $\varepsilon(g) = 1$, we have $F[G] \xrightarrow{\varepsilon} F \to 0$ as a short exact sequence. Then it is a surjective $F[G]$-module homomorphism (F is the $F[G]$-module of trivial representation). Note that the sequence splits, so there exists a section $f : F \to F[G]$. Then for all $g \in G$, $g \cdot f(1) = f(g \cdot 1) = f(1)$, so $f(1) = F[G]^G = F \cdot N$ where $N = \sum\limits_{g \in G} g$. Note that $f(1) = \lambda N$, then $1 = \varepsilon(f(1)) = \varepsilon(\lambda N) = \lambda |G|$, so $|G| \neq 0$, and so $\mathrm{char}(F) \neq |G|$.

($\Leftarrow$): Consider an arbitrary short exact sequence of $F[G]$-modules:

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "f"] & M \arrow[r, "g"] & P \arrow[r] & 0 \end{tikzcd}$$

then there exists $h : M \to N$ such that $hf = 1$. Note that only linear $\mathbf{Hom}_F$ needs $\mathbf{Hom}_{F[G]}$. We set $\bar{h} = \frac{1}{|G|} \sum\limits_{g \in G} g^{-1} h(gm)$. We only need to check that $\bar{h} f = 1$, with $\bar{h}$ an $F[G]$-linear map. Therefore, every short exact sequence splits, so $F[G]$ is semisimple. □

Remark 8.4.10. *$char(F) \nmid |G|$ if and only if $F[G]$ is semisimple. Then $F[G] = M_{d_1}(D_1) \times \cdots \times M_{d_r}(D_r)$. All simple $F[G]$-modules are $L_i = 0 \times \cdots \times 0 \times D_i^{d_i} \times 0 \times \cdots \times 0$. Now $|G| = \sum\limits_{i=1}^{r} d_i^2 \dim(D_i) < \infty$, where $D_i = End_{F[G]} L_i$ is also an F-algebra. In particular, $\dim_F L_i = d_i \dim(D_i) < \infty$.*

Claim 8.4.11. *Let M be an $F[G]$-module with $\dim_F(M) < \infty$, then $M = L_1^{\oplus a_1} \oplus \cdots \oplus L_r^{\oplus a_r}$ with integers $a_1, \cdots, a_r$ uniquely determined by M. Note that this also works for $\dim_F(M) = \infty$.*

Remark 8.4.12 (Translation)**.** *M finite dimensional G-space, L_i simple G-spaces.*

Remark 8.4.13 (Translation). *Let $\rho : G \to GL(V)$ be a representation with* $\dim_F(V) < \infty$*. We have $\rho_i : G \to GL(L_i)$ for $1 \le i \le r$ are irreducible representations of G. For all ρ, there is $\rho = \rho_1^{\oplus a_1} \oplus \cdots \oplus \rho_r^{\oplus a_r}$, so there exists a basis of V such that ρ is given by block matrices $\rho_1, \cdots, \rho_r$.*

From now on, we can assume F is algebraically closed with characteristic 0.

Lemma 8.4.14. *Let D be a finitely-dimensional division F-algebra over an algebraically closed field F, then $D = F$.*

Proof. Note we have $F \hookrightarrow D$ by $a \mapsto a \cdot 1$. For all $d \in D$, we have the set $\{1, d, d^2, \cdots\}$ that is linearly dependent over F. Then d is a root of $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$. Now because F is algebraically closed, then $f(x) = a_n(x - b_1) \cdots (x - b_n)$. Note $f(d) = 0$ and D is a division ring, so $d - b_i = 0$ for some i. Therefore, $d = b_i \in F$, so $D = F$. □

Remark 8.4.15. *Now $F[G] = M_{d_1}(F) \times \cdots \times M_{d_r}(F)$, so $|G| = d_1^2 + \cdots + d_r^2$. Note simple modules are $L_i = 0 \times \cdots \times 0 \times F^{d_i} \times 0 \times \cdots \times 0$, with $\dim_F(L_i) = d_i$. Therefore, $|G| = \sum_{i=1}^{r} d_i^2 = \sum_{i=1}^{r} (\dim_F(\rho_i))^2$.*

Example 8.4.16. *$F[G]$ as a left $F[G]$-module is called a regular $F[G]$-module, regular G-space or regular representation.*

We have $F[G] = M_{d_1}(F) \times \cdots \times M_{d_r}(F) \cong L_1^{\oplus d_1} \oplus \cdots \oplus L_r^{\oplus d_r}$, which are also corresponding to sum of columns of matrices. Therefore, $\rho_{reg} = \rho_1^{\oplus d_1} \oplus \cdots \oplus \rho_r^{\oplus d_r}$ for $d_i = \dim_F(\rho_i)$.

This creates a new question: how to find irreducible representations?

Lemma 8.4.17. *$Z(M_d(F)) = F$.*

Proof. $a = (a_{ij})$ is in the center, compute $a l_{kl} = l_{kl} a$, then $a_{ij} = 0$ for $i \neq j$, all a_{ii} are equal. □

Remark 8.4.18. *Now $F[G] = M_{d_1}(F) \times \cdots M_{d_r}(F)$, so $Z(F[G]) \cong \prod_{i=1}^{r} M_{d_i}(F) \cong F^r$, so the number of irreducible representations is just $\dim_F(Z(F[G]))$. Now $u = \sum_{g \in G} a_g g \in Z(F[G])$ if and only if $ux = xu$ for all $x \in G$. Therefore, we have*

$$\sum_{g \in G} a_g g x = \sum_{g \in G} a_g x g = \sum_{g \in G} a_g (x g x^{-1}) x = \sum_{g' \in G} a_{x^{-1} g' x} g' x,$$

so $a_g = a_{x^{-1} g x}$ for all $g, x \in G$.

Let $G = C_1 \sqcup \cdots \sqcup C_s$ be the disjoint union of conjugacy classes, and let $v_i = \sum_{g \in C_i} g$, then $\{v_i\}_{i \in I}$ forms a basis for $Z(F[G])$. Therefore, we conclude the following.

Theorem 8.4.19. *The number of conjugacy classes is the same as the number of irreducible representations.*

Remark 8.4.20. *Although they are equal, these two sets do not have a "good" bijection.*

Consider $G \to \mathrm{GL}_1(F) = F^\times$.

Proposition 8.4.21. *Let G be a finite group. The following are equivalent:*

1. *G is Abelian.*
2. *Every irreducible representation has dimension 1.*
3. *The number of irreducible representations is $|G|$.*

Proof. Recall $F[G] = M_{d_1}(F) \times \cdots \times M_{d_r}(F)$ where r is the number of irreducible representations $\rho_1, \cdots, \rho_r$, and $d_i = \dim(\rho_i)$. Then G is Abelian if and only if $F[G]$ is commutative if and only if $d_1 = d_2 = \cdots = d_r = 1$. Therefore, 1) $\iff$ 2). Also, because $|G| = \sum\limits_{i=1}^{r} d_i^2 \geq \sum\limits_{i=1}^{r} 1^2 = r$, so $r = |G|$ if and only if all d_i's are 1. Therefore, 2) $\iff$ 3). □

Therefore, for Abelian group G we have $|\mathbf{Hom}(G, F^\times)| = |G|$. Now, let G be an arbitrary finite group with homomorphism $\rho : G \to F^\times$. Note that there is the canonical decomposition into the Abelianization $G^{ab} = G/[G, G]$. Then $\mathbf{Hom}(G, F^\times) = \mathbf{Hom}(G^{ab}, F^\times)$. Hence, G has exactly $|G^{ab}| = [G : [G, G]]$ 1-dimensional representations. Note that 1-dimensional representations are irreducible.

Example 8.4.22. 1. *Suppose $G = S_n$. Note that the number of irreducible representations is the number of conjugacy classes.*

Note F^n is a S_n-space, called the standard S_n-space. Note that

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] & F^n \arrow[r, two heads] & F \arrow[r] & 0 \end{tikzcd}$$

where the map $F^n \to F$ is a surjective homomorphism of modules given by $(a_i) \mapsto \sum a_i$. Moreover, there is a section $F \to F^n$ given by $1 \mapsto \frac{1}{n} \sum g_i$. Now consider the kernel M, then $F^n \cong M \oplus F$. So M has $n-1$-dimensions.

We have $\rho_{st} = \rho'_{st} \oplus \mathbb{1}$, where $\mathbb{1}$ is the trivial action that sends every element to identity, and ρ'_{st} is irreducible. Then ρ'_{st} has dimension $n-1$.

For arbitrary n, consider $S_n \to F^\times$, but $[S_n, S_n] = A_n$, so $S_n/[S_n, S_n]$ is cyclic of order 2, then there are two representations $\sigma \mapsto Sgn(\sigma) = \pm 1$. In particular, for $G = S_3$, we have $d_n = 1, d_2 = 1, d_3 = 1$, with $\sum d_i^2 = 6 = |S_3|$.

For $G = S_4$, we have 5 representations by checking decomposition of 4, with two dimension-1 representations, then by decomposition we know $d_1 = d_2 = 1$, $d_3 = 2$, $d_4 = d_5 = 3$.

2. *For $G = D_8$ or Q_8, note $|G^{ab}| = 4$, $r = 3$, then $d_1 = 1, d_2 = 1, d_3 = 1, d_4 = 1, d_5 = 2$. In particular, $F[G] = F \times F \times F \times F \times M_2(F)$ for algebraically closed field, e.g. $\mathbb{C}$.*

   If $F = \mathbb{Q}$, the formula still holds for $G = D_8$, but $\mathbb{Q}[Q_8] = F \times F \times F \times F \times \mathbb{H}$, where $\mathbb{H} = M_1(\mathbb{H})$.

Remark 8.4.23 (Open Problem). *Suppose G, H are groups such that $\mathbb{Z}[G] \cong \mathbb{Z}[H]$, does $G \cong H$ hold?*

8.5 Characters

Definition 8.5.1 (Character). *Suppose we have a representation $\rho : G \to GL(V)$ for finite group G and $\dim(V) < \infty$, take $g \in G$, then the trace is $Tr(\rho(g)) = \chi_\rho(g)$. Here $\chi_\rho : G \to F$ is the character of ρ.*

Property 8.5.2.

1. *$\rho \cong \rho' \Rightarrow \chi_\rho = \chi_{\rho'}$.*
2. *$\chi_{\rho\oplus\rho'} = \chi_\rho + \chi_{\rho'}$.*
3. *$\chi_\rho(hgh^{-1}) = \chi_\rho(g)$.*
4. *$\chi_\rho(e) = \dim(\rho)$.*
5. *For 1-dimensional $\rho : G \to F^\times$, we have $\chi_\rho = \rho$.*

Example 8.5.3. *For $\rho_{reg} : G \to GL(F[G])$, $\chi_{reg} := \chi_{\rho_{reg}}$. Then G creates a basis for $F[G]$, so for any $g \in G$, $\rho_{reg}(g)(h) = gh$. Note $\rho_{reg}(g)$ is monomimal. Moreover, $gh \neq h$ for $g \neq e$, so $\chi_{reg}(g) = \begin{cases} 0, & \text{if } g \neq e \\ |G|, & \text{if } g = e \end{cases}$.*

Let $\rho_1, \cdots, \rho_r$ be characters of irreducible representations (irreducible characters). Then $\rho_{reg} = \rho_1^{d_1} \oplus \cdots \oplus \rho_r^{d_r}$ for $d_i = \dim(\rho_i)$. Hence, $\chi_{reg} = \sum\limits_{i=1}^{r} d_i\chi_i$, where $\chi_{reg}(g) = \begin{cases} 0, & \text{if } g \neq e \\ |G|, & \text{if } g = e \end{cases}$.

Remark 8.5.4. *χ extends to $F[G]$ in the natural sense with $\chi(g) = tr(l_g)$.*

Remark 8.5.5. *Let $F[G] = M_{d_1}(F) \times \cdots \times M_{d_r}(F)$ where $e_1, \cdots, e_r$ are orthogonal idempotents that partition 1. Let M_j be the corresponding simple modules with $\dim(M_j) = d_j$, then $M_j = 0 \times \cdots \times L_j \times \cdots \times 0$, where L_j is the minimal j-th component, $L_j = F[G]e_j$. Let $m \in M_j$, then $\chi_j(e_i m) = \begin{cases} \chi_j(m), & i = j \\ 0, & j \neq j \end{cases}$, with $\chi_j(e_i m) = \chi_j(e_i^2 m e_i^{-1}) = \chi_j(m)$.*

Let us write $e_i = \sum\limits_{g\in G} a_{ig}g$ for $a_{ig} \in F$. Then $\chi_{reg}(e_i g^{-1}) = \chi_{reg}(\sum\limits_{h\in G} a_{ih}hg^{-1}) = \sum\limits_{h\in G} a_{ih}\chi_{reg}(hg^{-1}) = |G|a_{ig}$, but $\chi_{reg}(e_i g^{-1}) = \sum\limits_{j=1}^{r} d_j\chi_j(e_i g^{-1}) = d_i\chi_i(g^{-1})$. Hence, $e_i = \frac{d_i}{|G|}\sum\limits_{g\in G} \chi_i(g^{-1})g$.

Remark 8.5.6. *Let $Ch(G) = \{f : G \to F : f(ghg^{-1}) = f(h), \forall g, h \in G\}$, then $\dim(Ch(G))$ is just the number of conjugacy classes in G. Moreover, $Ch(G)$ has a bilinear form $\langle \chi, \eta \rangle = \frac{1}{|G|}\sum\limits_{g\in G} \chi(g^{-1})\eta(g) \in F$.*

Proposition 8.5.7. *The irreducible representations $\chi_1, \cdots, \chi_r$ form an orthonormal basis of $Ch(G)$.*

Proof. Note $\chi_j(e_i) = d_i\delta_i$. Also,

$$\chi_j(e_i) = \chi_j(\frac{d_i}{|G|}\sum_{g\in G}\chi_i(g^{-1})g) = \frac{d_i}{|G|}\sum_{g\in G}\chi_i(g^{-1})\chi_j(g) = d_i\left\langle \chi_i, \chi_j \right\rangle.$$

From orthonormality, we conclude that we have a basis. □

Theorem 8.5.8. *Suppose F is an algebraically closed field with $char(F) \neq |G|$. Let G be a finite group with $\rho_1, \cdots, \rho_r$ as irreducible representations of G, with irreducible characters $\chi_1, \cdots, \chi_r$ correspondingly. Then*

1. *Every representation ρ of G is isomorphic to $\rho_1^{\oplus n_1} \oplus \cdots \oplus \rho_r^{\oplus n_r}$ where $n_i = \langle \chi_\rho, \chi_i \rangle \in \mathbb{Z}$ and $\chi_\rho = \sum\limits_{i=1}^{r} n_i\chi_i$.*

2. *Two representations ρ and μ are isomorphic as G-spaces if and only if $\chi_\rho = \chi_\mu$.*

3. *A representation ρ is irreducible if and only if $\langle \chi_\rho, \chi_\rho \rangle = 1$.*

Proof. 1. By induction.

2. From $\chi_\rho = \chi_\mu$ we get a decomposition of ρ and of μ, then apply the first property.

3. We have $\rho = \rho_1^{\oplus n_1} \oplus \cdots \oplus \rho_r^{\oplus n_r}$, then $\langle \chi_\rho, \chi_\rho \rangle = \sum_{i=1}^{r} n_i^2$.

□

Example 8.5.9. *1. Consider $G = S_n$. We have the standard representation ρ_{st} acts on F^n, then $\chi_{st}(\sigma)$ is the number of fixed entries of an entry $\sigma \in S_n$. In particular, $\langle \mathbb{1}, \rho_{st} \rangle = \frac{1}{n!} \sum_{\sigma \in S_n} Fix(\sigma) = 1$. Also, $\rho_{st} = \mathbb{1} \oplus \rho'_{st}$ where both $\mathbb{1}$ and ρ'_{st} are irreducible, then we have*

$$\frac{1}{n!} \sum_{\sigma \in S_n} Fix(\sigma)^2 = \frac{1}{n!} \sum_{\sigma \in S_n} \chi_{st}(\sigma)\chi_{st}(\sigma^{-1}) = \langle \chi_{st}, \chi_{st} \rangle = 2.$$

2. Suppose $G = S_3$. Then the three characters χ_1, χ_2, χ_3 are 1, 1 and 2, respectively with $\rho_i : G \to F^\times$. In particular, G is generated by σ and τ where $\sigma^3 = 1$, $\tau^2 = 1$ and $\tau\sigma\tau = \sigma^{-1}$. Therefore we have

	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
$\chi_1 = \mathbb{1}$	1	1	1	1	1	1
χ_2	1	1	1	-1	-1	-1
χ_3	2	-1	-1	0	0	0
χ_{st}	3	0	0	1	1	1

Figure 8.2: Character Table of S_3

Note $\chi_{reg} = \sum_i d_i\chi_i$ with $\sum_i d_i\chi(\varepsilon) = \begin{cases} |G|, & \varepsilon = 1 \\ 0, & \varepsilon \neq 1 \end{cases}$. Because $\chi_{st}(\varepsilon) = Fix(\varepsilon)$, we have $\chi_{st} = \chi_1 + \chi_3$, hence $\rho_{st} = \mathbb{1} \oplus \rho'_{st}$.

3. Suppose $G = Q_8$, then the five characters $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5$ are 1, 1, 1, 1 and 2, respectively with $\rho_i : G \to F^\times$. Note that Q_8 is generated with i, j such that $i^2 = \varepsilon = j^2$, $ji = \varepsilon ij$, $\varepsilon i = i\varepsilon$ and $\varepsilon j = j\varepsilon$. We have the following character table:

	1	i	j	ij	ε	εi	εj	εij
χ_1	1	1	1	1	1	1	1	1
χ_2	1	-1	1	-1	1	-1	1	-1
χ_3	1	1	-1	-1	1	1	-1	-1
χ_4	1	-1	-1	1	1	-1	-1	1
χ_5	2	0	0	0	-2	0	0	0

Figure 8.3: Character Table of Q_8

Note that there is the canonical decomposition

$$Q_8 \longrightarrow Q_8/\langle\varepsilon\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow F^\times$$

Therefore we have the map from $G \to GL_2(F)$ given by $i \mapsto \begin{pmatrix} \sqrt[4]{-1} & 0 \\ 0 & -\sqrt[4]{1} \end{pmatrix}$, $j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\varepsilon \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Recall $\mathbb{Q}[Q_8] = F \times F \times F \times F \times \mathbb{H}$ with dimensions 1, 1, 1, 1 and 4, respectively.

8.6 Hurwitz Theorem

Recall in $\mathbb{C}$ we have the norm as a function $N(x+yi) = (x+yi)(x-yi) = x^2+y^2$, and it is multiplicative that $N(z_1z_2) = N(z_1)N(z_2)$. Similarly, in $\mathbb{H}$, for $q = x_1+x_2i+x_3j+x_4ij$, we have $N(q) = x_1^2+x_2^2+x_3^2+x_4^2 = q \cdot \bar{q}$, where $\bar{q} = x_1 - x_2i - x_3j - x_4ij$.

Similarly, $(x_1^2+x_2^2+x_3^2+x_4)^2(y_1^2+y_2^2+y_3^2+y_4^2) = f_1^2+f_2^2+f_3^2+f_4$ where $f_i \in \mathbb{Z}[x,y]$.

A more common form of such case is the Cayley Algebra (Octonion Algebra), which is non-associative with N mapping an element to $\sum\limits_{i=1}^{8} x_i^2$. Informally, Hurwitz theorem states that such formula only works when $n = 1, 2, 4, 8$.

Theorem 8.6.1 (Hurwitz). *If there are $f_1, \cdots, f_n \in \mathbb{C}[x_1, \cdots, x_n, y_1, \cdots, y_n]$ such that*

$$(\sum_{i=1}^{n} x_i) \cdot (\sum_{i=1}^{n} y_i) = \sum_{i=1}^{n} f_i^2,$$

then $n = 1, 2, 4$ or 8.

In other words, the only Euclidean Hurwitz algebras are the real numbers, the complex numbers, the quaterions and the octonians.

Proof. Denote $f_i = \sum\limits_j a_{ij}(x) \cdot y_j$, where $a_{ij}(x)$ are linear homogeneous in x. Then

$$\begin{aligned}\sum_i f_i^2 &= \sum_i \sum_j a_{ij}(x)^2 y_j^2 + 2\sum_i \sum_{j<k} a_{ij}(x) \cdot a_{ik}(x) \cdot y_j y_k \\ &= (\sum_i x_i^2)(\sum_i y_i^2).\end{aligned}$$

For all j, $\sum\limits_i a_{ij}(x)^2 = \sum\limits_i x_i^2$, and $\sum\limits_i a_{ij}(x) \cdot a_{ik}(x) = 0$ for all $j \neq k$.

Take $A = A(x) = (a_{ij}(x))$, an $n \times n$ matrix of homogeneous linear polynomials. Then

$$A_t \cdot A = (\sum_i x_i^2) \cdot I_n,$$

equivalent to the original matrix.

We now write $A = \sum\limits_i A_i x_i$, where A_i is an $n \times n$ matrix over $\mathbb{C}$:

$$(\sum_i A_i^t \cdot x_i)(\sum_j A_j x_j) = (\sum_i x_i^2) \cdot I_n.$$

Note $A_i^t \cdot A_i = I_n$, with $A_i^t \cdot A_j + A_j^t \cdot A_i = 0$ for all $i \neq j$. Denote $B_i = A_n^t \cdot A_i$ for $i = 1, \cdots, n-1$, then $B_i^t = A_n^t \cdot A_n = -A_n^t \cdot A_i = -B_i$, which shows a skew-symmetry property. Moreover, $B_i^2 = A_n^t A_i A_n^t A_i = -A_i^t A_n A_n^t A_i = A_i^t A_i = I$. For $i \neq j$, we have

$$\begin{aligned}B_i B_j + B_j B_i &= A_n^t A_i A_n^t A_j + A_n^t A_j A_n A_i \\ &= -A_i^t A_j - A_j^t A_i \\ &= 0.\end{aligned}$$

Overall, the $n \times n$ matrices B_i over $\mathbb{C}$ for $i = 1, \cdots, n-1$ satisfies

- $B_i^2 = -1$.
- $B_i B_j = -B_j B_i$, $i \neq j$.

Therefore, this now looks more like a representation of a group.

Let G be a group generated by $a_1, \cdots, a_{n-1}, \varepsilon$ with relations:

- $a_i^2 = \varepsilon$.

- $a_j a_i = \varepsilon a_i a_j$ for all $i \neq j$.
- $\varepsilon^2 = 1$.
- $\varepsilon a_i = a_i \varepsilon$.

This is called the generalized quaternion group. Note that every $g \in G$ has the form $g = \varepsilon^s \cdot a_1^{t_1} \cdots a_{n-1}^{t_{n-1}}$, where $s, t_1, t_2, \cdots, t_{n-1}$ are 0 and 1. Then $|G| = 2^n$, and $[G, G] = \langle \varepsilon \rangle$.

In particular, we have $a_i \mapsto B_i$ with $\varepsilon \mapsto -I$, which is an n-dimensional representation of G. □

Now observe that $\rho : G \to \mathrm{GL}(V)$ irreducible, with $F[G] \to \mathbf{End}(V)$. Note that there is a generated map $Z(F[G]) \to \mathbf{End}_{F[G]}(V) = F$, by having the center acting by scalar multiplication.

Proposition 8.6.2. *Let $C(g)$ be the conjugacy classes of $g \in G$, and let ρ be an irreducible representation of G of dimension d. Denote $\chi = \chi_\rho$. Then $\frac{1}{d}|C(g)|\chi(g)$ is an algebraic integer (we can assume $F = \mathbb{C}$).*

Proof. Take $g \in G$. Let $x = \sum\limits_{h \in C(g)} h \in Z(F[G])$. Let $f : Z(F[G]) \to F$ and $\rho : F[G] \to \mathbf{End}(V)$ as above. Let $\alpha = f(x)$, then $\rho(x)$ is a diagonal matrix where every entry is α. Then we denote $d\alpha = \mathrm{Tr}(\rho(x)) = \chi(x) = \sum\limits_{h \in C(g)} \chi(h) = |C(g)|\chi(g)$. Therefore, character is invariant under conjugation. Hence, we have

$$\frac{|C(g)|\chi(g)}{d} = \alpha.$$

Note x has integral coefficients, so $x \in Z(\mathbb{Z}[G])$. Therefore is now an induced map $\bar{f} : Z(\mathbb{Z}[G]) \to \mathbb{C}$, and $\alpha \in \mathrm{im}(\bar{f}) \subseteq \mathbb{C}$, and $\mathrm{im}(\bar{f})$ is a finitely generated subring.

Therefore, $\mathbb{Z}[\alpha]$ is a faithful $\mathbb{Z}[\alpha]$-module, finitely generated subring of $\mathbb{C}$. Therefore, α is an algebraic integer. □

Theorem 8.6.3. *Let d be the dimension of an irreducible representation of G over $\mathbb{C}$. Then $d \mid |G|$.*

Proof. Let $n = |G|$ and let χ be the character. Then we know

$$1 = \langle \chi, \chi \rangle = \frac{1}{n} \sum_{g \in G} \chi(g^{-1})\chi(g).$$

Let $G = C(g_1) \sqcup C(g_2) \sqcup \cdots \sqcup C(g_r)$ be the conjugacy classes. Then we have

$$1 = \frac{1}{n} \sum_{i=1}^{r} |C(g_i)| \chi(g_i^{-1}) \chi(g_i).$$

Hence, $\frac{n}{d} = \sum\limits_{i=1}^{r} \frac{|C(g_i)|}{d} \chi(g_i)\chi(g_i^{-1})$, where g_i and g_i^{-1} are both algebraic integers. Therefore, $\frac{n}{d}$ is also an algebraic integer, so $d \mid n$. □

Now suppose $F \subseteq K$ and both are algebraically closed with characteristic 0. Now for every representation $\rho L : G \to \mathrm{GL}_n(F)$, we can compose $G \to \mathrm{GL}_n(F) \hookrightarrow \mathrm{GL}_n(K)$. As a functor, we know $\mathrm{Rep}_F(G) \to \mathrm{Rep}_K(G)$ by $M \mapsto K \otimes_F M$. We then have $K[G] \cong K \otimes_F F[G]$.

Claim 8.6.4. *ρ is irreducible if and only if ρ_K is irreducible.*

Proof. Note $\chi_\rho = \chi_{\rho_K}$ and irreducible if and only if $\langle \chi, \chi \rangle = 1$. This is true in algebraically closed fields with characteristic 0. □

Also note that $\dim(\rho) = \dim(\rho_K)$. Therefore, irreducible representations over K are exactly those obtained from irreducible representations over F.

For F algebraically closed and characteristic 0, we have a one-to-one correspondence between irreducible representations, so it suffices to prove for $\mathbb{C}$ only.

$$\begin{tikzcd}
F \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{C} \arrow[dl, dash] \\
& \mathbb{Q}_{alg} &
\end{tikzcd}$$

8.7 Tensor Product of Representations

Definition 8.7.1 (Tensor Product of Representation)**.** *Suppose $\rho_1 : G_1 \to GL(V)$ and $\rho_2 : G_2 \to GL(W)$, then $V \otimes W$ is a $G_1 \times G_2$-space by $(g_1, g_2)(v \otimes w) = g_1 v \otimes g_2 w$. This is well-defined because the left hand side is a bilinear map. This is the tensor product of representations $\rho_1 \otimes \rho_2$. Furthermore, we have* $\dim(\rho_1 \otimes \rho_2) = \dim(\rho_1) \cdot \dim(\rho_2)$*. If $\{x_1, \cdots, x_m\}$ is a basis for V and $\{y_1, \cdots, y_n\}$ is a basis for W, then $\{x_i \otimes y_i\}_{i,j}$ is a basis for $V \otimes W$.*

Let $g_1 \in G$ and $g_2 \in G_2$, and let $\rho_1(g_1)(x_i) = \cdots + a_i x_i + \cdots$ and $\rho_2(g_2)(y_j) = \cdots + b_j y_j + \cdots$, so $(\rho_1 \otimes \rho_2)(g_1, g_2)(x_i \otimes y_j) = \cdots + a_i b_j (x_i \otimes y_j) + \cdots$.

In particular, we know

$$\chi_{\rho_1\otimes\rho_2}=\sum_{i=1}^{m}\sum_{j=1}^{n}a_ib_j=(\sum_{i=1}^{m}a_i)(\sum_{j=1}^{n}b_j)=\chi_{\rho_1}\cdot\chi_{\rho_2}.$$

Let $\rho_i, \mu_i u$ be the representations of G_i for $i = 1, 2$. Therefore, we have

$$\begin{aligned}\langle\rho_1\otimes\rho_2,\mu_1\otimes\mu_2\rangle &= \frac{1}{|G_1||G_2|}\sum_{g_1\in G_1}\sum_{g_2\in G_2}\chi_{\rho_1\otimes\rho_2}(g_1g_2)\chi_{\mu_1\otimes\mu_2}(g_1^{-1}g_2^{-1})\\ &= \frac{1}{|G_1||G_2|}\sum_{g_1\in G_1}\sum_{g_2\in G_2}\chi_{\rho_1}(g_1)\chi_{\rho_2}(g_2)\chi_{\mu_1}(g_1^{-1})\chi_{\mu_2}(g_2^{-1})\\ &= \langle\rho_1,\mu_1\rangle\langle\rho_2,\mu_2\rangle.\end{aligned}$$

Hence, if ρ_1, ρ_2 are irreducible, so is $\rho_1 \otimes \rho_2$.

Claim 8.7.2. *Let $\rho_i^{(1)}, \cdots, \rho_i^{(r_i)}$ be all the irreducible representations of G_i for $i = 1, 2$. Then $\{\rho_1^{(i)} \otimes \rho_2^{(j)}\}_{i,j}$ are all the irreducible representations of $G_1 \times G_2$.*

Proof. Look at the number of conjugacy classes or sum of square of dimensions. □

Note that this only works for algebraically closed field with characteristic 0.

Now suppose we have the map $H \xrightarrow{f} G \to \mathrm{GL}(V)$, then f gives a functor $\mathrm{Rep}(G) \xrightarrow{f^*} \mathrm{Rep}(H)$. In particular, if $H < G$, then f is the restriction functor. However, the restriction functor does not preserve irreducibility.

If $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$, then we have a map $\rho_1 \otimes \rho_2 : G \times G \to \mathrm{GL}(V_1 \otimes V_2)$. We can now restrict to the diagonal functor

$$G \xhookrightarrow{\Delta} G_1 \times G_2.$$

This is also called tensor product of $\rho_1 \otimes \rho_2$. Note that this "tensor product" may not preserve irreducibility as well.

Now $\oplus$ and $\otimes$ are operations that make $\mathrm{Rep}(G)$ a tensor category. The set of isomorphisms of $\mathrm{Rep}(G)$ is a ring with the two operations. This gives a free Abelian group with basis irreducible representations.

Definition 8.7.3 (Representation Ring)**.** *Let G be a finite group and let $\rho_1, \cdots, \rho_r$ irreducible representations. We now define*

$$R(G) = \{\sum_{i=1}^{r} a_i p_i, a_i \in \mathbb{Z}\}$$

as the free Abelian group generated by $[\rho_1], \cdots, \rho_r]$. *Note that* $R(G)$ *is a ring: note* $\rho_i \otimes \rho_j = \coprod_{k=1}^{r} \rho_k^{\oplus b_k}$ *and set* $[\rho_i][\rho_j] = \sum_{k=1}^{r} b_k \rho_k = [\rho_i \otimes \rho_j]$.

We can check $[\varepsilon] \cdot [\mu] = [\varepsilon \otimes \mu]$ *for all representations. Therefore, the multiplication operation is associative. The identity is given by* $[\mathbb{1}]$, *and* $R(G)$ *is called the representation ring.*

Without using irreducible representations, another way to define $R(G)$ is using generators and relations. The generators are given by isomorphism classes of all (finite-dimensional) representations. The relations are given by the generators commuting, with $[\varepsilon \oplus \mu] = [\varepsilon] + [\mu]$. Then $[\varepsilon] = [\coprod_{i=1}^{r} b_i \rho_i] = \sum_{i=1}^{r} b_i [\rho_i]$. This agrees with $R(G)$ above. One needs to show that $[\rho_1], \cdots, [\rho_i]$ are linearly independent.

Definition 8.7.4 (Grothendieck Group/Ring)**.** *In general,* $R(G)$ *can be defined for any category with direct sum/tensor product. This is called the Grothendieck group/ring.*

Now let A be the set of isomorphism classes of representations, then A is actually a monoid with respect to $\oplus$. Consider $A^+ = A \times A / \sim$ where $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1 \oplus y_2) = y_1 \oplus x_2$. Then this is a group with component-wise addition. In particular, we have $(x, y)^{-1} = (y, x)$ since $(x, y) + (y, x) = (x \oplus y, y \oplus x) \sim (0, 0)$. In general, this is a functor that is the left adjoint of the forgetful functor:

Consider A in **CMon** and G in **Ab**. Now any map $f : A \to G$ is corresponding to the map $A^+ \to G$ by setting $(x, y) \mapsto f(x) - f(y)$, then we have $\mathbf{Hom}_{\mathbf{CMon}}(A, G) = \mathbf{Hom}_{\mathbf{Ab}}(A^+, G)$. We can then define $R(G) = A^+$.

Recall that $\mathrm{Ch}(G) = \{f : G \to F, f(ghg^{-1}) = f(h)\}$ is a vector space. Now $R(G)$ is the subgroup of $\mathrm{Ch}(G)$ generated by χ_ρ for all representations ρ, which is essentially the same as the free Abelian subgroup generated by all irreducible characters $\chi_1, \cdots, \chi_\rho$. The product in $R(G)$ is the usual product in F, given by $\chi_{\rho \oplus \mu} = \chi_\rho \cdot \chi_\mu$. This is convenient for computation.

Example 8.7.5. *Suppose* G *is a finite Abelian group. Then* $G^* = \mathbf{Hom}(G, F^\times)$ *are all irreducible characters/representations, with* $R(G) = \mathbb{Z}[G^*]$. *Then* G^* *is called the character group, with* $G^* \cong G$ *as a non-canonical isomorphism.*

Example 8.7.6. *Recall* $G = S_3 = \langle \sigma, \tau : \sigma^3 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$. *We also had the character table*

	1	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
$\chi_1 = \mathbb{1}$	1	1	1	1	1	1
χ_2	1	1	1	-1	-1	-1
χ_3	2	-1	-1	0	0	0

As a group, $R[G] = \mathbb{Z} \cdot \mathbb{1} \oplus \mathbb{Z} \cdot x \oplus \mathbb{Z} \cdot y$. As a ring, we know $\mathbb{1}$ is the identity, and $x^2 = \mathbb{1}$, $xy = yx = y$, with $y^2 = \mathbb{1} + x + y$. Therefore,

$$R(G) \cong \mathbb{Z}[X,Y]/(X^2 - 1, XY - Y, Y^2 - Y - X - 1).$$

Theorem 8.7.7. *Let G be a finite group and ρ is a irreducible representation, set $d = \dim(\rho)$, then $d \mid [G : Z(G)]$. Recall we have shown that $d \mid |G|$.*

Proof. Denote $\rho : G \to \mathrm{GL}(V)$ with $\dim(V) = d$. Consider $\rho^{\otimes m} : G^m \to \mathrm{GL}(V^{\otimes m})$, then $\dim(\rho^{\otimes m}) = d^m$. Let $S \subseteq G^m$ by $S = \{(g_1, \cdots, g_m) \in Z(G), g_1 \cdots g_m = 1\}$. Then S is a normal subgroup, with $|S| = |Z(G)|^{m-1}$. Now ρ is irreducible, so for all $g \in Z(G)$, there exists $\alpha \in F$ such that $gv = \alpha v$ for all $v \in V$.

Consider $(g_1, \cdots, g_m)(v_1 \otimes \cdots \otimes v_m) = (\alpha_1 v_1) \otimes \cdots \otimes (\alpha_m v_m) = (\alpha_1 \cdots \alpha_m)(v_1 \otimes \cdots \otimes v_m)$. Note that if $gv = \alpha v$ and $hv = \beta v$, then $(gh)v = \alpha\beta v$.

We have $\alpha_1 \alpha_2 \cdots \alpha_n = 1$ since $g_1 \cdots g_m = 1$. Hence, S acts on $V^{\otimes m}$ by identity, so $\rho^{\otimes m}(s) = I$. Therefore, $S \subseteq \ker(\rho)$. Then $\rho : G^m/S \to \mathrm{GL}(V^{\otimes m}$. Note $\rho^{\otimes m} : G^m \to \mathrm{GL}$ is still irreducible. Then $d^m \mid [G^m : S] = |G|^m/|Z(G)|^{m-1}$ for all m. Therefore, we have $d \mid |G|/|Z(G)|$. □

Theorem 8.7.8 (Burnside's pq-Theorem)**.** *Let p and q be prime integers. Every group of order $p^a q^b$ is solvable for all $a, b \in \mathbb{Z}_{\geq 0}$.*

We would develop the proof for the theorem gradually.

Lemma 8.7.9. *Let G be a finite group and ρ is an irreducible representation over $\mathbb{C}$ of dimension d. Denote $\chi = \chi_\rho$. Let $C \subseteq G$ be a conjugacy class such that $\gcd(|C|, d) = 1$. Then every element $g \in C$ either satisfies $\chi(g) = 0$ or $\rho(g)$ is a scalar matrix.*

Proof. Suppose $a|c| + bd = 1$ with $a, b \in \mathbb{Z}$, then

$$a\frac{|c|\chi(g)}{d} + b\chi(g) = \frac{\chi(g)}{d}$$

where $\chi(g)$ and $\frac{|c|\chi(g)}{d}$ are algebraic integers. Therefore, $\frac{\chi(g)}{d}$ is an algebraic integer. Also, $|\chi(g)| \leq d$ and if $|\chi(g)| = d$ then $\rho(g)$ is a scalar matrix.

Suppose $\alpha = \frac{\chi(g)}{d}$ with $\alpha < 1$. Let $n = |G|$. Let $\Gamma = \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$. Write $\chi(g) = \chi_1 + \cdots + \chi_d$ for $\chi_1, \cdots, \chi_d \in \mu_n$, the set of primitive n-th root of unity. For all $\gamma \in \Gamma$, we have $\gamma\chi(g) = \gamma\chi_1 + \cdots + \gamma\chi_d$. Hence, we know $|\gamma\chi(g)| \leq |\gamma\chi_1| + \cdots + |\gamma\chi_d| = d$. Therefore,

$$|\gamma\alpha| = |\frac{\gamma\chi(g)}{d}| \leq 1.$$

Now $c = \prod_{\gamma\in\Gamma} \gamma\alpha \in \mathbb{Q}(\xi_n)^\tau = \mathbb{Q}$, where $\mathbb{Q}(\xi_n)^\tau$ is the set of fixed points of the Galois group. Moreover, we know $|c| = \prod_{\gamma\in\Gamma} |\gamma\alpha| < 1$, where $|\gamma\alpha| < 1$ when $\gamma = \mathbf{id}$. But c is also an algebraic integer, so $c = 0$. Therefore, $\alpha = 0$, and so $\chi(g) = 0$. □

Proposition 8.7.10. *Suppose $C \subsetneq G$ is a conjugacy class, and $|C| = p^a > 1$ for prime p. Then G is not simple.*

Proof. Suppose G is simple. Let $\rho_1, \cdots, \rho_r$ be irreducible representations of G. Let $\chi_1, \cdots, \chi_r$ be their characters. Let $d_1, \cdots, d_r$ be their dimensions. Also set $\rho_1 = \mathbb{1}$.

Claim 8.7.11. *If $p \nmid d_i$ for some $i > 1$, then $\chi_i(g) = 0$ for all $g \in C$.*

Subproof. Set $H = \{g \in G : \rho_i(g) \text{ is a scalar matrix}\}$, then $H \lhd G$. Note $\ker(\rho_i) \lhd G$ and $\ker(\rho_i) \neq G$ since $\rho_i \neq \mathbb{1}$ for G simple. Therefore, ρ_i is injective. ■

If $G = H$, then $G \cong \mathrm{im}(\rho_i)$ is Abelian, contradiction. Therefore, $H = \{e\}$. Also $e \notin C$ since $|C| > 1$. Then $\chi(g) = 0$ for all $g \in C$ by lemma.

Now note that $\chi_{reg} = \sum_{i=1}^{r} d_i\chi_i$ for all $g \in C$, and $0 = \chi_{reg}(g) = 1 + \sum_{i=2}^{r} d_i\chi_i(g)$ because $g \neq e$. Hence,

$$-\frac{1}{p} = \sum_{i=2}^{r} \frac{d_i\chi_i(g)}{p}.$$

If $p \mid d_i$, then $\frac{d_i\chi_i(g)}{p}$ is an algebraic integer. If $p \nmid d_i$, then $\chi_i(g) = 0$. Therefore, $-\frac{1}{p}$ is an algebraic integer, contradiction. □

We now prove the Burnside Theorem above.

Proof. Assume $p \neq q$ and $a, b > 0$. Otherwise the case is known. Let $|G| = p^a q^b$. It suffices to show G is not simple by induction.

Let $Q < G$ be a Sylow q-subgroup. Then $[G : Q] = p^a$ with $Q \neq 1$. Let $g \in Z(Q)$ be non-trivial, and note non-trivial q-groups have non-trivial center. Then let H be the centralizer of g in G, then $Q < H < G$, so $[G : H] = p^r$ for some $r \geq 0$. Let $C \subseteq G$ be the conjugacy class of g in G. Then $|C| = \frac{|G|}{|H|} = p^r$. Note that G acts on C by conjugation by the orbit-stabilizer theorem.

If $|C| = 1$, then $g \in Z(G)$, so $\langle g \rangle \lhd G$. Then either G has a proper non-trivial subgroup $\langle g \rangle$ or G is cyclic, therefore G is solvable. (Actually for $g \in Q$ we know the order of g is q^s, then $\langle g \rangle \neq G$. If $|C| > 1$, then G is not simple by proposition. □

8.8 Simple Algebra

Fix a field F and let A be an F-algebra. Denote A as a ring and a vector space over F with compatible operations. There is a ring homomorphism $F \to Z(A)$ if $A \neq 0$ by sending $x \mapsto x \cdot 1$. This map is injective since F is a field. Then we can identify F as a subfield of $Z(A)$.

Let A, B be F-algebras, then $A \otimes_F B$ is also an F-algebra by $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 b_1 \otimes a_2 b_2$.

Property 8.8.1. *1.* $\dim_F(A \otimes_F B) = \dim_F(A)\dim_F(B)$.

2. *Let $(a_i)_{i \in I}$ be a basis of A. Then every element of $A \otimes_F B$ can be uniquely written as $\sum\limits_i a_i \otimes b_i$ for $b_i \in B$. This also works for B because of symmetry argument.*

3. *$F \otimes_F A \cong A \cong A \otimes_F F$ canonically.*

4. *$A \otimes_F B \cong B \otimes_F A$ canonically.*

5. *$(A \otimes_F B) \otimes_F C \cong A \otimes_F (B \otimes_F C)$ canonically.*

6. *The set of all $n \times n$ matrices $M_n(F)$ is an F-algebra. For all F-algebra A, we have $M_n(F) \otimes_F A \cong M_n(A)$.*

7. *$M_n(F) \otimes_F M_m(F) \cong M_{mn}(F)$. This is true by viewing it as $\mathbf{End}(V) \otimes F \mathbf{End}(W) \xrightarrow{\sim} \mathbf{End}(V \otimes_F W)$ by "$\alpha \otimes \beta \mapsto \alpha \otimes \beta$". Note $\dim(\mathbf{End}(V)) = m$, $\dim(\mathbf{End}(W)) = n$ and $\dim(\mathbf{End}(V \otimes_F W)) = mn$.*

We now focus on simple algebra of finite dimensions. Recall the following proposition:

Proposition 8.8.2. *Let A be an F-algebra and $\dim_F(A) < \infty$. The following are then equivalent:*

1. *A is simple.*

2. *$A \neq 0$, A is semisimple and has only one simple A-algebra.*

3. *$A \cong M_n(D)$ for D a division F-algebra.*

Note that here $D = \mathbf{End}_A(M)$ where M is a (unique) simple left A-module.

Remark 8.8.3. *Note that there is the map*

$$\begin{aligned} F &\subseteq Z(A) \\ x &\mapsto x \cdot 1. \end{aligned}$$

One can prove that $Z(A)$ is a field, and we can view A as a $Z(A)$-algebra.

Definition 8.8.4 (Simple Algebra)**.** *An F-algebra A is simple if $Z(A) = F$.*

Remark 8.8.5. *Every F-algebra is simple over $Z(A)$.*

Definition 8.8.6 (Central Algebra)**.** *An F-algebra A is called a central simple algebra over F if A is simple and $Z(A) = F$.*

Example 8.8.7. *Note $M_n(F) \supseteq F$ is central.*

Definition 8.8.8 (Centralizer)**.** *Suppose $S \subseteq A$ is a subalgebra, the centralizer is $C_A(S) = \{x \in A : xs = sx \forall s \in S\} \subseteq A$.*

Remark 8.8.9. *$C_A(F) = A$ and $C_A(A) = Z(A)$.*

Remark 8.8.10. *We can view A and B as subalgebras of $A \otimes_F B$ by sending $a \mapsto a \otimes 1$ and $b \mapsto 1 \otimes b$.*

Denote $a = \sum_i \alpha_i a_i$ where $(a_i)_i$ forms a basis for a. We can also write $(b_j)_j$ as a basis for B with $b_1 = 1$ without loss of generality. Therefore, there is the mapping $a_i \mapsto a_i \otimes b_1$. Note that $(a_i \otimes b_j)$ forms a basis for $A \otimes_F B$.

Therefore, there is the relation

$$(a \otimes 1)(1 \otimes b) = a \otimes b = (1 \otimes b)(a \otimes 1).$$

Consider $S \subseteq A$ and $T \subseteq B$ as subalgebras. Then we have $C_A(S) \subseteq A$ and $C_B(T) \subseteq B$, which means $C_A(S) \otimes C_B(T) \subseteq A \otimes B$. We also know that $S \otimes T \subseteq A \otimes B$ and therefore $C_{A \otimes B}(S \otimes T) \subseteq A \otimes B$. A obvious question is the relation between these two structures.

Proposition 8.8.11. *$C_{A\otimes B}(S\otimes T)=C_A(S)\otimes C_B(T)$.*

Proof. The $\supseteq$ direction is obvious. We prove the other one.

Let $(a_i)_i$ be a basis of A, then $C_{A\otimes B}(S\otimes T)\supseteq\sum a_i\otimes b_i=u$ for $b_i\in B$. For $t\in T$, because $1\otimes t\subseteq S\otimes T$, then we have $(\sum_i a_i\otimes b_i)(1\otimes t)=(1\otimes t)\sum_i(a_i\otimes b_i)$, and so we get $\sum_i a_i\otimes b_it=\sum_i a_itb_i$.

Hence, $\sum a_i\otimes(b_it-tb_i)=0$. Therefore $b_it-tb_i=0$ for all t and all i, then $b_i\in Z_B(T)$ must be true.

Now, there is a basis (b_i) of $C_B(T)$ such that $u=\sum a_i\otimes b_i$ for some $a_i\in A$. Take $s\in S$, then

$$(\sum_i a_i\otimes b_i)(s\otimes 1)=(s\otimes 1)(\sum a_i\otimes b_i).$$

Therefore, $\sum a_is\otimes b_i=\sum sa_i\otimes b_i$, and so $\sum(a_is-sa_i)\otimes b_i=0$. Therefore, $a_is-sa_i=0$ for all $s\in S$ and all i. Hence, $a_i\in C_A(S)$ and so $u\in C_A(S)\otimes C_B(T)$. □

Corollary 8.8.12. *$Z(A\otimes_F B)=Z(A)\otimes_F Z(B)$.*

Corollary 8.8.13. *If A and B are central algebras, so is $A\otimes_F B$.*

Example 8.8.14. *Let L/F be a finite field extension. Then L is a simple F-algebra. There is a map $f:L\otimes L\to L$ that sends $x\otimes y\mapsto xy$ and this is a homomorphism with $xx'\otimes yy'\mapsto xx'yy'$ by taking $x\otimes y\mapsto xy$ and $x'\otimes y'\mapsto x'y'$. Moreover, this is a surjective algebra homomorphism. Let $I=\ker(f)$, then $\dim(I)=n^2-n>0$ for $n=[L:F]>1$. Therefore, I is a proper two-sided ideal in $L\otimes_F L$, and so $L\otimes_F L$ is not simple.*

Proposition 8.8.15. *Let A and B be simple F-algebras and A is central. Then $A\otimes_F B$ is simple.*

Proof. Let $0\neq I\subseteq A\otimes_F B$ be a two-sided ideal. Take $0\neq u\in I$. Then $u=\sum_{i=1}^n a_i\otimes b_i$ for b_i linearly independent in B and n is the smallest possible.

For $a_1\neq 0$, $Aa_1A\subseteq A$ is a two-sided ideal. Because A is simple, then $Aa_1A=A$. Therefore, there is $1=\sum_j x_ja_iy_j$ for $x_j,y_j\in A$. Then $I\ni\sum_j(x_j\otimes 1)u(y_j\otimes 1)=\sum_{i,j}x_ja_iy_j\otimes b_i=\sum_i(\sum_j x_ja_iy_j)\otimes b_i=1\otimes b_1+a_2'\otimes b_2+\cdots+a_n'\otimes b_n$ because $\sum_j x_ja_iy_j=1$ if $i=1$. We now set $v=1\otimes b_1+a_2'\otimes b_2+\cdots+a_n'\otimes b_n$.

For $a\in A$, $I\ni(a\otimes 1)v-v(a\otimes 1)=\sum_{i=2}^n(aa_i'-a_i'a)\otimes b_i=0$, and so $aa_i'=a_i'a$ for all $a\in A$ and all $i>1$. Then $a_i'\in Z(A)=F$.

We now have $0 \neq v = 1 \otimes b_1 + a_2' \otimes b_2 + \cdots + a_n' \otimes b_n = 1 \otimes b$ by linear independence. Then $b \neq 0$, and so $BbB = B$ since B is simple. Hence, $1 = \sum_j s_j t b_j$ for $s_j, t_j \in B$. Therefore, $I \ni \sum_j (1 \otimes s_j) v (1 \otimes t_j) = 1 \otimes \sum_j s_j b t_j = 1 \otimes 1 = 1_{A \otimes B}$. □

Corollary 8.8.16. *If A and B are central simple algebras, then so is $A \otimes B$.*

Note $F \otimes_F A = A$. This gives a monoidal structure of algebra. If we factor out central simple algebra by some equivalence relation, we get a group, namely the Brauer group.

8.9 Brauer Group

Consider a central simple (finite-dimensional) F-algebra for a fixed field F. We define the equivalence relation $A \sim B$ to be that $M_n(A) \cong M_m(B)$ for some m, n. This relation is indeed an equivalence relation, with reflexivity and symmetry clear. The transitivity follows from that if $M_n(A) \cong M_m(B)$ and $M_k(B) \cong M_s(C)$, then by tensoring the equations on the right with $M_k(F)$ and $M_m(F)$ respectively, we have $M_{nk}(A) \cong M_{mk}(B) \cong M_{ms}(C)$. Therefore, this is an equivalence relation indeed.

Proposition 8.9.1. *Let $A_1 = M_{n_1}(D_1)$ and $A_2 = M_{n_2}(D_2)$ be two central simple F-algebras with D_1, D_2 division F-algebras. Then $A_1 \sim A_2$ if and only if $D_1 \cong D_2$.*

Proof. If $A_1 \sim A_2$, then $M_{s_1}(A_1) \cong M_{s_2}(A_2)$, so $M_{s_1 n_1}(D_1) \cong M_{s_2 n_2}(D_2)$, hence $D_1 \cong D_2$. Conversely, $M_{n_2}(A_1) \cong M_{n_1 n_2}(D_1) \cong M_{n_1 n_2}(D_2) \cong M_{n_1}(A_2)$, hence $A_1 \sim A_2$. □

Therefore, the class $[A]$ of $A = M_n(D)$ is $\{M_i(D)\}$ for $i \geq 1$. In particular, $D \in [A]$, so we have a correspondence between equivalence classes and central division F-algebras.

Write $\mathrm{Br}(F)$ for the set of equivalence classes with operation $[A][B] = [A \otimes_F B]$. The operation is well-defined: if $A_1 \sim A_2$, i.e. $M_{s_1}(A_1) \cong M_{s_2}(A_2)$ and $B_1 \sim B_2$, i.e. $M_{t_1}(B_1) \cong M_{t_2}(B_2)$, then

$$M_{s_1 t_1}(A_1 \otimes_F B_1) \cong M_{s_1}(A_1) \otimes_F M_{t_1}(B_1) \cong M_{s_2}(A_2) \otimes_F M_{t_2}(B_2) \cong M_{s_2 t_2}(A_2 \otimes_F B_2),$$

i.e. $A_1 \otimes_F B_1 \sim A_2 \otimes_F B_2$.

Theorem 8.9.2. *The set $Br(F)$ is an Abelian group.*

Proof. The operation is obviously commutative and associative. The class $[F]$ is the identity. Let A be a central simple algebra of finite dimension over F. We show that

$[A]^{-1} = [A^{\mathrm{op}}]$. Consider a map

$$\begin{aligned} f : A \otimes_F A^{\mathrm{op}} &\to \mathrm{End}_F(A) \\ f(x \otimes y^{\mathrm{op}})(a) &= xay. \end{aligned}$$

This is a homomorphism of simple F-algebras of the same dimension, hence f is an isomorphism. It follows that $[A][A^{\mathrm{op}}] = [\mathrm{End}_F(A)] = [F] = 1$. □

Definition 8.9.3 (Brauer Group)**.** *The Abelian group Br(F) is the Brauer group of F.*

Remark 8.9.4. *Every class $[A]$ in Br(F) contains a central division algebra that is unique up to isomorphism. Thus, we have a bijection between the set Br(F) and the set of isomorphism classes of central division F-algebras of finite dimension.*

Note that Br$(F) = 1$ if and only if every central division F-algebra of finite dimension is F.

Example 8.9.5. *If F is algebraically closed, then Br$(F) = 1$.*

Theorem 8.9.6. *If F is a finite field, then Br$(F) = 1$.*

Proof. Let $F = \mathbb{F}_q$ and let A be a central division F-algebra of finite dimension. We show that $A = F$.

Suppose $\dim_F(A) = n$, so $|A| = q^n$. Hence $|A^\times| = q^n - 1$. For any $a \in A$ non-zero, the centralizer $C_A(a) \subseteq A$ is a subspace, so $|C_A(a)| = q^k$ for some k, hence $|C_{A^\times}(a)| = q^k - 1$. Note that k divide n as $\frac{n}{k}$ is the rank of A as a module over the division algebra $C_A(a)$. Therefore, the conjugacy class of a in $A^\times$ has $\frac{q^n-1}{q^k-1}$ elements. The elements of $Z(A)^\times = F^\times$ have conjugacy classes of size 1, so there are exactly $q-1$ of them. As $A^\times$ is the disjoint union of conjugacy classes, we have

$$q^n - 1 = \sum_{k<n} \frac{q^n-1}{q^k-1} + (q-1).$$

If k divides n and $k < n$, the polynomial $\frac{x^n-1}{x^k-1}$ is divisible by the cyclotomic polynomial $\Phi_N(x)$, hence $\Phi_n(q)$ divides $\frac{q^n-1}{q^k-1}$. It follows that $\Phi_n(q)$ divides $q-1$, hence $|\Phi_n(q)| \le q-1$. On the other hand, $\Phi_n(x) = \prod(x-\xi)$, where the product is taken over all primitive n-th roots of unity ξ, hence $\Phi_n(q) = \prod(q-\xi)$. As $|q-\xi| \geq q-1 \geq 1$, we must have $n = 1$. □

Example 8.9.7. *The quaternion algebra $\mathbb{H}$ is a central $\mathbb{R}$-algebra of dimension 4, so Br$(\mathbb{R}) \neq 1$. If F is a field of characteristic not 2 and $a, b \in F^\times$. The F-algebra $(a, b)_F$*

with basis $\{1, i, j, k\}$ and multiplication table $i^2 = a$, $j^2 = b$ and $j = ij = -ji$ is called the (generalized) quaternion algebra. We will see that $(a, b)_F$ is a central simple algebra over F.

Example 8.9.8. *An anti-automorphism of an F-algebra A is a linear automorphism $\sigma : A \to A$ such that $\sigma(x + y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(y)\sigma(x)$ for all $x, y \in A$. An anti-automorphism σ can be viewed as an isomorphism betweedn A and A^{op}. If an anti-automorphism $\sigma \circ \sigma = \mathbf{id}_A$, we say that σ is an involution.*

If A is a central simple F-algebra that admits an anti-automorphism, then $A \cong A^{op}$ and hence $[A]^{-1} = [A]$ in $Br(F)$.

Theorem 8.9.9 (Noether-Skolem)**.** *Let A be a finite-dimensional central simple algebra over F, and let $S, T \subseteq A$ be simple subalgebras. Let $f : S \to T$ be an F-algebra isomorphism. Then there exists $a \in A^\times$ such that $f(s) = asa^{-1}$ for all $s \in S$.*

Proof. Regard A as a right $(A^{\mathrm{op}} \otimes_F S)$-module in two ways. First, we define

$$a \cdot (b^{\mathrm{op}} \otimes s) = bas.$$

Second, we define

$$a * (b^{\mathrm{op}} \otimes s) = baf(s).$$

Since S is simple and A^{op} is central simple, $A^{\mathrm{op}} \otimes_F S$ is simple. Over a simple algebra every two right modules of the same dimension are isomorphic. Therefore, the two module structures are isomorphic. Let $g : A \to A$ be an isomophism, so that

$$g(bas) = bg(a)f(s)$$

for all $a, b \in A$ and $s \in S$. For $a = s = 1$, we get $g(b) = bg(1)$. As g is an isomorphism, this implies $g(1)$ left invertible, hence right invertible since A has finite dimension over F. For $a = b = 1$, we get $sg(1) = g(s) = g(1)f(s)$, so $f(s) = g(1)^{-1}sg(1)$ as desired. □

Remark 8.9.10. *The condition that A is central cannot be dropped. Otherwise, take $S = T = A$ to be a (non-trivial) Galois field extension of F. For $S = T = A$, we get $Aut_{\mathbf{F}-alg}(A) \cong A^\times/F^\times$ for the F-algebra automorphism group, with the action by conjugation. If $A = M_n(F)$, then $A^\times = GL_n(F)$ and $Aut_{\mathbf{F}-alg}(M_n(F)) = GL_n(F)/F^\times = PGL_n(F)$.*

Example 8.9.11. *Let S be an F-algebra and $B = End_F(S)$. Then $S \subseteq B$ by left multiplication and $S^{op} \subseteq B$ by right multiplication. In fact, $S^{op} = C_B(S)$ and $S = C_B(S^{op})$. Indeed, $f \in C_B(S)$ if and only if $f(ax) = af(x)$ for all $a, x \in A$. Plugging $x = 1$, we get $f(a) = af(1)$, i.e. f is right multiplication by $f(1)$. Conversely, if $f(a) = ab$ for some $b \in A$, then $f(ax) = (ax)b = a(xb) = af(x)$, i.e. $f \in C_B(S)$.*

Theorem 8.9.12 (Double Centralizer Theorem)**.** *Let A be a central simple algebra over F and let $S \subseteq A$ be simple subalgebra. Then*

1. *$C_A(S)$ is simple with $Z(C_A(S)) = S \cap C_A(S) = Z(S)$.*

2. *$(\dim S) = (\dim C_A(S)) = \dim(A)$.*

3. *$C_A(C_A(S)) = S$.*

Proof. 1. Let $S \subseteq B = \mathrm{End}_F(S)$. Then $C_B(S) = S^{\mathrm{op}}$. We have

$$S = S \otimes F \subseteq A \otimes_F B$$

and

$$S = F \otimes_F S \subseteq A \otimes_F B.$$

The first inclusion has

$$C_{A\otimes B}(S \otimes F) = C_A(S) \otimes C_B(F) = C_A(S) \otimes B,$$

while the second inclusion has

$$C_{A\otimes B}(F \otimes S) = C_A(F) \otimes C_B(S) = A \otimes S^{\mathrm{op}},$$

which is simple. By Noether-Skolem, $S \otimes F$ and $F \otimes S$ are conjugate. Hence their centralizers $C_A(S) \otimes B$ and $A \otimes S^{\mathrm{op}}$ are conjugate, hence isomorphic. As $A \otimes S^{\mathrm{op}}$ is simple, so is $C_A(S) \otimes B$ and hence $C_A(S)$ is simple.

For the equalities, that $Z(S) = S \cap C_A(S)$ is clear. By the third result, $Z(C_A(S)) = C_A(S) \cap C_A(C_A(S)) = C_A(S) \cap S$.

2. We have $(\dim C_A(S))(\dim B) = (\dim A)(\dim S^{\mathrm{op}})$, and the result follows from $\dim B = (\dim S)^2$.

3. By the second result, $\dim C_A(C_A(S)) = \dim S$ and $S \subseteq C_A(C_A(S))$, so $C_A(C_A(S)) = S$.

□

Corollary 8.9.13. *Let S be a central simple subalgebra of a central simple algebra A. Then $A = S \otimes_F C_A(S)$.*

Proof. Consider the F-algebra homomorphism $f : S \otimes_F C_A(S) \to A$ given by $f(x \otimes y) = xy$. By the theorem, $S \otimes_F C_A(S)$ is a simple F-algebra of the same dimension as A. Hence, f is an isomorphism. □

Remark 8.9.14. *Let A be a central simple algebra over F and let L/F be a field extension. Then $A_L = A \otimes_F L$ is a central simple L-algebra, as it is simple and $Z(A \otimes_F L) = Z(A) \otimes_F Z(L) = F \otimes_F L = L$. Moreover, $\dim_L A_L = \dim_F A$.*

Suppose $A \sim B$ over F. Then $M_n(A) \cong M_n(B)$ for some n and m, so $M_n(A_L) \cong M_m(B_L)$. Therefore, $M_n(A_L) \cong M_m(B_L)$, so $A_L \cong B_L$ over L. Thus, we have a group homomorphism $Br(F) \to Br(F)$ given by extension of scalars $[A] \mapsto [A_L]$.

Proposition 8.9.15. *If A is a central simple algebra over F, then $\dim_F(A) = n^2$ for some n.*

Proof. Let L be the algebraic closure of F. Then A_L is a central simple algebra over L, so $A_L \cong M_n(L)$ for some n. Then $\dim_F(A) = \dim_L(A_L) = n^2$. □

The value n is called the degree of A. Then $\deg(M_k(A)) = k \deg(A)$. Let A be a central simple algebra over F with $A \cong M_k(D)$ for some central division F-algebra D. If $m = \deg(D)$ and $n = \deg(A)$, then $n = km$. The value m is the index of A, denoted $\operatorname{ind}(A)$. From the definition, $\operatorname{ind}(A) \mid \deg(A)$, with equality if and only if A is a division algebra.

8.10 Maximal Subfield

If A is a central simple algebra over F, then $(\deg A)^2 = \dim_F(A)$. Writing $A = M_s(D)$ for a central division F-algebra, the index of A is $\operatorname{ind}(A) = \deg(D)$, so $\deg(A) = s\operatorname{ind}(A)$ and $\deg(D) = \operatorname{ind}(D)$.

Let D be a central division algebra over F and let $L \subseteq D$ be a subalgebra. Then L is a division subalgebra and L is a field extension of F if L is commutative. In the latter case, we will simply say that L is a subfield, with the containment of F understood.

Proposition 8.10.1. *If $L \subseteq D$ is a subfield, then L is maximal if and only if $C_D(L) = L$.*

Proof. ($\Rightarrow$): Suppose $\alpha \in C_D(L)$, then $L \subseteq L[\alpha] \subseteq D$ and $L[\alpha]$ is a subfield of D, so $L[\alpha] = L$.

($\Leftarrow$): Let $L' \subseteq D$ be a subfield containing L. Then $L' \subseteq C_D(L) = L$, so $L' = L$. □

Corollary 8.10.2. *Let L be a maximal subfield of a central division F-algebra D. Then $[L : F] = \deg(D)$.*

Proof. The double centralizer theorem gives $(\dim L)^2 = (\dim L)(\dim C_D(L)) = \dim D = (\deg D)^2$. □

Corollary 8.10.3. *Let L be a subfield of D. Then $[L : F]$ divides $\deg D$.*

Proof. There is a maximal subfield L' of D containing L. Hence $[L : F]$ divides $[L' : F] = \deg D$. □

Example 8.10.4. *Let D be a finite division ring. Then $F = Z(D)$ is a finite field and D is central as an F-algebra. Let L be a maximal subfield of D. Let $\alpha \in D^\times$ and L' a maximal subfield of D containing α. Then $[L : F] = \deg(D) = [L : F]$. As F is a finite field, the fields L and L' are isomorphic over F, hence conjugate by Noether-Skkolem theorem. It follows that $\alpha \in \beta L^\times \beta^{-1}$ for some $\beta \in D^\times$.*

We have proved that $D^\times = \bigcup_{\beta \in D^\times} \beta L^\times \beta^{-1}$, so since the groups are finite, $L\times = D^\times$. Hence $L = D$. Computing dimensions, it follows that $\deg D = 1$.

Let A be a central simple algebra over F and let K/F be a field extension. Then $A_K = A \otimes_F K$ is a central simple algebra over K and $\deg_F A = \deg_K A_K$.

Definition 8.10.5 (Splitting Field)**.** *A central simple F-algebra A is split over F if $A \cong M_n(F)$ for $n = \deg A$. Let A be a central simple F-algebra and K/F a field extension. We say that K is a splitting field of A (or A is split over K) if A_K is split over K.*

Equivalently, A is split over K if $[A] \in \ker(\mathrm{Br}(F) \to \mathrm{Br}(K))$. If K is an algebraic closure of F, then $\mathrm{Br}(K)$ is trivial, so every central simple algebra is split over the algebraic closure.

Remark 8.10.6. *If A is an F-algebra such that $A_K = A \otimes_F K \cong M_n(K)$ for some n, then A is a central simple algebra over F of degree n. In fact, the central simple algebras over F are of this form for some K. These are referred to as twisted forms of $M_n(F)$, since $A \otimes_F K \cong M_n(K) = M_n(F) \otimes_F K$.*

Proof. Computing dimensions, $\dim_F A = \dim_K A_K$. We have

$$Z(A) \otimes_F K = Z(A \otimes_F K) = K = F \otimes_F K$$

and $F \subseteq Z(A)$, so computing dimensions, $Z(A) = F$. Hence A is central. To see that A is simple, if $I \subseteq A$ is a two-sided ideal, then $I \otimes_F K \subseteq A \otimes_F K = M_n(K)$ is a two-sided ideal, so $I \otimes_F K$ is 0 or $A|otimes_F K$. Hence I is either 0 or A. □

Theorem 8.10.7. *Let A be a central simple algebra over F with* $\deg(A) = n$. *Let $L \subseteq A$ be a subfield with $[L : F] = n$. Then L is a splitting field of A.*

Proof. Since $A \otimes_F L$ and $M_n(L)$ are central simple algebras of the same dimension, it suffices to find any homomorphism. Define $f : A \otimes_F L \to \mathrm{End}_L(A) \cong M_n(L)$ with A viewed as a right L-module by $f(a \otimes l)(m) = aml$. □

Corollary 8.10.8. *Every maximal subfield of a central division algebra D is a splitting field of D.*

Corollary 8.10.9. *Every central simple algebra A over F has a splitting field L such that $[L : F] = ind(A)$.*

Proof. Write $A = M_s(D)$ for a central division algebra D of degree $n = \mathrm{ind}(A)$. Then a maximal subfield L of D is a splitting field for D, hence for A. □

Let D be a central division F-algebra and $\alpha \in D$. Then $F[\alpha] \subseteq D$ is a subfield and $[F[\alpha] : F] < \infty$, so α is algebraic over F.

Lemma 8.10.10. *Let D be a central division F-algebra with $D \neq F$. Then there exists $\alpha \in D\backslash F$ which is separable over F.*

Proof. If $\mathrm{char}(F) = 0$, then we are done. Otherwise, let $p = \mathrm{char}(F) > 0$. Suppose all $\alpha \in D\backslash F$ are not separable. Pick $\alpha \in D\backslash F$. Then the maximal separable extension of F contained in $F(\alpha)$ is F, so $F(\alpha)/F$ is purely inseparable. Therefore, $\alpha^{p^n} \in F$ for some n. Choose n as small as possible and let $\beta = \alpha^{p^{n-1}}$, so $\beta^p \in F$.

Define $f : D \to D$ by $f(a) = \beta a - a\beta$. Then $f \neq 0$, since D is central and $D \neq F$, while $f^p(a) = \beta^p a - a\beta^p = 0$. Thus f is nilpotent, so we can choose the smallest $k > 1$ with $f^k = 0$.

Let $\gamma = f^{k-1}(\delta) \neq 0$ for some $\delta \in D$, so then $f(\gamma) = 0$. If $\varepsilon = f^{k-2}(\delta)$, then $\gamma = f(\varepsilon) = \beta\varepsilon - \varepsilon\beta$ and $\beta\gamma - \gamma\beta = 0$, i.e. β and γ commute. Since D is a division algebra, we can write $\gamma = \beta\zeta$ for some $\zeta \in D$. Note that β, γ and ζ commute. Then $\beta\zeta = \zeta\beta$, so

$$\beta = \gamma\zeta^{-1} = (\beta\varepsilon - \varepsilon\beta)\zeta^{-1} = \beta\varepsilon\zeta^{-1} - \varepsilon\beta\zeta^{-1} = \beta\varepsilon\zeta^{-1} - \varepsilon\zeta^{-1}\beta = \beta\theta - \theta\beta$$

for $\theta = \varepsilon\zeta^{-1}$. Thus $1 = \theta - \beta^{-1}\theta\beta$, hence $\theta = 1 + \beta^{-1}\theta\beta$, so

$$\theta^{p^m} = (1 + \beta^{-1}\theta\beta)^{p^m} = 1 + \beta^{-1}\theta^{p^m}\beta = 1 + \theta^{p^m},$$

for large m since $\theta^{p^m} \in F$, a contradiction. □

Corollary 8.10.11. *Every central division F-algebra admits a maximal subfield which is separable over F.*

Proof. Let $L \subseteq D$ be the maximal separable subfield extending F. Then $L \subseteq C_D(L)$, with equality if and only if L is a maximal subfield of D. If $L \neq C_D(L)$, since $C_D(L)$ is central division L-algebra, by the lemma, there exists $\alpha \in C_D(L) \backslash L$ such that $L(\alpha)/L$ is non-trivial and separable, but then $L(\alpha)/F$ is separable, contradicting maximality of L as a separable extension. □

Corollary 8.10.12. *Every central simple F-algebra is split by a (finite) separable extension of F.*

Proof. Let A be a central simple F-algebra and write $A = M_s(D)$ for D a central division F-algebra. Let $L \subseteq D$ be a maximal subfield which is separable over F. Then L is a splitting field for D, so also for A. □

Example 8.10.13. *If F is separably closed, i.e. it has no non-trivial separable extensions, then $Br(F) = 1$. One can construct the separable closure of a field by taking all separable elements in an algebraic closure.*

Theorem 8.10.14. *Let A be a central simple F-algebra and K/F be a field extension.*

1. *$ind(A_K) \mid ind(A)$;*
2. *If K/F is a finite field extension, then $ind(A) \mid [K : F] \cdot ind(A_K)$. Moreover, if $A_K = M_s(D)$ for a central division K-algebra D, then $D \hookrightarrow M_p(A)$ for $p = [K : F] ind(A_K)/ind(A)$.*

Proof. 1. Let $A = M_n(E)$ for a division algebra E, then $\operatorname{ind}(A) = \deg(E)$. We have $A_K = M_n(E_K)$, so $\operatorname{ind}(A_K) = \operatorname{ind}(E_K) \mid \deg(E_K) = \deg(E) = \operatorname{ind}(A)$.

2. First suppose A is a division algebra. Let $r = [K : F]$ and consider the embedding $K \hookrightarrow \mathrm{End}_F(K) = M_r(F)$ via left multiplications. Therefore,

$$M_s(F) \subseteq M_s(D) \cong A_K = A \otimes K \hookrightarrow A \otimes M_r(F) = M_r(A).$$

Let $C = C_{M_r(A)}(M_s(F))$. Since $M_s(F)$ and $M_r(A)$ are central simple algebras, C is also central simple and we have $M_s(C) \cong M_s(F) \otimes C \cong M_r(A)$. As A is division algebra, we have $C \cong M_p(A)$, where $p = \frac{r}{s}$. We have $s = \frac{\deg(A_K)}{\deg(D)} = \frac{\mathrm{ind}(A)}{\mathrm{ind}(A_K)}$, hence $p = [K : F] \cdot \frac{\mathrm{ind}(A_K)}{\mathrm{ind}(A)}$, i.e. $\mathrm{ind}(A)$ divides $[K : F]\mathrm{ind}(A_K)$. Note that $D \subseteq C \cong M_p(A)$.

In the general case, we write $A = M_n(E)$ for a division algebra E. We have $\mathrm{ind}(E) = \mathrm{ind}(A)$ and $\mathrm{ind}(E_K) = \mathrm{ind}(A_K)$. Also, by the above, $D \hookrightarrow M_p(E) \subseteq M_p(A)$.

□

Corollary 8.10.15. *If a finite extension K/F splits a central simple F-algebra A, then ind$(A) \mid [K : F]$.*

Corollary 8.10.16. *If A is a central simple F-algebra and K/F is a splitting field for A of degree $r$ind(A), then $K \hookrightarrow M_r(A)$. If A is a division algebra and $[K : F] =$ ind(D), then K is isomorphic to a maximal subfield of A.*

Proposition 8.10.17. *Let D be a division algebra, then the intersection of the subfields of D and the splitting fields of D is exactly the maximal subfields of D.*

8.11 Cyclic Algebra

Definition 8.11.1 (Cyclic Algebra)**.** *Let L/F be a cyclic field extension with Galois group $G =$ Gal(L/F) generated by σ. Let $n = [L : F]$ and $a \in F^\times$. The cyclic algebra $(L/F, \sigma, a)$ is the F-algebra given by*

$$A = (L/F, \sigma, a) = \bigoplus_{i=0}^{n-1} L \cdot u = (L \cdot 1) \oplus (L \cdot u) \oplus \cdots \oplus (L \cdot u^{n-1}),$$

where $1, u, \cdots, u^{n-1}$ is a basis for L/F. The multiplication is defined by $u^n = a \cdot 1$ and extending the relations $(xu^i)(yu^j) = x\sigma^i(y)u^{i+j}$ for $x, y \in L$. In particular, $uyu^{-1} = \sigma(y)$.

Example 8.11.2. 1. *Suppose char$(F) \neq 2$. Let $L = F(\sqrt{b}) = F[j]/(j^2 - b)$ for $b \in F$ not a square. Then for $a \in F^\times$, we have*

$$(L/F, \sigma, a) = (L \cdot 1) \oplus (L \cdot i) = (F \cdot 1) \oplus (F \cdot i) \oplus (F \cdot j) \oplus (F \cdot ji)$$

with $i^2 = a$, $j^2 = b$, $ij = -ji$. Hence $(L/F, \sigma, a) = (a, b)_F$ is the generalied quaternion algebra. The usual quaternions are $\mathbb{H} = (\mathbb{C}/\mathbb{R},$ conjugation $, -1)$.

2. *If char$(F) = 2$, then polynomials $x^2 + x + a$ for $a \in F$ are separable. Let $L = F(\theta)$ for θ a root of $x^2 + x + a$ (assumed irreducible). Then $\sigma(\theta) = \theta + 1$, so $(L/F, \sigma, a)$ has basis $\{1, \theta, u, \theta u\}$ with relations $\theta^2 + \theta + a = 0$, $u^2 = a$, $u\theta = (\theta + 1)u$.*

Proposition 8.11.3. *$A = (L/F, \sigma, a)$ is a central simple algebra.*

Proof. Suppose $s = \sum_i \alpha_i u^i \in Z(A)$ where $\alpha \in L$ and let $\beta \in L$. Then

$$0 = \beta s - s\beta = \sum_i (\alpha_i \beta - \alpha_i \sigma^i(\beta)) u^i,$$

hence $\alpha_i(\beta - \sigma^i(\beta)) = 0$ for all i. If $i \neq 0$, then we can choose β so that $\sigma^i(\beta) \neq \beta$, so then $\alpha_i = 0$. Hence $s = \alpha_0 \cdot 1$, so $C_A(L) = L$. From $us = su$, we get $\sigma(\alpha_0) = \alpha_0$. This shows that $\alpha_0 \in F$, so $Z(A) = F$.

Let $0 \neq I \subseteq A$ be an ideal. We must show that $1 \in I$. Let $s = \sum_i \alpha_i u^i \in I \neq 0$ have the smallest number of non-zero terms. By replacing s with su^k for some k, we can suppose $\alpha_0 \neq 0$. For $\beta \in L$, we have $\beta s - s\beta = \sum_i \alpha_i(\beta - \sigma^i(\beta))u^i \in I$. For $i = 0$, we get 0, so $\beta s - s\beta = 0$. Therefore, $\alpha_i = 0$ for $i \neq 0$, so $s = \alpha_0 \cdot 1$ for $\alpha_0 \in L$ non-zero. Hence, $\alpha_0^{-1} s = 1 \in I$. □

Therefore, A is a central simple algebra of dimension n^2 containing L as a subfield of dimension n over F. In particular, L/F is a splitting field for A, so

$$[A] = \ker(\mathrm{Br}(F) \to \mathrm{Br}(L)) =: \mathrm{Br}(L/F)$$

(the relative Brauer group). If A is a division algebra, then L is also a maximal subfield of A.

It can also be shown that $C(L/F, \sigma, a)$ and $C(L/F, \sigma^i, a^i)$ are isomorphic for i coprime to n.

Lemma 8.11.4. *Let L/F be a cyclic field extension of degree n and let A be a central simple algebra of degree n over F. If $L \hookrightarrow A$, then $A \cong C(L/F, \sigma, a)$ for some σ generating $G = Gal(L/F)$, and $a \in F^\times$.*

Proof. By Noether-Skolem theorem, $\sigma : L \to L$ extends to an inner automorphism $\sigma(\alpha) = \beta\alpha\beta^{-1}$ for some $\beta \in A^\times$ and all $\alpha \in L$. Then $\alpha = \sigma^n(\alpha)$ shows that $\beta^n \in C_A(L) = L$. Since $\beta^n = \sigma(\beta^n)$, in fact $\beta^n \in F$. Take $a = \beta^n$, then define a map

$$\begin{aligned} C(L/F, \sigma, a) &\to A \\ \alpha \in L &\mapsto \alpha \in L \subseteq A \end{aligned}$$

and $u \mapsto \beta$. It is easily checked that this is well-defined and a map of central simple algebras of the same dimension, hence an isomorphism. □

Proposition 8.11.5. *Let L/F be a cyclic extension. Then*

$$Br(L/F) = \{[C(L/F, \sigma, a)] \mid a \in F^\times\}.$$

Proof. Let $[A] \in \mathrm{Br}(L/F)$ for A a division algebra. Then $\deg(A) = \mathrm{ind}(A) = m$. We know that $n = [L : F]$ is divisible by m, so $n = mk$ for some k and $L \hookrightarrow M_k(A)$. The degree of $M_k(A)$ is $km = n$, so there is a cyclic algebra $C(L/F, \sigma, a)$ isomorphic to $M_k(A)$, hence $[A] = [C(L/F, \sigma, a)]$. □

Lemma 8.11.6. $C(L/F, \sigma, 1) \cong M_n(F)$ *for* $n = [L : F]$.

Proof. Define an F-algebra isomorphism $C(L/F, \sigma, 1) \to \mathrm{End}_F(L) = M_n(F)$ by $\alpha \in L \mapsto l_\alpha \in \mathrm{End}_F(L)$ and $1 \mapsto \sigma$. □

Lemma 8.11.7. *Let L/F be cyclic extension of degree n, $\sigma \in Gal(L/F)$ be a generator, and $a, b \in F^\times$. Then $C(L/F, \sigma, a) \cong C(L/F, \sigma, b)$ if and only if $b/a \in N_{L/F}(L^\times)$.*

Proof. ($\Rightarrow$): Let $f : C(L/F, \sigma, a) \to C(L/F, \sigma, b)$ be an isomorphism. Then $f(L)$ and L are isomorphic subfields of $C(L/F, \sigma, b)$, so by Noether-Skolem theorem, we can modify f by conjugation to suppose f fixes L. If u gneerates $C(L/F, \sigma, a)$ and v generates $C(L/F, \sigma, b)$, then $f(u)$ and v act by conjugation in the same way on $L \subseteq C(L/F, \sigma, b)$. Hence, $f(u)v^{-1}$ is in the centralizer of L, which is L itself, so $f(u) = \alpha^{-1}v$ for some $\alpha \in L^\times$. It follows by computation that $b = aN_{L/F}(\alpha)$.

($\Leftarrow$): Suppose $b = aN_{L/F}(\alpha)$ for some $\alpha \in L^\times$. Let u be a generator of $C(L/F, \sigma, a)$ and v be a generator of $C(L/F, \sigma, b)$. We can then define a homomorphism $C(L/F, \sigma, a) \to$

$C(L/F,\sigma,b)$ by fixing $L^\times$ and mapping $u \mapsto \alpha^{-1}v$. Since the two algebras are central simple algebras, the homomorphism is automatically an isomorphism. □

Corollary 8.11.8. $[C(L/F,\sigma,a)] = 1$ *if and only if* $a \in N_{L/F}(L^\times)$.

Example 8.11.9. *Let* $F = \mathbb{F}_q$ *be a finite field. We have* $Br(F) = \bigcup\limits_{L/F} Br(L/F)$ *with* L/F *ranging over all finite extensions. Since* F *is finite,* L/F *is cyclic and* $N_{L/F} : L^\times \to F^\times$ *is surjective, so* $Br(L/F) = 1$.

Let L/F *be cyclic and* $\sigma \in Gal(L/F)$ *be a generator. Define* $f : F^\times \to Br(L/F)$ *given by* $a \mapsto [C(L/F,\sigma,a)]$.

Theorem 8.11.10. *If* L/F *is a cyclic field extension,* f *is a surjective homomorphism and* $\ker(f) = N_{L/F}(L^\times)$. *In particular,*

$$Br(L/F) \cong F^\times/N_{L/F}(L^\times).$$

Consider $p : L \otimes_F L \to L^n$ *by* $p(x \otimes y) = (xy, x\sigma(y), \cdots, x\sigma^{n-1}(y))$.

Proposition 8.11.11. p *is an* F*-algebra isomorphism.*

Proof. Write $L = F(\alpha) = F[t]/(f)$ with $f(t) = (t-\alpha)\cdots(t-\sigma^{n-1}(\alpha)) \in L[t]$. Then $L \otimes_F L = L[t]/(f)$ and the map p takes $g \in L[t]/(f)$ to $(g(\alpha), \cdots, g(\sigma^{n-1}(\alpha)))$. This is an isomorphism by the Chinese Remainder Theorem. □

If $G = \mathrm{Gal}(L/F)$, then G acts on $L \otimes_F L$ by $\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y)$. If G acts on L^n component-wise, then p respects the action of G, so $(L \otimes_F L)^G \cong F^n$.

Lemma 8.11.12. *Let* A *be a central simple algebra of degree* n *over* F. *If* $F^n \hookrightarrow A$ *as a subalgebra, then* $A \cong M_n(F)$.

Proof. We have $A \cong \mathrm{End}_D(V) \cong M_k(D)$ for some central division F-algebra D and V a D-module of rank k. Let $e_1, \cdots, e_n \in F^n$ be orthogonal idempotents. Then $V = e_1(V) \oplus \cdots \oplus e_n(V)$ gives $\mathrm{rank}_D(V) \geq n$. On the other hand, if $\deg(D) = m$, then $n = km$, so $\mathrm{rank}_D(V) = k = \frac{n}{m} \geq n$, so $m = 1$ and $k = n$, so $D = F$. □

Proposition 8.11.13. $[C(L/F,\sigma,a)] \cdot [C(L/F,\sigma,b)] = [C(L/F,\sigma,ab)] \in Br(L/F)$.

Proof. It suffices to show that

$$C(L/F,\sigma,a) \otimes_F C(L/F,\sigma,b) \cong M_n(C(L/F,\sigma,ab)).$$

To do this, we find an embedding of $C(L/F, \sigma, ab)$ into the tensor product with centralizer $M_b(F)$. Let

$$A = C(L/F, \sigma, a) = \bigoplus_i Lu^i$$

and

$$B = C(L/F, \sigma, b) = \bigoplus_i Lv^i.$$

Then $A \otimes_F B = \bigoplus (L \otimes_F L)(u^i \otimes v^j)$. If $D = C(L/F, \sigma, ab) = \bigoplus Lw^i$, then

$$\bigoplus (L \otimes_F F)(u^i \otimes v^i) \cong D$$

by $u \otimes v \mapsto w$, which embeds in $A \otimes_F B$. Note that the diagonal G-action on $L \otimes_F L = L^n$ coincides with the component-wise G-action. Hence, the centralizer of D contains $(L \otimes_F L)^G = F^n$, so the centralizer of D is $M_n(F)$ by the lemma. □