Suns

Eric Liu

CONTENTS

CHAPTER 3   ALGEBRAIC GEOMETRY ———— PAGE 109——

3

Chapter 1

Groups

1.1 Definition of Groups

Let M be a set equipped with a binary operation $M \times M \to M$. We say M is a **monoid** if the binary operation is associative and there exists a two-sided identity $e \in M$.

> **Example 1.1.1: Identity of monoids is required to be two-sided**
>
> Defining $(x, y) \mapsto y$, we see that the operation is associative and every element is a left identity, but no element is a right identity unless $|M| = 1$. This is an example why identity must be two-sided.

Because the identity of a monoid is defined to be two-sided, clearly it must be unique. Suppose every element of monoid M has a left inverse. Fix $x \in M$. Let $x^{-1} \in M$ be a left inverse of x. To see that x^{-1} is also a right inverse of x, let $(x^{-1})^{-1} \in M$ be a left inverse of x^{-1} and use

$$(x^{-1})^{-1} = (x^{-1})^{-1}e = (x^{-1})^{-1}(x^{-1}x) = ((x^{-1})^{-1}x^{-1})x = ex = x$$

to deduce

$$xx^{-1} = (x^{-1})^{-1}x^{-1} = e$$

In other words, if we require every element of a monoid M to has a left inverse, then immediately every left inverse upgrades to a right inverse. In such case, we call M a **group**. Notice that inverses of elements of a group are clearly unique.

Theorem 1.1.2. (Group criteria) If a binary operation $G \times G \to G$ is associative, has a left identity, and always has a left inverse, then G forms a group.

Proof. If $y \in G$ is **idempotent**, then it must be identity, since $y = (y^{-1}y)y = y^{-1}y = e$. Because of such, we see a left inverse is also a right inverse, since $(xx^{-1})(xx^{-1}) = xex^{-1} = $

xx^{-1}. This then shows that the left identity is also a right identity, since $xe = x(x^{-1}x) = x$. ∎

Theorem 1.1.3. (Group criteria for finite set) Let $|G| \in \mathbb{N}$. If the binary operation $G \times G \to G$ is associative and both cancellation laws holds:

$$au = aw \implies u = w \quad \text{and} \quad ua = wa \implies u = w$$

then G forms a group.

Proof. Because the set is finite, for all a, we may attach it with an natural number $n(a)$ such that $a^{n(a)+1} = a$. Clearly,

$$aa^{n(a)}b = a^{n(a)+1}b = ab = ab^{n(b)+1} = ab^{n(b)}b$$

This then by cancellation laws implies $a^{n(a)} = b^{n(b)}$, which can be easily checked to be the identity. ∎

Theorem 1.1.4. (Subgroup criteria for finite subset) Let G be a group and $S \subseteq G$ be finite. If S is closed under the binary operation, then S forms a group.

Proof. Because S is finite, for all $a \in S$, there exists $n(a) \in \mathbb{N}$ such that

$$a^{n(a)}a = a$$

Multiplying both side with a^{-1}, we see that $a^{n(a)} = e$ and $a^{-1} = a^{n(a)} \in S$. ∎

Example 1.1.5: Euler's totient function

By theorem 1.1.3, we see that the set of nonzero integer relatively prime to n and modulo n forms a group under multiplication modulo n, called the **multiplicative group of integer modulo** n, or equivalently the unit group of the ring $\mathbb{Z}_n$. This immediately shows that

$$a^{\phi(a)} \equiv 1 \pmod{n}$$

for all $a \in \mathbb{N}$ coprime with n, where the **totient function** $\phi(a)$ is the number of natural numbers $\leq a$ and coprime with a. We now have **Fermat's little theorem** as a special case.

Unlike the category of monoids, the category of groups behaves much better. Given two groups G, H and a function $\varphi : G \to H$, if φ respects the binary operation, then φ also respects the identity:

$$e_H = (\varphi(x)^{-1})\varphi(x) = (\varphi(x)^{-1})\varphi(xe_G) = (\varphi(x)^{-1}\varphi(x))\varphi(e_G) = \varphi(e_G)$$

which implies that φ must also respect inverse. In such case, we call φ a **group homomorphism**. In this note, by a **subgroup** H of G, we mean an injective group homomorphism $H \hookrightarrow G$. Clearly, a subset of G forms a subgroup if and only if it is closed under both the binary operation and inverse. Note that one of the key basic property of subgroup $H \leq G$ is that if $g \notin H$, then $hg \notin H$, since otherwise $g = h^{-1}hg \in H$.

Let S be a subset of G. The group of **words** in S:

$$\{s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \in G : n \in \mathbb{N} \cup \{0\} \text{ and } s_i \in S \text{ and } \epsilon_i = \pm 1\}$$

is clearly the smallest subgroup of G containing S. We say this subgroup is **generated** by S. If G is generated by a single element, we say G is **cyclic**. Let $x \in G$. The **order** of G is the cardinality of G, and the order of x is the cardinality of the cyclic subgroup $\langle x \rangle \subseteq G$, or equivalently the infimum of the set of natural numbers n that makes $x^n = e$.

Let G be a group and H a subgroup of G. The **right cosets** Hx are defined by $Hx \triangleq \{hx \in G : h \in H\}$. Clearly, when we define an equivalence relation in G by setting:

$$x \sim y \overset{\triangle}{\iff} xy^{-1} \in H$$

the equivalence class $[x]$ coincides with the right coset Hx. Note that if we partition G using **left cosets**, the equivalence relation being $x \sim y \iff x^{-1}y \in H$, then the two partitions need not to be identical.

> **Example 1.1.6: An non-normal subgroup**
>
> Let $H \triangleq \{e, (1,2)\} \subseteq S_3$. The right cosets are
>
> $$H(2,3) = \{(2,3), (1,2,3)\} \quad \text{and} \quad H(1,3) = \{(1,3), (1,3,2)\}$$
>
> while the left cosets being
>
> $$(2,3)H = \{(2,3), (1,3,2)\} \quad \text{and} \quad (1,3)H = \{(1,3), (1,2,3)\}$$

However, as one may verify, we have a well-defined bijection $xH \mapsto Hx^{-1}$ between the sets of left cosets and right cosets of H. Therefore, we may define the **index** $[G : H]$ of H in G to be the cardinality of the collection of left cosets of H, without falling into the discussion of left and right. Moreover, let K be a subgroup of H, by axiom of choice, clearly we have:

$$[G : K] = [G : H] \cdot [H : K]$$

which gives **Lagrange's theorem**

$$o(G) = [G : H] \cdot o(H)$$

7

as a corollary.

<div style="border:1px solid #ccc; padding:10px;">

Example 1.1.7: Isomorphic subgroups can have different indices

Note that every nontrivial subgroups of $\mathbb{Z}$ are isomorphic, yet they are of distinct index. However, subgroups $H \leq G$ isomorphic through an automorphism $\varphi \in \mathrm{Aut}(G)$ must have the same index, since $xH \mapsto \varphi(x)\varphi(H)$ forms a well-defined bijection.

</div>

Theorem 1.1.8. (Order formula) Let $H, K \leq G$. Then

$$|HK| \cdot o(H \cap K) = o(H) \cdot o(K)$$

and

$$[G : H \cap K] \leq [G : H] \cdot [G : K]$$

If moreover that H, K both have finite index, then

$$\mathrm{lcm}\left([G : H], [G, K]\right) \leq [G : H \cap K]$$

Proof. The first formula follows from checking that the natural map from the left coset space $K/H \cap K$ to the left coset space HK/H forms a well-defined bijection. The second formula follows from checking that the natural map from the left coset space $G/H \cap K$ to the product $G/H \times G/K$ of left coset spaces forms a well-defined injection. The third formula follows from

$$[G : H \cap K] = [G : H] \cdot [H : H \cap K] = [G : K] \cdot [K : H \cap K]$$

$\blacksquare$

1.2 Group Action

Let G be a group and X a set. If we say G **acts on** X **from left**, we are defining a function $G \times X \to X$ such that

(i) $e \cdot x = x$ for all $x \in X$.

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

Note that there is a difference between left action and right action, as gh means $g \circ h$ in left action and means $h \circ g$ in right action. Because groups admit inverses, a G-action is in fact a group homomorphism $G \to \mathrm{Bij}(X)$.

Let $x \in X$. We call the set $\Gamma \triangleq \{g \cdot x \in X : g \in G\}$ the **orbit** of x. Clearly the set $\mathrm{Stab}(x)$ of all elements of G that fixes x forms a group, called the **stabilizer subgroup**. Consider the action left, and let $G / \mathrm{Stab}(x)$ denote the left coset space. The fact that the obvious mapping between $G / \mathrm{Stab}(x)$ and Γ forms a bijection is called the **orbit-stabilizer theorem**, which relates the index of $\mathrm{Stab}(x)$ and the length of Γ:

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

The two most important group action are **left multiplication** and **left conjugation**:

$$g \cdot A \triangleq \{ga \in G : a \in A\} \quad \text{and} \quad g \cdot A \triangleq \{gag^{-1} \in G : a \in A\}$$

on the power set of G. Clearly, orbit of a subgroup under left multiplication is its left coset space.

Theorem 1.2.1. (Cauchy's theorem for finite group) Let G be a finite group and p a prime number that divides $o(G)$. Then the number of elements of order divided by p is a positive multiple of p.

Proof. The set X of p-tuples $(x_1, \ldots, x_p)$ that satisfies $x_1 \cdots x_p = e$ clearly has cardinality $o(G)^{p-1}$. Consider the group action $C_p \to \mathrm{Bij}(X)$ defined by

$$g \cdot (x_1, \ldots, x_p) \triangleq (x_p, x_1, \ldots, x_{p-1}), \quad \text{where } C_p = \langle g \rangle$$

Notice that $x^p = e$ if and only if $(x, \ldots, x) \in X$. Therefore the number of cardinality 1 orbit equals to number of solution to $x^p = e$. By orbit-stabilizer theorem, an orbit in X either has cardinality p or 1. Therefore, we may write

$$p \mid o(G)^{p-1} = m + kp$$

with m the number of cardinality 1 orbits and k the number of cardinality p orbits. Clearly we have $p \mid m$, as desired. ∎

1.3 Normal Subgroups

Because the inverse of an injective group homomorphism forms a group homomorphism, we know $\mathrm{Aut}(G)$ forms a group. We say $\phi \in \mathrm{Aut}(G)$ is an **inner automorphism** if ϕ takes the form $x \mapsto gxg^{-1}$ for some fixed $g \in G$. We say two elements $x, y \in G$ are **conjugated** if there exists some inner automorphism that maps x to y. Clearly conjugacy forms an equivalence relation. We call its classes **conjugacy classes**.

From the point of view of inner automorphism, we see that it is well-defined whether an element $g \in G$ **normalize** a subset $S \subseteq G$:

$$gSg^{-1} = S$$

independent of left and right. Because of the independence, for each subset $S \subseteq G$, we see that the set of elements $g \in G$ that normalize S forms a group, called the **normalizer** of S, in fact the stabilizer subgroup $\mathrm{Stab}(S)$ under the conjugacy action.

Example 1.3.1: Conjugation can send subgroups to proper subgroup

Consider $G \triangleq \mathrm{GL}_2(\mathbb{R})$ and consider:

$$H \triangleq \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : n \in \mathbb{Z} \right\} \quad \text{and} \quad g \triangleq \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

Note that $gHg^{-1} < H$.

Given $x, y \in G$, the notation $[x, y] \in G$ is called the **commutator of x and y**. In this note, we take the convention:

$$[x, y] \triangleq xyx^{-1}y^{-1}$$

The other convention is $[x, y] = x^{-1}y^{-1}xy$, and the differences lies in sides. In our convention, we see that $[x, y] \in H$ if and only if $Hxy = Hyx$, while the other convention leads us to $[x, y] \in H \iff xyH = yxH$. However, because $[x, y]$ in our convention is just $[x^{-1}, y^{-1}]$ in the other convention, if $H, K \leq G$, then the set $[H, K]$ is defined the same using either. In general, $[H, K]$ doesn't form a group. In fact, we clearly have $[H, K] = [K, H]^{-1}$.

Equivalent Definition 1.3.2. (Normal subgroups) Let $N \leq G$. We say N is a **normal subgroup** of G if any of the followings hold true:

(i) $\phi(N) \subseteq N$ for all $\phi \in \mathrm{Inn}(G)$

(ii) $\phi(N) = N$ for all $\phi \in \mathrm{Inn}(G)$

(iii) $xN = Nx$ for all $x \in G$.

(iv) The set of all left cosets of N equals the set of all right cosets of N.

(v) N is a union of conjugacy classes.

(vi) $[N, G] \subseteq N$.

(vii) For all $x, y \in G$, we have $xy \in N \iff yx \in N$.

Proof. (i) $\implies$ (ii): Let $\phi \in \mathrm{Inn}(G)$. By premise, $\phi(N) \subseteq N$ and $\phi^{-1}(N) \subseteq N$. Applying ϕ to both side of $\phi^{-1}(N) \subseteq N$, we have $\phi(N) \subseteq N \subseteq \phi(N)$, as desired.

(ii) $\implies$ (iii): Consider the automorphisms:

$$\phi_{L,x}(g) = xg \quad \text{and} \quad \phi_{L,x^{-1}}(g) = x^{-1}g \quad \text{and} \quad \phi_{R,x}(g) = gx$$

Because $\phi_{L,x^{-1}} \circ \phi_{R,x} \in \mathrm{Inn}(G)$, by premise we have:

$$xN = \phi_{L,x}(N) = \phi_{L,x} \circ \phi_{L,x^{-1}} \circ \phi_{R,x}(N) = \phi_{R,x}(N) = Nx$$

(iii) $\implies$ (iv) is clear. (iv) $\implies$ (iii): Let $x \in G$. By premise, there exists some $y \in G$ that makes $xN = Ny$. Let $x = ny$. The proof then follows from noting

$$xN = Ny = N(n^{-1}x) = Nx$$

(iii) $\implies$ (v): Let $n \in N$ and $x \in G$. We are required to show $xnx^{-1} \in N$. Because $xN = Nx$, we know $xn = \widetilde{n}x$ for some $\widetilde{n} \in N$. This implies

$$xnx^{-1} = \widetilde{n}xx^{-1} = \widetilde{n} \in N$$

(v) $\implies$ (vi): Fix $n \in N$ and $x \in G$. By premise, $xn^{-1}x^{-1} \in N$. Therefore, $n(xn^{-1}x^{-1}) \in N$, as desired.

(vi) $\implies$ (vii): Let $xy \in N$. To see yx also belong to N, observe:

$$(xy)^{-1}(yx) = (xy)^{-1}x^{-1}xyx = [xy, x] \in N$$

(viii) $\implies$ (i): Let $n \in N$ and $x \in G$. Because $(nx)x^{-1} = n \in N$, by premise we have $x^{-1}nx \in N$, as desired. $\blacksquare$

Notably, since given the "conjugate by left" $\varphi_g \in \mathrm{Inn}(G)$ and $\phi \in \mathrm{Aut}(G)$, we have $\phi \circ \varphi_g \circ \phi^{-1} = \varphi_{\phi(g)}$, we see that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. We call $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ the **outer automorphism group** of G.

Example 1.3.3: Dedekind and Hamiltonian group

A group is said to be **Dedekind** if all of its subgroups are normal. Clearly every abelian group is Dedekind. Non-abelian Dedekind groups are called **Hamiltonian**. The simplest Hamiltonian group is the **quaternion group** Q_8, which is the group of the quaternions under multiplication:

$$Q_8 \triangleq \{1, i, j, k, -1, -i, -j, -k\}$$

Note that Q_8 is Dedekind because every nontrivial element is of order 4. Clearly, Q_8 has center $\{\pm 1\}$. Because $Z(Q_8)$ has index 4, we know $Q_8/Z(Q_8)$ is abelian. This then by correspondence theorem implies $Q_8^{(1)} \leq Z(Q_8)$. Because Q_8 is non-abelian, we now see $Q_8^{(1)} = Z(Q_8) = \{\pm 1\}$. Note that Q_8 clearly has the conjugacy classes

$$\{1\} \cup \{-1\} \cup \{\pm i\} \cup \{\pm j\} \cup \{\pm k\}$$

Interestingly, Q_8 is a group that contains a smallest non-trivial subgroup. Every non-trivial subgroup of Q_8 must contains the group $\{\pm 1\}$.

1.4 Isomorphism Theorems

Let $N \trianglelefteq G$. We say a group homomorphism $\pi : G \to G/N$ satisfies the **universal property of quotient group** G/N if

(i) π vanishes on N. **(Group condition)**

(ii) For all group homomorphism $f : G \to H$ that vanishes on N there exist a unique group homomorphism $\widetilde{f} : G/N \to H$ that makes the diagram:

$$
\begin{array}{ccc}
G & \xrightarrow{\ \ \pi\ \ } & G/N \\
 & {\scriptstyle f}\searrow & \downarrow{\scriptstyle \widetilde{f}} \\
 & & H
\end{array}
$$

commute. **(Universality)**

Theorem 1.4.1. (First isomorphism theorem for groups) The group homomorphism $\pi : G \to G/N$ is always surjective with kernel N. Let $f : G \to H$ be a group homomorphism. Then $\ker f$ is normal in G, and the induced homomorphism $\widetilde{f} : G/\ker f \to H$ is injective.

Proof. They are consequences of the construction. ∎

Theorem 1.4.2. (Third isomorphism theorem and correspondence theorem for groups) Let $N \trianglelefteq G$. The canonical projection $\pi : G \to G/N$ gives rise to a bijection between the set of subgroups of G that contains N and the set of subgroups of G/N. The bijection is moreover a bijection between the set of normal subgroups of G that contains N and the set of normal subgroups of G/N. The bijection also maps normalizer of subgroups $\leq G$ that contains N to the normalizer of the image of the subgroup.

In fact, given $K \trianglelefteq G$ that contains N, if we identify K/N as a subgroup of G/N the natural way:

$$
\begin{array}{ccc}
K & \xrightarrow{\ \ \pi\ \ } & \frac{K}{N} \\
 & \searrow & \downarrow \\
 & & \frac{G}{N}
\end{array}
$$

then $\frac{K}{N} \trianglelefteq \frac{G}{N}$ is the normal subgroup that corresponds to $K \trianglelefteq G$, and we have a natural isomorphism $\frac{G}{K} \cong \frac{\frac{G}{N}}{\frac{K}{N}}$.

Proof. Routine. ∎

Theorem 1.4.3. (Second isomorphism theorem for groups) Let $H \leq G$. If $K \leq N_G(H)$, then their product:

$$HK \triangleq \{hk \in G : h \in H \text{ and } k \in K\}$$

forms a group (in fact, the subgroup generated by $H \cup K$) and is defined independent of left and right. Moreover, $H \trianglelefteq HK$ with $hkH = Hk$, and $H \cap K \trianglelefteq K$ with

$$HK/H \cong K/H \cap K \quad \text{via} \quad kH \longleftrightarrow k(H \cap K)$$

Proof. To see $HK \subseteq KH$, simply observe $hk = k(k^{-1}hk)$. The converse inclusion is proved similarly. The fact that HK forms a group now follows. The rest are clear. ∎

Example 1.4.4: Product of two subgroups

In general, product of two subgroups needs not to form a group. For example, consider the product of the subgroup H generated by $(1,2) \in S_3$ and the subgroup K generated by $(2,3) \in S_3$. Since $(2,3)(1,2) \notin HK$, we see HK isn't a group.

On the other hand, given two normal subgroups $N, M \trianglelefteq G$. By the preserved-by-conjugations definition of normal subgroups, clearly both NM and $N \cap M$ are normal in G.

1.5 Free Group and Presentation

Equivalent Definition 1.5.1. (Core of a subgroup) Let $H \leq G$. The largest subgroup of H normal in G exists, called the **core** of H. Let $\varphi : G \to \text{Bij}(G/H)$ be the left multiplicative action on the left coset space of H. It is exactly:

$$\ker \varphi = \bigcap_{g \in G} H^g, \quad \text{where } H^g \triangleq gHg^{-1}$$

Proof. Routine. ∎

As we will see, consideration of core is in fact useful in theory of finite group.

Theorem 1.5.2. (Properties of core) Let G be a finite group. Then

(i) $[G : \text{Core}(H)]$ divides $([G : H])!$, for all $H \leq G$

(ii) Any proper subgroup of G of smallest possible index is normal.

Proof. (i) is a consequence of first isomorphism theorem, since we have an injective group homomorphism $G/\text{Core}(H) \hookrightarrow \text{Bij}(G/H)$. (ii) follows from (i), since we would get $\text{Core}(H) = H$. ∎

Equivalent Definition 1.5.3. (Normal closure) Let $S \subseteq G$. Then

$$\langle \{s^g \in G : s \in S, g \in G\} \rangle = \bigcap_{S \subseteq N \trianglelefteq G} N$$

is the smallest normal subgroup of G that contains S, called the **normal closure** of S in G.

Proof. The latter expression is clearly the smallest normal subgroup of G that contains S. $\leq$ part is clear. The only part we need to prove is $\geq$, which requires us to prove the former expression is normal, which is a consequence of computing

$$h(g_1 s_1 g_1^{-1})^{\epsilon_1} \cdots (g_n s_n g_n^{-1})^{\epsilon_n} h^{-1} = (x_1 s_1 x_1^{-1})^{\epsilon_1} \cdots (x_n s_n x_n^{-1})^{\epsilon_n}$$

where $x_i \triangleq hg_1$ if $\epsilon_i = 1$ and hg_i^{-1} if $\epsilon_i = -1$. ∎

Let S be a set. By the **free group generated by** S, we mean a group F_S together with an injective function $i : S \hookrightarrow F_S$ such that for all group G and function $f : S \to G$, there exists a unique group homomorphism $\widetilde{f} : F_S \to G$ that makes the diagram:

15

commutes. Given a set of **relators** $R \subseteq F_S$, by **presentation** $\langle S \mid R \rangle$, we mean the group $F_S / \operatorname{ncl}_{F_S}(R)$. Since kernel is normal, such group clearly satisfies the universal property that for all group G and function $f : S \to G$ such that the kernel of induced group homomorphism $\widetilde{f} : F_S \to G$ contains R, there exists a unique group homomorphism $\widehat{f} : \langle S \mid R \rangle \to G$ that makes the diagram

$$S \xrightarrow{\;\; \pi \circ \iota \;\;} \langle S \mid R \rangle$$

$$f \searrow \qquad \Big\downarrow \widehat{f}$$

$$G$$

commutes.

Example 1.5.4: Dihedral group

The **Dihedral group** D_n is defined by

$$D_n \triangleq \langle r, s \mid r^n = s^2 = e, \, srs^{-1} = r^{-1} \rangle$$

Clearly, every element can be written as $r^a s^b$ with $0 \leq a \leq n-1$ and $b \in \{0, 1\}$. This implies that D_n has at most $2n$ number of elements. To see that $o(D_n) = 2n$, one first consider the group homomorphism $D_n \to \operatorname{GL}_2(\mathbb{C})$ induced by

$$r \mapsto \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \quad \text{and} \quad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where $\xi \triangleq \exp(2\pi i / n)$. Because

$$r^a = \begin{pmatrix} \xi^a & 0 \\ 0 & \xi^{-a} \end{pmatrix} \quad \text{and} \quad r^a s = \begin{pmatrix} 0 & \xi^a \\ \xi^{-a} & 0 \end{pmatrix}$$

We now see that indeed $o(D_n) = 2n$. Moreover, because from the relators, we have the formula

$$(r^a s^b)(r^c s^d) = r^{a + (-1)^b c} s^{b + d}$$

which by direct computation implies $D'_n = \langle r^2 \rangle$. Suppose $r^a s^b \in Z(D_n)$ with $0 \leq a \leq n-1$ and $b \in \{0, 1\}$. Then form the formula, we must have

$$a + (-1)^b c \equiv c + (-1)^d a \pmod{n}, \quad \text{for all } c, d \in \mathbb{Z} \tag{1.1}$$

Because d can be arbitrary, this implies

$$2a \equiv 0 \pmod{n}$$

Clearly we have $D_1 \cong C_2$ and $D_2 \cong C_2 \times C_2$. Therefore, we from now on suppose $n \geq 3$.

Let n be odd. Then clearly $a = 0$. Since $rs \neq sr$ in general, we see that we also must have $b = 0$. We have shown that D_n is centerless for odd $n \geq 3$.

Let n be even. Then we must have $a \in \left\{0, \frac{n}{2}\right\}$. If $a = 0$, then again because $rs \neq sr$ in general, we must have $b = 0$. If $a = \frac{n}{2}$, then from the equation 1.1, regardless of d, we see

$$(-1)^b c \equiv c \pmod{n}, \quad \text{for all } c \in \mathbb{Z}$$

which can only be true if $b = 0$. We have shown that D_n has center $\left\{e, r^{\frac{n}{2}}\right\}$ for even $n \geq 3$. Note that again by direct computation, one can check that the pattern of conjugacy classes differ according to parity of n. Regardless of parity, for fixed $k \in \mathbb{Z}$, the set $\left\{r^{\pm k}\right\}$ form a conjugacy class. If n is odd, then the rest $\{r^t s : 1 \leq t \leq n - 1\}$ forms a class. If n is even, then the rest forms two classes:

$$\{r^r s \in D_n : 1 \leq t \leq n - 1 \text{ is even }\} \cup \{r^t s \in D_n : 1 \leq t \leq n - 1 \text{ is odd }\}$$

1.6 Center and Commutator

Let $S \subseteq G$. Clearly $N_G(S)$ is the largest subgroup in which S is preserved by inner automorphism. Consider its **centralizer** $C_G(S) \triangleq \{g \in G : gs = sg \text{ for all } s \in S\}$. To see that $C_G(S) \trianglelefteq N_G(S)$, one simply observe that $C_G(S)$ is the kernel of the conjugacy action $N_G(S) \longrightarrow \mathrm{Bij}(S)$, where $\mathrm{Bij}(S)$ can be replaced by $\mathrm{Aut}(S)$ if S forms a subgroup G. In such case, first isomorphism theorem gives us an injection

$$N_G(S) / C_G(S) \longhookrightarrow \mathrm{Aut}(S)$$

We call the centralizer of the whole group $Z(G) \triangleq C_G(G)$ **center**.

Equivalent Definition 1.6.1. (Property of center) Let $S \subseteq G$. Then

(i) $S \subseteq Z(G) \iff C_G(S) = G$. (**Equivalent condition to lies in center**)

(ii) $o(G) = o(Z(G)) + \sum [G : C_G(x)]$ (**Class equation**)

(iii) Regardless of G, we always have a natural surjective group homomorphism $G \longrightarrow\!\!\!\rightarrow \mathrm{Inn}(G)$. Such group homomorphism is injective (and thus an isomorphism) if and only if G is centerless.

Proof. Routine. Class equation is a consequence of orbit-stabilizer theorem. ∎

Let $N \trianglelefteq G$. Because $xy \in N$ if and only if $yx \in N$, regardless of notation convention for commutator, we see that

$$[g, h] \in N \iff gN, hN \in G/N \text{ commutes}$$

Therefore, the factor group G/N is abelian if and only if $[G, G] \subseteq N$. In this note, we use $G^{(1)}$ to denote the **commutator subgroup** of G, the subgroup generated by $[G, G]$. From our observation, clearly $G^{(1)}$ is the smallest normal subgroup that makes the quotient abelian. In fact, any subgroup H containing $G^{(1)}$ is normal, since if $ghg^{-1}h^{-1} \in H$, then we clearly have $ghg^{-1} \in H$. We call $G^{\mathrm{ab}} \triangleq G/G^{(1)}$ the **abelianization** of G.

Example 1.6.2: $\mathrm{GL}_2(\mathbb{R})^{(1)} = \mathrm{SL}_2(\mathbb{R})$

Clearly we have $\mathrm{GL}_2(\mathbb{R})^{(1)} \leq \mathrm{SL}_2(\mathbb{R})$. The opposite relation requires computation. Compute

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \left[\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right], \qquad \text{for all } x \in \mathbb{R}$$

Compute that

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} = \left[\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right], \qquad \text{for all } x \in \mathbb{R}^{\times}$$

We now see that for $a \neq 0$, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^{(1)}$$

Compute that

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \left[\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 2 \end{pmatrix} \right]$$

We now see that for $a = 0$, we have

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\frac{d}{b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & b \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^{(1)}$$

Theorem 1.6.3. ("Symmetry" between commutator subgroup and center) Let G be a group and $N \trianglelefteq G$. We have:

(i) If $N \cap G^{(1)} = 1$, then $N \leq Z(G)$.

(ii) Let $C \subseteq G$ be the set of commutators. If $[G : Z(G)] \triangleq n$, then

$$|C| \leq n^2 \quad \text{and} \quad o\left(G^{(1)}\right) \leq n^{2n^3}$$

(iii) Let $G \triangleq \langle g_1, \ldots, g_m \rangle$ be finitely generated. If $o(G^{(1)}) \triangleq n$, then

$$[G : Z(G)] \leq n^m$$

The last two are called **Schur's upper bound**.

Proof. (i): Fix $n \in N$ and $g \in G$. Because N is normal, we know $gng^{-1}n^{-1} \in N$. It then follows from $N \cap G^{(1)} = 1$ that $gng^{-1}n^{-1} = e$, which implies $gn = ng$.

(ii): To prove $|C| \leq n^2$, we show that

$$\begin{cases} aZ(G) = cZ(G) \\ bZ(G) = dZ(G) \end{cases} \implies [a,b] = [c,d]$$

19

The premise gives us $ac^{-1} \in Z(G)$ and $bd^{-1} \in Z(G)$. We then can compute

$$aba^{-1}b^{-1} = aba^{-1}(cc^{-1})b^{-1} = cbc^{-1}b^{-1} = cbc^{-1}b^{-1}(dd^{-1}) = cdc^{-1}d^{-1} \text{ (done)}$$

Before proving the second part, we first prove a necessary lemma:

$$[a,b]^{n+1} = [a,b^2] \cdot [bab^{-1}, b]^{n-1}, \quad \text{for all } a, b \in G$$

The premise $[G : Z(G)] = n$ implies $g^n \in Z(G)$ for all $g \in G$. Therefore, we may compute

$$[a,b]^{n+1} = aba^{-1}[a,b]^n b^{-1} = ab^2 a^{-1} b^{-1}[a,b]^{n-1}b^{-1} = [a,b^2]b[a,b]^{n-1}b^{-1}$$
$$= [a,b^2]\left(b[a,b]b^{-1}\right)^{n-1} = [a,b^2] \cdot [bab^{-1}, b]^{n-1} \text{ (done)}$$

Recall that $C = \{c^{-1} \in G : c \in C\}$. Since $|C| \leq n^2$, to prove $o\left(G^{(1)}\right) \leq n^{2n^3}$, we only have to show that

For all $g \in G^{(1)}$, when written in the form $g \triangleq c_1 \cdots c_m$, where $c_i \in C$, we may require $m \leq n^3$.

Fix g. Let $g \triangleq c_1 \cdots c_m$ with smallest m. We prove such by showing that each c_i can occurs at most n times in the expression $c_1 \cdots c_m$. Assume some c_j occurs $> n$ times in the expression. Because in general, we have

$$z[x,y] = [zxz^{-1}, zyz^{-1}]z^{-1}$$

in groups, we may pull the c_j to the most left in the expression. Then our lemma $[a,b]^{n+1} = [a,b^2] \cdot [bab^{-1}, b]^{n-1}$ gives a contradiction, to the minimality of m. (done)

(iii): Clearly we have

$$Z(G) = \bigcap_{i=1}^{m} C_G(g_i)$$

Orbit-stabilizer theorem says that

$$[G : C_G(g_i)] = |\Gamma|$$

where Γ is the orbit of g_i under the conjugacy action $G \longrightarrow \text{Inn}(G)$. Since $xg_ix^{-1} = [x, g_i]g_i$, for all $x \in G$, we see $|\Gamma| \leq n$. The proof then follows from order formula:

$$[G : Z(G)] = [G : \bigcap_{i=1}^{m} C_G(g_i)] \leq \prod_{i=1}^{m} [G : C_G(g_i)] \leq n^m$$

∎

20

Equivalent Definition 1.6.4. (Abelian group) A group G if **abelian** if any of the followings hold true:

(i) $Z(G) = G$

(ii) $G^{(1)} = 1$

(iii) $g \mapsto g^{-1}$ forms an automorphism.

(iv) $\mathrm{Inn}(G)$ is trivial.

(v) $G/Z(G)$ is cyclic.

Proof. Routine. ∎

> ### Example 1.6.5: Criteria for abelian group
>
> The cyclic criteria of $G/Z(G)$ can not be weaken to that $G/Z(G)$ being abelian. For example, consider D_4. Because $o(Z(D_4)) = 2$, we know $D_4/Z(D_4)$ is abelian, but D_4 isn't.

Corollary 1.6.6. (Finite group with order ≥ 3 has a nontrivial automorphism) If $o(G) \geq 3$, then $\mathrm{Aut}(G)$ is nontrivial.

Proof. If G is non-abelian, then $\mathrm{Inn}(G)$ is non-trivial. If G is abelian, then we have the inversion automorphism. Such inversion automorphism is non-trivial unless all nontrivial elements of G has order 2. In such case, G forms a finite-dimensional $\mathbb{F}_2$-vector space, which allow us to easily find an inversion automorphism. ∎

Theorem 1.6.7. (Abelian criteria for finite group) Let G be a finite group and $\varphi \in \mathrm{Aut}(G)$ be an automorphism that satisfies

$$\left|\{g \in G : \varphi(g) = g^{-1}\}\right| > \frac{3}{4} \cdot o(G)$$

Then G is abelian.

Proof. Denote $S \triangleq \{x \in G : \varphi(x) = x^{-1}\}$. Because of consideration of order, we only have to prove $S \subseteq Z(G)$. Fix $x \in S$. We prove that $C_G(x) = G$. Now, since

$$y^{-1}x^{-1} = \varphi(xy) = \varphi(x)\varphi(y) = x^{-1}y^{-1}, \quad \text{for all } y \in S \cap x^{-1}S$$

we see that $S \cap x^{-1}S \subseteq C_G(x)$. The proof then follows from computing

$$\left|S \cap x^{-1}S\right| = |S| + \left|x^{-1}S\right| - \left|S \cup x^{-1}S\right|$$
$$\geq \frac{3}{2} \cdot o(G) + 2\epsilon - o(G) > \frac{1}{2} \cdot o(G)$$

and consideration of the order. ∎

Example 1.6.8: Lower bound in our abelian criteria for finite group is necessary

Consider

$$D_4 \triangleq \langle r, s \mid r^4 = s^2 = e, srs^{-1} = r^{-1} \rangle$$

There are exactly three quarters of elements of order dividing 2, i.e., $\{e, r^2, rs, r^2s, r^3s\}$. The identity automorphism send them to their inverse, but the group is not abelian.

1.7 Characteristic Subgroups

Equivalent Definition 1.7.1. (Characteristic subgroup) Let G be a group. We say $K \leq G$ is a **characteristic subgroup** and write K char G if any of the followings holds true:

(i) $\varphi(K) \leq K$ for all $\varphi \in \mathrm{Aut}(G)$

(ii) $\varphi(K) = K$ for all $\varphi \in \mathrm{Aut}(G)$.

Proof. (i) $\implies$ (ii) follows from noting $\varphi^{-1}(K) \leq K \leq \varphi^{-1}(K)$. (ii) $\implies$ (i) is clear. ∎

Theorem 1.7.2. (Basic properties of characteristic subgroups) Let G be a group. Then:

(i) If there exists a unique subgroup $H \leq G$ of a fixed index, then H is is characteristic. **(unique subgroup of fixed index is characteristic)**

(ii) If K char $H \trianglelefteq G$, then $K \trianglelefteq G$. **(characteristic subgroup is transitive)**

(iii) If K char H char G, then K char G.

Proof. (i): To show that H is characteristic, we are required to prove $[G : H] = [G : \varphi(H)]$ for all $\varphi \in \mathrm{Aut}(H)$, which follows from checking that $xH \mapsto \varphi(x)\varphi(H)$ forms a well-defined bijection between the left cosets spaces of H and $\varphi(H)$.

(ii) and (iii): Because $H \trianglelefteq G$, every inner automorphism can be restricted $\mathrm{Aut}(H)$. (ii) then follows. The proof for (iii) is the same, in which every automorphism of G can be restricted automorphism of H. ∎

> ### Example 1.7.3: A normal subgroup that isn't characteristic
>
> Consider the additive group of $\mathbb{Q}$. $\mathbb{Z} \leq \mathbb{Q}$ is then normal but not characteristic, since $x \mapsto \frac{1}{2}$ is an automorphism that doesn't preserve $\mathbb{Z}$.

Note that even though normal subgroups need not be preserved by automorphisms, the property of being a normal subgroup is: Given $N \trianglelefteq G$ and $\varphi \in \mathrm{Aut}(G)$, we have $\varphi(N) \trianglelefteq G$.

A subgroup $H \leq G$ is said to be **strictly characteristic** if it is preserved by all surjective endomorphism. If H is moreover preserved by all endomorphism, then we say it is **fully characteristic**. Clearly, centers are all strictly characteristic, and commutator subgroups are all fully characteristic.

Example 1.7.4: A center that isn't fully characteristic

Consider $S_3 \times C_2$. This group has center $1 \times C_2$. The function:

$$(\pi, 0) \mapsto (e, 0) \quad \text{and} \quad (\pi, 1) \mapsto ((1, 2), 0), \quad \text{for all } \pi \in S_3$$

is clearly an endomorphism that doesn't preserve the center.

Notably, given a normal subgroup $N \trianglelefteq G$ and an endomorphism $f \in \text{End}(G)$, in general we can't naturally induce an endomorphism on G/N. If we were to require a subgroup to always allow us to induce endomorphism on its factor group, then we would need it to be fully characteristic. However, when we only want to induce automorphism from an automorphism $f \in \text{Aut}(G)$, a characteristic subgroup clearly suffices. In fact, given a characteristic subgroup $K \,\text{char}\, G$, this gives us a group homomorphism $\text{Aut}(G) \longrightarrow \text{Aut}(G/K)$.

1.8 Semi-Direct Product

Let N, H be two groups and $\varphi : H \to \text{Aut}(N)$ be a group homomorphism. Clearly, when we define a binary operation on $N \times H$ by

$$(n_1, h_1) \cdot (n_2, h_2) \triangleq (n_1 \varphi_{h_1}(n_2), h_1 h_2)$$

We have the **external semidirect product group** $N \rtimes_\varphi H$ in which the inverse of (n, h) is $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$. Remarkably, the automorphism $\varphi_h \in \text{Aut}(N)$ is always the restriction of the inner automorphism $n \mapsto hnh^{-1}$ in the parent group $N \rtimes_\varphi H$. In particular, given a group G, indeed, every automorphism $\psi \in \text{Aut}(G)$ of G is a restriction of the inner automorphism

$$(g, \varphi) \mapsto (e, \psi) \cdot (g, \varphi) \cdot (e, \psi)^{-1}$$

of the **holomorph group** $\text{Hol}(G) \triangleq G \rtimes_{\text{id}} \text{Aut}(G)$.

Theorem 1.8.1. (Universal property of semidirect product) Let N, H be two groups and $\varphi : H \to \text{Aut}(N)$ be a group homomorphism. If group homomorphisms $f : N \to G, g : H \to G$ satisfy

$$f\left(\varphi_h(n)\right) = g(h) f(n) g(h^{-1}), \quad \text{for all } n \in N, h \in H$$

then there exists a unique $k : N \rtimes_\varphi H \to G$ that makes the diagram:

commutes.

Proof. It is routine to check that $k(n, h) \triangleq f(n)g(h)$ suffices. The uniqueness follows from noting $(n, e) \cdot (e, h) = (n, h)$ for all $n \in N$ and $h \in H$. ∎

It is worth mentioning here that direct product is a special case of semidirect product. If $\varphi : H \to \text{Aut}(N)$ is trivial, then $N \rtimes_\varphi H \cong N \times H$. Also, it is not true that every two distinct group homomorphism $\psi, \varphi : H \to \text{Aut}(N)$ must induce distinct semidirect product. For example, given $f \in \text{Aut}(H)$, we have

$$N \rtimes_{\varphi \circ f} H \cong N \rtimes_\varphi H \quad \text{via} \quad (n, f^{-1}(h)) \mapsto (n, h) \tag{1.2}$$

Theorem 1.8.2. (Presentation of semidirect product) Let $N \triangleq \langle X \mid R \rangle, H \triangleq \langle Y \mid S \rangle$ and $\varphi : H \to \operatorname{Aut}(N)$ be a group homomorphism. We have

$$N \rtimes_\varphi H = \langle X \cup Y \mid R, S, yxy^{-1} = w_y(x) \text{ for all } x \in X, y \in Y \rangle$$

where $w_y(x)$ is a fixed word in X that stands for $\varphi_y(x) \in N$.

Proof. See Chapter 10, Section 1, Corollary 1 of the book Presentations of Groups (2nd ed.) by D.L. Johnson. The proof is not difficult, but without his approach, can be rather lengthy and tedious. $\blacksquare$

Example 1.8.3: Classification of semidirect product of $C_8 \rtimes C_2$

Write $\operatorname{Aut}(C_8) \triangleq \{1, 3, 5, 7\}$, so there are four distinct action $C_2 \longrightarrow \operatorname{Aut}(C_8)$ giving us possibly four distinct semidirect product of $C_8 \rtimes C_2$:

$$\langle x, y \mid x^8 = y^2 = e, yxy^{-1} = x^n \rangle, \quad n \in \{1, 3, 5, -1\}$$

Because every word clearly can be written as $x^a y^b$ with $0 \le a \le 7$ and $b \in \{0, 1\}$, regardless of n, and because as a priori, we are already aware that $C_8 \rtimes C_2$ has order 16, we know that indeed the elements $x^a y^b$ are nontrivial unless $a = b = 0$. To see that the four groups are non-isomorphic, one can first use the formula:

$$(x^a y)^2 = x^{a(n+1)}$$

to count the number of elements of order 2, and therefore confirm that the only possible isomorphism is between $n = 1$ and $n = 5$, which is also impossible, since $n = 5$ is clearly non-abelian.

Equivalent Definition 1.8.4. (Recognition theorem for inner semidirect product) Let $N \trianglelefteq G$ and $H \le G$. The followings are equivalent

(i) $G = NH$ and $N \cap H = 1$.

(ii) Every g can be uniquely written as $g = nh$.

(iii) The composition of $\pi : G \twoheadrightarrow G/N$ and $i : H \hookrightarrow G$ forms an isomorphism $H \to G/N$.

(iv) There exists a homomorphism $r : G \to H$, called the **retraction**, that is identity on H and has kernel N. Such retraction then give us a right split sequence

$$1 \longrightarrow N \longrightarrow G \xrightarrow{r} H \longrightarrow 1$$

since $r \circ i = \mathbf{id}_H$.

Proof. (i) $\implies$ (ii) is clear. (ii) $\implies$ (iii): Let $h \in N$. To prove that $H \longrightarrow G/N$ is injective, we are required to show $h = e$. Because $h \in N$, we know $h = eh = he$ implies that $h = e$. Surjectivity is clear.

(iii) $\implies$ (iv): Clearly $r \triangleq (\pi \circ i)^{-1} \circ \pi$ suffices.

(iv) $\implies$ (i): $N \cap H = 1$ is clear. To see that $G = NH$, just observe that $g = gr(g^{-1})r(g)$, where $gr(g^{-1}) \in N$, since $r(gr(g^{-1})) = r(g)r(r(g^{-1})) = r(g)r(g^{-1}) = e$. $\blacksquare$

Suppose $N \trianglelefteq G$ and $H \leq G$ satisfies the conditions in the recognition theorem for inner semidirect product. Defining $\varphi : H \to \mathrm{Aut}(N)$ by $\varphi_h(n) \triangleq hnh^{-1}$, we see that the natural map $N \rtimes_\varphi H \to G$ indeed forms a well-defined group isomorphism. Because of such, when the short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

right splits, we know that

$$G = N \rtimes_\varphi (G/N)$$

Example 1.8.5: Inner semidirect product

Clearly we have a right split sequence:

$$1 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\mathrm{sgn}} C_2 \longrightarrow 1$$

Since the sequence right splits via $g \mapsto (1,2)$, where $C_2 \triangleq \langle g \rangle$, recognition theorem for inner semi-direct product implies:

$$A_n \rtimes_\varphi C_2 \cong S_n, \quad \text{with } \varphi_g(\sigma) \triangleq (1,2)\sigma(1,2)^{-1}$$

where the semi-direct product can be considered internal if we view $C_2 \triangleq \langle (1,2) \rangle \leq S_n$.

Let $\mathbb{F}$ be a field, and view $\mathbb{F}^\times$ as a subgroup of $\mathrm{GL}_n(\mathbb{F})$ by sending $c \mapsto \mathrm{diag}(c, 1, \ldots, 1)$. We see that we have a right split sequence:

$$1 \longrightarrow \mathrm{SL}_n(\mathbb{F}) \longrightarrow \mathrm{GL}_n(\mathbb{F}) \xrightarrow{\det} \mathbb{F}^\times \longrightarrow 1$$

Therefore, recognition theorem for inner semi-direct product implies:

$$\mathrm{SL}_n(\mathbb{F}) \rtimes_\varphi \mathbb{F}^\times \cong \mathrm{GL}_n(\mathbb{F}), \quad \text{with } \varphi_c(A) \triangleq D(c)AD(c^{-1}) \text{ and } D(c) \triangleq \mathrm{diag}(c, 1, \ldots, 1)$$

where the semi-direct product can be considered internal if we view $\mathbb{F}^\times \triangleq \{\mathrm{diag}(c, \ldots, 1)\} \leq \mathrm{GL}_n(\mathbb{F})$.

Note that if H is also normal in G, then the action $\varphi_h(n) = hnh^{-1}$ become trivial, since we would have $[H, N] \subseteq H \cap N = 1$. This agrees with the recognition theorem for direct product.

Equivalent Definition 1.8.6. (Recognition theorem for direct product) Let $N_1, \ldots, N_k$ be normal subgroups of G. We say G is an **internal direct products of** N_i if any of the followings hold true:

(i) The natural map $N_1 \times \cdots \times N_k \to G$ forms a group isomorphism.

(ii) $N_1 \cdots N_k = G$ and $N_i \cap \prod_{j \neq i} N_j = 1$ for all i.

(iii) $N_1 \cdots N_k = G$ and $N_i \cap \prod_{j < i} N_j = 1$ for all i.

Proof. (i) $\implies$ (ii): Clearly we have $N_1 \cdots N_k = G$. Let $n_2 \cdots n_k \in N_1$. Because $n_2 \cdots n_k$ is both the image of $(n_2 \cdots n_k, e, \ldots, e)$ and $(e, n_2, \ldots, n_k)$, by injectivity of the natural map, we know $n_2 = \cdots = n_k = e$.

(ii) $\implies$ (iii) is clear. It remains to show (iii) $\implies$ (i). The proof relies on induction on k. We first prove the base case $k = 2$. Because $[N_1, N_2] \leq N_1 \cap N_2 = 1$, we know the natural map forms homomorphism. Surjectivity is clear. For injectivity, if $n_1 n_2 = e$, then since $n_1 = n_2^{-1} \in N_2$, we know $n_1 = n_2 = e$.

We now prove the inductive case. By the base case, the natural map:

$$(N_1 \cdots N_k) \times N_{k+1} \longrightarrow N_1 \cdots N_k N_{k+1} = G$$

forms a group isomorphism. By inductive hypothesis, the natural map:

$$N_1 \times \cdots \times N_k \longrightarrow N_1 \cdots N_k$$

also forms a group isomorphism. Composing the two together, we get the desired isomorphism. $\blacksquare$

It should be noted that we didn't define internal direct products for infinite index, since the original statement can not be naively generalized to the infinite case. The ill behavior can be seen from multiple aspect. For example, we have

$$\prod_{i \in I} N_i \trianglelefteq \prod_{i \in I} G_i \quad \text{and} \quad \frac{\prod G_i}{\prod N_i} \cong \prod_{i \in I} \frac{G_i}{N_i} \quad \text{and} \quad Z\left(\prod_{i \in I} G_i\right) = \prod_{i \in I} Z(G_i)$$

even if the index set I is infinite, but we only have

$$\left(\prod_{i \in I} G_i\right)^{(1)} \leq \prod_{i \in I}(G_i^{(1)})$$

where the equality holds if I is finite.

Equivalent Definition 1.8.7. (Recognition theorem for direct product for finite group) Let G be a finite group, and let $N_1, \ldots, N_k \trianglelefteq G$ satisfy $G = N_1 \cdots N_k$ and $o(G) = o(N_1) \cdots o(N_k)$. Then G is the internal direct product of N_i.

Proof. The proof is done by induction on k. The base case $k = 1$ is trivial. For the inductive case, one first use the order formula to compute

$$o(N_1) \cdots o(N_k)o(N_1 \cap (N_2 \cdots N_k)) = o(G)o(N_1 \cap (N_2 \cdots N_k)) = o(N_1)o(N_2 \cdots N_k)$$

which gives

$$o(N_1 \cap (N_2 \cdots N_k)) = \frac{o(N_2 \cdots N_k)}{o(N_2) \cdots o(N_k)} \leq 1$$

which by recognition theorem implies G is the internal direct product $N_1 \times (N_2 \cdots N_k)$. The rest then follows from the inductive hypothesis. ∎

Example 1.8.8: The requirement in definitions of internal direct products for groups

Let $G \triangleq C_4 \times C_2$. Clearly the direct product of $\langle (1,0) \rangle$ and $\langle (2,0) \rangle$ is isomorphic to G, but they do not form an internal direct product of G. It is because of such, we must require $N_1 \times \cdots \times N_k$ not only isomorphic to G, but moreover the natural way in definition of internal direct products for groups.

Example 1.8.9: The requirement in definitions of internal direct products for groups

Let $G \triangleq \mathbb{Z} \times \mathbb{Z}$. Clearly $N_1 \triangleq \mathbb{Z} \times \{0\}, N_2 \triangleq \{0\} \times \mathbb{Z}, N_3 \triangleq \{(x,x) \in G : x \in \mathbb{Z}\}$ satisfies

$$G = N_1 N_2 N_3 \quad \text{and} \quad N_1 \cap N_2 = N_1 \cap N_3 = N_2 \cap N_3 = 1$$

Yet, later we will see that we can never have a group isomorphism $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. This is why we must require $N_i \cap \prod_{j \neq i} N_j = 1$ in the definition internal direct product.

Example 1.8.10: Subgroups are not products of intersections.

In general, we don't have

$$H \leq G_1 \times \cdots \times G_k \implies H = (G_1 \cap H) \times \cdots \times (G_k \cap H)$$

even in the category of abelian group. For example, consider $H \triangleq \{(x,x) \in \mathbb{Z}^2 : x \in \mathbb{Z}\}$.

1.9 Structure Theorem for Finitely Generated Abelian Groups

Theorem 1.9.1. (Change of basis for finitely generated abelian group) Let $k \in \mathbb{N}$, $G = \langle x_1, \ldots, x_k \rangle$ be abelian and $c_1, \ldots, c_k \in \mathbb{N}$ satisfies $\gcd(c_1, \ldots, c_k) = 1$. Then there exists $y_1, \ldots, y_k \in G$ such that $G = \langle y_1, \ldots, y_k \rangle$ and $y_1 = c_1 x_1 + \cdots + c_k x_k$.

Proof. Such is proved via induction on $s \triangleq c_1 + \cdots + c_k$. The base case $s = k$ is clear. We now prove the inductive case. Because $\gcd(c_1, \ldots, c_k) = 1$, by changing the order if necessary, we may write $c_1 > c_2$. Now, because $\gcd(c_1 - c_2, c_2, \ldots, c_k) = 1$ and $G = \langle x_1, x_2 - x_1, x_3, \ldots, x_k \rangle$, we see by inductive hypothesis that there exists $y_1, \ldots, y_k$ such that $G = \langle y_1, \ldots, y_k \rangle$ and

$$\begin{aligned} y_1 &= (c_1 - c_2)x_1 + c_2(x_2 + x_1) + \cdots + c_k x_k \\ &= c_1 x_1 + \cdots + c_k x_k \end{aligned}$$

as desired. ∎

Theorem 1.9.2. (Structure theorem for finitely generated abelian group) Let G be a finitely generated abelian group. Then we may write:

$$G \cong C_{n_1} \times \cdots \times C_{n_s} \times \mathbb{Z}^r$$

for $n_i \geq 2$. Moreover, we know that

(i) Such r is unique, called the **rank** of G.

(ii) Under the assumption that n_i each is a power of some prime, the expression exists and is unique, called the **primary decomposition form**.

(iii) Under the assumption that $n_i \mid n_{i+1}$ for all i, the expression exists and is unique, called the **invariant factor form**.

Proof. We first show the existence via induction on the number of generators. The base case is clear. Suppose that the existence holds true for any abelian group that has a generating set of cardinality $k - 1$, and suppose that G has a generating set $\{x_1, \ldots, x_k\}$ where x_1 has order smaller than any elements of any generating sets of cardinality k.

By inductive hypothesis, we only have to show that G is an internal direct product of $\langle x_1 \rangle$ and $\langle x_2, \ldots, x_k \rangle$. Assume not for a contradiction. Then there exists $m_1 \neq 0$ such that $m_1 x_1 + m_2 x_2 + \cdots + m_k x_k = 0$. By possibly changing sign of some of the x_i and exchanging the order, we may suppose $m_1 < o(x_1)$ and $m_1, \ldots, m_t \in \mathbb{N}$ and $m_{t+1} = \cdots = m_k = 0$.

Let $c_i \triangleq \frac{m_i}{\gcd(m_1,\ldots,m_t)}$ for all $i \in \{1,\ldots,t\}$. By theorem 1.9.1, we know there exists $y_1,\ldots,y_t \in G$ such that $\langle y_1,\ldots,y_t \rangle = \langle x_1,\ldots,x_t \rangle$ with $y_1 = c_1 x_1 + \cdots + c_t x_t$. Clearly, we have $G = \langle y_1,\ldots,y_t,x_{t+1},\ldots,x_k \rangle$. Compute

$$\gcd(m_1,\ldots,m_t)y_1 = m_1 x_1 + \cdots + m_t x_t = 0$$

We now see $o(y_1) \le m_1 < o(x_1)$, a contradiction to the choice that x_1 has the smallest order. (done)

(i): Fix an expression of G, and let p be a prime that satisfies $p \nmid n_i$ for all i. The rest then follows from checking that $G/pG \cong C_p^r$.

(ii): The existence follows from noting that

$$\gcd(m,n) = 1 \implies C_{mn} \cong C_m \times C_n$$

The uniqueness follows from noting that given a primary decomposition form whose p-part has the form $C_{p^{n_1}} \times \cdots \times C_{p^{n_k}}$, then the **torsion p-subgroup G_{T_p} of G**

$$G_{T_p} \triangleq \{x \in G : o(x) = p^n \text{ for some } n \ge 0\}$$

is

$$G_{T_p} \cong C_{p^{n_1}} \times \cdots \times C_{p^{n_k}}$$

and that

$$\frac{p^{d-1}C_{p^{n_i}}}{p^d C_{p^{n_i}}} \cong \begin{cases} C_p & \text{if } d-1 < n_i \\ 1 & \text{if } d-1 \ge n_i \end{cases}$$

(iii): Both the existence and uniqueness of invariant factor form follows form that of primary decomposition form: Just consider that C_{n_s} can only be $C_{p_1}^{d_1} \times \cdots \times C_{p_m}^{d_m}$, where p_i non-repeatedly running through all the occurring prime with d_i being the highest exponential. ∎

Structure theorem for finitely generated abelian group in fact also gives a structure theorem for automorphism group of finite abelian group. See this paper. A particular case is that

$$\mathrm{Aut}(C_p^n) \cong \mathrm{GL}_n(\mathbb{F}_p)$$

Corollary 1.9.3. (Finite abelian group has subgroups of all possible order) Let G be a finite abelian group with $m \mid o(G)$. Then there exists subgroup of G of order m.

Proof. The proof follows from the primary decomposition form and the fact that for all $e < d \in \mathbb{N} \cup \{0\}$,

$$\{0, p^{d-e}, \ldots, (p^e - 1)p^{d-e}\} \subseteq C_{p^d}$$

is a subgroup of C_{p^d} of order p^e. ∎

Theorem 1.9.4. (Subgroup of finitely generated abelian group) Let G be a finitely generated abelian group that has rank r whose p-part is

$$G_{T_p} \cong C_{p^{n_1}} \times \cdots \times C_{p^{n_k}}, \quad \text{with } n_1 \geq \cdots \geq n_k$$

Then for any subgroup $H \leq G$, if we write

$$H_{T_p} \cong C_{p^{d_1}} \times \cdots \times C_{p^{d_s}}, \quad \text{with } d_1 \geq \cdots \geq d_s$$

then the rank of H is $\leq r$, and we have $s \leq k$ and $n_i \geq d_i$ for all i.

Proof. Clearly we have $H_{T_p} \leq G_{T_p}$. Consider $\Omega_1(H_{T_p}) \triangleq \{h \in H_{T_p} : h^p = e\}$. Clearly, we have

$$C_p^s \cong \Omega_1(H_{T_p}) \leq \Omega_1(G_{T_p}) \cong C_p^k$$

Therefore, by counting order, we see that indeed $s \leq k$. The rest is

$$C_p^{\text{card}\{\geq d_i\}} \cong \Omega_1(p^{d_i-1}H_{T_p}) \leq \Omega_1(p^{d_i-1}G_{T_p}) \cong C_p^{\text{card}\{\geq d_i\}}$$

We now prove that H has rank $\leq r$. Let t be the rank of H and q be a prime not in the decomposition. Since

$$\mathbb{Z}^t \cong qH \leq qG \cong \mathbb{Z}^r$$

We have an injective group homomorphism $f : \mathbb{Z}^t \to \mathbb{Z}^r$. Denote the group homomorphism by a r-by-t matrix $A \in M_{r \times t}(\mathbb{Z})$. The injectivity of f then means $Av = 0 \implies v = 0$ for all $v \in \mathbb{Z}^s$. Let $w \in \mathbb{Q}^t$ and $m \gg 0$ be a natural number large enough so that $mw \in \mathbb{Z}^t$. We then see

$$Aw = 0 \implies Amw = mAw = 0 \implies mw = 0 \implies w = 0$$

In other words, the matrix $A \in M_{r \times t}(\mathbb{Q})$ has rank r, which is only possible given that $t \leq r$. ∎

32

1.10 Sylow theorems

In this section, we prove Sylow theorems using combinatorics. Note that first Sylow theorem also shows that indeed as one might expect: Every p-subgroup of a finite group is a subgroup of some Sylow p-subgroup.

Theorem 1.10.1. (Combinatorial facts) Let p be prime. Then:

(i) Given $m \geq r \in \mathbb{N} \cup \{0\}$ with $t \in \mathbb{N}$ coprime with p, the natural number $\binom{p^m t}{p^r}$ has p-part p^{m-r}.

(ii) We have

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}$$

when we write $m = m_k p^k + \cdots + m_0 p^0$ and $n = n_k p^k + \cdots + n_0 p^0$. This is called **Lucas modulo binomial formula**.

Proof. (i) follows from noting that

$$\binom{p^m t}{p^r} = \frac{p^m t (p^m t - 1) \cdots (p^m t - (p^r - 1))}{p^r (p^r - 1) \cdots (p^r - (p^r - 1))}$$

and that for all $i \in \{1, \ldots, p^r - 1\}$, the three natural number $\{i, p^m t - i, p^r - i\}$ share the same p-part.

(ii): Let M be a set of m elements. Partition M into m_i cycles of length p^i, i.e.,

$$M \triangleq \bigcup_{i=0}^{k} \bigcup_{j=1}^{m_i} \Gamma_{i,j}, \quad \text{where } |\Gamma_{i,j}| = p^i$$

Because of such, we see that M can be acted on by the group

$$G \triangleq \prod_{i=0}^{k} \overbrace{C_{p^i} \times \cdots \times C_{p^i}}^{m_i}$$

Clearly, G also acts on the set X of the set of subsets of M that has n elements. Because G is a p-group, orbit-stabilizer theorem tell us that

$$\binom{m}{n} = |X| \equiv |\text{Fix}(G)| \pmod{p}$$

where $\mathrm{Fix}(G)$ is the set of elements of X fixed by all $g \in G$. Because of uniqueness of representation in base p, we know that elements of $\mathrm{Fix}(G)$ are exactly those subsets of X that contains n_i cycles of length p^i. The proof now follows from directly computing that $|\mathrm{Fix}(G)| = \prod_{i=0}^{k} \binom{m_i}{n_i}$. ∎

Theorem 1.10.2. (First and Third Sylow theorem, Wielandt's proof) Let G be a finite group of order $p^m t$ with $\gcd(p, t) = 1$. Let $1 \leq r \leq m$. Then the number n_p of p-subgroup with order p^r satisfies

$$n_p \equiv 1 \pmod{p}$$

Proof. Let X be the set of subset of G with cardinality p^r. Our goal is to find all elements of X that forms a group. Clearly we may define a left G-action on X be setting

$$g \cdot \{x_1, \ldots, x_{p^r}\} \triangleq \{gx_1, \ldots, gx_{p^r}\}$$

Let Γ be an orbit. If Γ contains a group, then we see that Γ is the left coset space of that group, containing exactly one group and satisfying $|\Gamma| = p^{m-r} t$. If Γ doesn't contain any group, there still exists some $S \in \Gamma$ such that $e \in S$, and clearly we will have $\mathrm{Stab}(S) \subseteq S$. Because S isn't a group, we see $p^r = |S| > o(\mathrm{Stab}(S))$, which by orbit-stabilizer theorem implies that $|\Gamma| = [G : \mathrm{Stab}(S)] = p^{m-r+c} t$ for some $c \geq 1$.

In summary, by counting orbit, we have shown that:

$$\binom{p^m t}{p^r} = |X| = n_p p^{m-r} t + l p^{m-r+1} t, \quad \text{for some } l \in \mathbb{N}$$

Let $ut \equiv 1 \pmod{p}$. Recalling that $\binom{p^m t}{p^r}$ has p-power p^{m-r}, it remains to show

$$u \cdot \frac{\binom{p^m t}{p^r}}{p^{m-r}} \equiv 1 \pmod{p}$$

which follows from noting:

$$u \cdot \frac{\binom{p^m t}{p^r}}{p^{m-r}} = ut \cdot \binom{p^m t - 1}{p^r - 1} \equiv \binom{p^m t - 1}{p^r - 1} \equiv 1 \pmod{p}$$

where the last equality follows from Lucas modulo binomial formula and the observation that

$$p^m t - 1 = t_k p^{m+k} + \cdots + (t_0 - 1)p^m + (p-1)p^{m-1} + \cdots + (p-1)p^0$$

where $t = t_k p^k + \cdots + t_0 p^0$ with $t_0 > 0$. ∎

34

Corollary 1.10.3. (Every p-subgroup is contained by some Sylow p-subgroup) Let G be a finite group and $H \leq G$ a p-group. Then H must be contained by some Sylow p-subgroup of G.

Proof. Consider the conjugacy action $H \longrightarrow \mathrm{Bij}\left(\mathrm{Syl}_p(G)\right)$. First Sylow theorem and orbit-stabilizer theorem shows that there must be a singleton orbit. Let that singleton be P.

We claim $H \leq P$. Because $\{P\}$ is a singleton orbit of the conjugacy action, we know $H \leq N_G(P)$. Then by second isomorphism theorem, we see that HP is a group such that $HP/P \cong H/H \cap P$. This implies that HP is a p-group. The fact HP contains P forces $P = HP$, which implies $H \leq P$. ∎

Before proving Second Sylow theorem, we need a lemma for actions of p-groups.

Lemma 1.10.4. (Counting lemma for p-group) Let G be a p-group acting on a finite set X. Then

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

where $\mathrm{Fix}(G) \triangleq \{x \in X : gx = x \text{ for all } g \in G\}$ is the set of points fixed by all $g \in G$.

Proof. This is a consequence of orbit-stabilizer theorem. ∎

Theorem 1.10.5. (Second Sylow theorem) Sylow p-subgroups are conjugated to each other.

Proof. Let H and P be two Sylow p-subgroups of G, and let H acts on left coset space of P by left multiplication. Because P is Sylow, by counting lemma for p-group, we know the number of fixed points gP is nonzero. Let gP be a fixed point. We then see that, as desired, $g^{-1}hg \in P$ for all $h \in H$, since $hgP = gP$. ∎

Even without third Sylow theorem, second Sylow theorem already gives some interesting applications.

Corollary 1.10.6. (Normalizers of Sylow subgroups Don't satisfy normalizer condition) Let G be a finite group and $P \in \mathrm{Syl}_p(G)$. Then

$$N_G(P) = N_G(N_G(P))$$

Proof. Let $x \in N_G(N_G(P))$. We are required to show $x \in N_G(P)$. By definition, we have

$$xPx^{-1} \leq xN_G(P)x^{-1} = N_G(P)$$

In other words, both P and xPx^{-1} are Sylow p-subgroup of $N_G(P)$. Therefore, by second Sylow theorem, there exists some $y \in N_G(P)$ such that

$$xPx^{-1} = yPy^{-1} = P$$

This then implies $x \in N_G(P)$. ∎

Corollary 1.10.7. (Restriction of conjugacy classes onto normalizer of Sylow subgroups, on element of center of Sylow subgroups) Let G be a finite group, $P \in \mathrm{Syl}_p(G)$, and $a, b \in Z(P)$. If a, b are conjugate in G, then they are conjugate in $N_G(P)$.

Proof. Write $b = xax^{-1}$ with $x \in G$. By definition, we have

$$(x^{-1}gx)a(x^{-1}gx)^{-1} = x^{-1}gbg^{-1}x = x^{-1}bx = a, \quad \text{for all } g \in P$$

In other words, $x^{-1}Px \leq C_G(a)$. Then since both P and $x^{-1}Px$ are Sylow p-subgroup of $C_G(a)$, by second Sylow theorem, we know there exists $y \in C_G(a)$ such that $P = y^{-1}x^{-1}Pxy$. We now see that $xy \in N_G(P)$ and $(xy)a(xy)^{-1} = b$, as desired. ∎

Second Sylow theorem moreover stated that given $n_p > 1$, the conjugacy action $G \longrightarrow \mathrm{Bij}(\mathrm{Syl}_p(G)) \cong S_{n_p}$ is nontrivial, and thus injective when G is simple. This is a trick particularly useful to classify finite simple group.

Theorem 1.10.8. (Remaining part of third Sylow theorem) Let G be a finite group, and let n_p be the number of Sylow p-subgroup of G. For all Sylow p-subgroup P of G, we have

$$n_p = [G : N_G(P)]$$

Proof. This is a consequence of second Sylow theorem and orbit stabilizer theorem, where we note that when G acts on $\mathrm{Syl}_p(G)$ by conjugation we have $\mathrm{Stab}(P) = N_G(P)$. ∎

1.11   Nilpotency and Solvability

A **normal series** of a group G is a finite chain of subgroups:

$$1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n \trianglelefteq G_{n+1} \trianglelefteq \cdots \trianglelefteq G$$

where each G_n is normal only G_{n+1}, but not necessarily G. A **composition series** is a maximal normal series.

Example 1.11.1: Subgroups in normal series need not all be normal

Consider

$$D_4 \triangleq \langle r, s \mid r^4 = s^2 = e, srs^{-1} = r^{-1} \rangle$$

We have normal series

$$\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_4$$

where normality follows from index 2. Clearly $\langle s \rangle$ is not normal in D_4.

Equivalent Definition 1.11.2. (Solvable groups) We say a group G is **solvable** if any of the followings holds true:

(i) G admits a finite normal series whose factor groups are all abelian.

(ii) The **derived series**

$$\cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} \triangleq G, \quad \text{where } G^{(k+1)} \triangleq \langle [G^{(k)}, G^{(k)}] \rangle$$

reach to 1.

Proof. Routine. Note that if $1 = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$ is a normal series whose factor groups are all abelian, then clearly we have $G^{(k)} \leq G_k$. ∎

Clearly, solvable groups are closed under **group extension**. Given a short exact sequence of groups

$$1 \longrightarrow A \longrightarrow G \longrightarrow B \longrightarrow 1$$

If A and B are both solvable, then G is solvable. Conversely, let G be solvable and $H \leq G$. Then clearly

$$1 = G^{(n)} \cap H \trianglelefteq \cdots \trianglelefteq G^{(1)} \cap H \trianglelefteq H$$

is normal series whose factor groups are all abelian. Because of such, we say solvable groups are **subgroup-closed**. Let $N \trianglelefteq G$ and $\pi : G \to G/N$ be the natural projection. Since

$\pi\left(G^{(k)}\right)$ is the derived series of G/N, we see that solvable groups are also **quotient-closed**. Since taking direct product and taking commutator subgroup commutes, we moreover have

$$\left(\prod_{i=1}^{n} G_i\right)^{(k)} = \prod_{i=1}^{n} G_i^{(k)}$$

Therefore, solvable groups are also **finite direct product-closed**.

Equivalent Definition 1.11.3. (Finite solvable groups) A finite group G is solvable if and only if it admits a composition series whose factor group are all cyclic of prime order.

Proof. Routine. ∎

Equivalent Definition 1.11.4. (Nilpotent groups) We call a group G **nilpotent** if G admits a **central series**, a normal series:

$$1 = G_0 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that

$$[G, G_k] \leq G_{k-1}, \quad \text{for all } k \in \{1, \ldots, n\}$$

Clearly, all G_k are normal in G. Given a series of normal subgroups, we then clearly see that it is central if and only if

$$\frac{G_k}{G_{k-1}} \leq Z\left(\frac{G}{G_{k-1}}\right), \quad \text{for all } k \in \{1, \ldots, n\}$$

A group is nilpotent if and only if its **lower central series**:

$$\cdots \trianglelefteq G_{(2)} \trianglelefteq G_{(1)} \trianglelefteq G_{(0)} \triangleq G, \quad \text{where } G_{(k)} \triangleq [G, G_{(k-1)}] \text{ for all } k \in \mathbb{N}$$

reach to 1. A group is nilpotent if and only if its **upper central series**:

$$1 \triangleq Z_{(0)} \trianglelefteq Z_{(1)} \trianglelefteq Z_{(2)} \trianglelefteq \cdots, \quad \text{where } \frac{Z_{(k+1)}}{Z_{(k)}} \triangleq Z\left(\frac{G}{Z_{(k)}}\right) \text{ for all } k \in \mathbb{N}$$

reach to G. The central series $1 = G_0 \triangleleft \cdots \triangleleft G_n = G$ is said to have **length** n. The **nilpotency class** of a nilpotent group is the smallest length of its central series. If a group is nilpotent, then both its lower and upper central series has length of its nilpotent class.

Proof. Clearly both lower and upper central series are central by definition. Suppose a central series

$$1 = G_0 \trianglelefteq \cdots \trianglelefteq G_n = G$$

exists. To see the lower central series reach to 1 with smallest length, use induction to show $G_{(k)} \leq G_{n-k}$ for all k. (thus the name **fastest descending series**). To see the upper central series reach to G with smallest length, use induction to show $G_k \leq Z_{(k)}$ for all k. (thus the name **fastest ascending series**) ∎

Clearly, every nilpotent group is solvable, but solvable group need not be nilpotent.

> **Example 1.11.5: A solvable group that isn't nilpotent**
>
> Consider S_3. Because S_3 is the extension of C_3 and C_2:
>
> $$1 \longrightarrow A_3 \longrightarrow S_3 \longrightarrow C_2 \longrightarrow 1$$
>
> We know S_3 is solvable. However, since S_3 clearly has 3 Sylow 2-subgroups and finite nilpotent group has normal Sylow subgroups, we know S_3 isn't nilpotent.

Again, one can check that central series are closed under taking intersection with a subgroup, under taking finite direct product and under surjective group homomorphism, so nilpotency is also subgroup-closed, quotient-closed and finite-direct-product-closed.

Theorem 1.11.6. (Proper subgroups of nilpotent groups satisfy normalizer condition) If G is nilpotent, then any $H < G$ satisfies normalizer condition.

Proof. Note that if H doesn't contain $Z(G)$, then the elements of $Z(G)$ that lies outside H complete the proof, so we only have to consider the case $Z(G) \leq H$.

This is proved by induction on nilpotency class n of G. The base case $n = 1$ is clear. The inductive case follows from third isomorphism theorem for groups and the observation $G/Z(G)$ has the nilpotent class one smaller than that of G. $\blacksquare$

Theorem 1.11.7. (Properties of finite p-groups) Let P be a finite p-group. Then:

(i) P has nontrivial center.

(ii) P is nilpotent.

(iii) Groups of order p^2 is either $C_p \times C_p$ or C_{p^2}.

(iv) Groups of order p^3, if not abelian, must satisfies $o(Z(G)) = p$ and $Z(G) = G^{(1)}$.

(v) Nontrivial normal subgroup $1 < N \trianglelefteq P$ satisfies $N \cap Z(P) > 1$.

Proof. (i) is a consequence of class equation. Both (ii) and (iii) follows from (i). If the center of a group of order p^2 has order p, then a contradiction about abelian occurs. Let G be a group of order p^3. The fact $o(Z(G)) = p$ also follows from (i) and same abelian contradiction. The fact $G^{(1)} = Z(G)$ follows from definition of abelian group and the fact that (ii) implies $G/Z(G)$ is abelian. We have shown (iv).

Lastly, we prove (v). Let P acts on N by conjugation. By our counting lemma for p-group, we have

$$0 \equiv o(N) \equiv \left|\{n \in N : gng^{-1} = n \text{ for all } g \in P\}\right| \pmod{p}$$

Noting that the latter set $= N \cap Z(P)$, we now see $N \cap Z(P) > 1$. ∎

> **Example 1.11.8: Infinite p-group**
>
> The **Prüfer group** $\mathbb{Z}(p^\infty)$ is defined by
>
> $$\mathbb{Z}(p^\infty) \triangleq \{\exp(2\pi i m/p^n) \in \mathbb{C} : m \in \mathbb{Z} \text{ and } n \in \mathbb{N}\}$$
>
> It is an infinite group whose every nontrivial element has order p^n for some $n \in \mathbb{N}$.

Equivalent Definition 1.11.9. (Finite nilpotent group) Let G be a finite group. The followings are equivalent:

(i) G is nilpotent.

(ii) Proper subgroups of G satisfies normalizer condition.

(iii) Sylow subgroups of G are all normal.

(iv) G is the internal direct product of its Sylow subgroups.

Proof. (i) $\implies$ (ii): This is true even if G is infinite.

(ii) $\implies$ (iii): If G is a p-group, then the proof is trivial. Let G not be a p-group and let $P \in \mathrm{Syl}_p(G)$. To see P is normal, just observe that since normalizers of Sylow subgroups don't satisfy normalizer condition, the normalizer of P must be G.

(iii) $\implies$ (iv): This follows from the definition of finite internal direct product.

(iv) $\implies$ (i): This follows from the fact that p-groups are nilpotent and that nilpotency is closed under taking finite direct product. ∎

1.12   Old Numbers

Abstract

This section proves some elementary number theory that are in essence group theory.

Theorem 1.12.1. (Group property of totient function) Let ϕ be the Euler totient function. Then

$$n \mid \phi(a^n - 1), \quad \text{for all } a, n \in \mathbb{N}$$

Proof. This is a consequence of the fact that $a \in \mathbb{Z}_{a^n-1}^{\times}$ and that a has order n in the group. ∎

Before the first application, we first show that:

Theorem 1.12.2. ($\mathbb{Z}_p^{\times}$ is cyclic) Let p be prime. Then the unit group $\mathbb{Z}_p^{\times}$ is cyclic.

Proof. We are required to show the existence of elements of order $p - 1$. Let l be the least common multiple of orders of all elements, so $x^l - 1 \in \mathbb{Z}_p[x]$ has $p - 1$ distinct roots in $\mathbb{Z}_p$. This implies $l \geq p - 1$. Because the group is abelian, we now see from its primary decomposition form that indeed it is cyclic. ∎

Theorem 1.12.3. (Group theoretic side of Wilson's theorem) Let p be prime. Then

$$(p - 1)! \equiv -1 \pmod{p}$$

Proof. Consider the symmetric group S_p. The proof follows from $n_p \equiv 1 \pmod{p}$ and directly counting that $n_p = (p - 2)!$. This is easy to count, since the Sylow p-group of S_p are those generated by a single p-cycle. ∎

Theorem 1.12.4. (Wolstenholme's theorem) Let p be an odd prime, and write

$$H(p - 1) \triangleq 1 + \frac{1}{2} + \cdots + \frac{1}{p - 1} \in \mathbb{Q}$$

Then

$$H(p - 1) \equiv 0 \pmod{p^2}$$

Proof. Because p is odd, we can group the terms of $H(p - 1)$ by pairs:

$$H(p - 1) = \left(1 + \frac{1}{p - 1}\right) + \left(\frac{1}{2} + \frac{1}{p - 2}\right) + \cdots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{p - \frac{p-1}{2}}\right)$$

41

Reduce each pair to a common denominator:

$$H(p-1) = \frac{p}{p-1} + \frac{p}{2(p-2)} + \cdots + \frac{p}{\frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right)}$$

We then can write

$$H(p-1) \triangleq p \cdot \frac{A}{(p-1)!} \tag{1.3}$$

where

$$A \triangleq \frac{(p-1)!}{p-1} + \frac{(p-1)!}{2(p-2)} + \cdots + \frac{(p-1)!}{\frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right)}$$

Since $p \nmid (p-1)!$, equation 1.3 reduce the proof into proving $p \mid A$. We first show that

$\frac{(p-1)!}{a(p-a)} \equiv a^{-2} \pmod{p}$, for $a \in \{1, \ldots, p-1\}$, where the power a^{-2} occurs in the cyclic group $\mathbb{Z}_p^\times \cong C_{p-1}$.

Denote $x \triangleq \frac{(p-1)!}{a(p-a)} \in \mathbb{Z}$, so by Wilson's theorem, we have

$$a(p-a)x = (p-1)! \equiv -1 \pmod{p}$$

which gives us

$$a^2 x \equiv 1 \pmod{p} \text{ (done)}$$

We may now write

$$A \equiv 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} \pmod{p}$$

Because p is odd, we only have to prove $2A \equiv 0 \pmod{p}$:

$$2A \equiv 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} + 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2}$$

$$\equiv 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} + (-1)^{-2} + \cdots + \left(-\frac{p-1}{2}\right)^{-2}$$

$$\equiv 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} + \left(\frac{p+1}{2}\right)^{-2} + \cdots + (p-1)^{-2}$$

Since the inversion $x \mapsto x^{-1}$ forms a bijection in $\mathbb{Z}_p^\times$. Therefore, we have

$$2A \equiv 1^2 + \cdots + (p-1)^2$$
$$= \frac{p(p-1)(2p-1)}{6} \equiv 0 \pmod{p}$$

$\blacksquare$

42

1.13 Symmetric Groups

Abstract

This section develop some common sense about symmetric groups.

Given the **symmetric group** S_n, to define parity, the fastest way is to realize it as the **group of permutation matrix**, and then call those that have determinant 1 **even**, while those that have determinant -1 **odd**. Clearly we have the **alternating group**

$$A_n \triangleq \{g \in S_n : \det(g) = 1\}$$

To see that $[S_n : A_n] = 2$ for all $n \geq 2$, just consider that for any $g \in S_n - A_n$, we have a bijection between A_n and $S_n - A_n$ defined by

$$a \mapsto ag$$

By direct observation, we see that every permutation has a fixed **cycle type**. Because

$$\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$$

we see that the conjugacy classes of S_n coincides with cycle type classes.

At this point, it is worth mentioning that, given $g \in S_n$, even though we are definitely aware of what its centralizer is, in the sense that given any $h \in S_n$, we can immediately tell whether $h \in C_{S_n}(g)$, but to actually describe $C_{S_n}(g)$ may be annoying. See this MSE post.

> **Example 1.13.1: Conjugacy classes of A_n are either half a cycle type or all.**
>
> Recall that conjugacy classes is just the orbit of conjugacy action, and orbit-stabilizer theorem links the orbit Γ of an element x with its stabilizer group by
>
> $$|\Gamma| = [G : \mathrm{Stab}(x)]$$
>
> Now, since we clearly have
>
> $$\mathrm{Stab}_{A_n}(x) = A_n \cap \mathrm{Stab}_{S_n}(x)$$
>
> if $\mathrm{Stab}_{S_n}(x) \leq A_n$, then the conjugacy class of x in A_n is the half of its conjugacy class in S_n. On the other hand, if $\mathrm{Stab}_{S_n}(x) \nleq A_n$, then since $A_n \cdot \mathrm{Stab}_{S_n}(x) = S_n$, by order formula, we know $[A_n : \mathrm{Stab}_{A_n}(x)] = [S_n : \mathrm{Stab}_{S_n}(x)]$, which implies that the conjugacy class of x in A_n is the same as in S_n.

Theorem 1.13.2. (S_n **is centerless for** $n \geq 3$) Let $n \geq 3$. Then $Z(S_n) = 1$.

Proof. Let $\tau \neq e \in S_n$. Because τ is nontrivial, we know $\tau(i) = j$ for some $i \neq j$. Let $\sigma(i) = i$ and $\sigma(j) \neq j$. We now see $\sigma \circ \tau \circ \sigma^{-1} \neq \tau$, as desired. ■

Theorem 1.13.3. (Generators of S_n**)** Let $n \geq 2$. Then S_n can be generated by any of the followings:

(i) transpositions.

(ii) $\{(1, k) \in S_n : 2 \leq k \leq n\}$.

(iii) $\{(1, 2), (1, \ldots, n)\}$.

Proof. (i) follows from:

$$(1, \ldots, k) = (2, 3)(3, 4) \cdots (k - 2, k - 1)(k - 1, k)(1, k)$$

(ii) then follows from:

$$(i, j) = (1, i)(1, j)(1, i)^{-1}$$

To prove (iii), we then only have to prove that (ii) can be generated by (iii), which is done by two inductions, with one of them being

$$(k, k + 1)(1, k)(k, k + 1)^{-1} = (1, k + 1)$$

while the other being

$$g(i, i + 1)g^{-1} = (i + 1, i + 2), \quad \text{for all } i \leq n - 2$$

where we denote $g \triangleq (1, \ldots, n)$. ■

Theorem 1.13.4. (A_n **are generated by 3-cycles for** $n \geq 3$**)** Let $n \geq 3$. Then A_n is generated by 3-cycles.

Proof. Such is proved via induction on n. The base case is clear. We now prove the inductive case. Let $\sigma \in A_n$. By inductive hypothesis, if σ doesn't move n, then σ can be generated by 3-cycles. If σ move n, then because inverse of a 3-cycle is a 3-cycle, and because there exists a 3-cycle τ such that $\tau \circ \sigma$ fix n, we see σ can also be generated by 3-cycles. ■

Theorem 1.13.5. ($S_n^{(1)} = A_n$ **for** $n \geq 3$**)** Let $n \geq 3$. Then $S_n^{(1)} = A_n$.

Proof. $S_n^{(1)} \leq A_n$ follows from computation. Because A_n is generated by 3-cycles, to show $S_n^{(1)} = A_n$, we only have to show $S_n^{(1)}$ contains all 3-cycles, which follows from computing

$$(a, b, c) = [(a, b), (a, c)]$$

■

We are now ready to prove that A_n is simple for $n \geq 5$.

Theorem 1.13.6. (Simplicity of A_n) A_3 is a simple group. A_4 is not a simple group, since it has the characteristic 2-Sylow subgroup:

$$\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \tag{1.4}$$

Let $n \geq 5$. Then A_n is simple.

Proof. Simplicity of A_3 follows from $o(A_3) = 3$. We now prove (ii): There are three ways to partition $\{1, 2, 3, 4\}$ into 2 disjoint subsets, each of cardinality 2, i.e.,

$$\Pi_1 \triangleq \{\{1, 2\}, \{3, 4\}\} \quad \text{and} \quad \Pi_2 \triangleq \{\{1, 3\}, \{2, 4\}\} \quad \text{and} \quad \Pi_3 \triangleq \{\{1, 4\}, \{2, 3\}\}$$

Clearly, S_4 acts on $\{\Pi_1, \Pi_2, \Pi_3\}$, that is, $S_4 \longrightarrow \mathrm{Sym}(\{\Pi_1, \Pi_2, \Pi_3\}) \cong S_3$. Direct computation now shows that we have a surjective group homomorphism $A_4 \twoheadrightarrow A_3$ with kernel is set 1.4.

(iii): We first prove A_5 is simple. Because $A_5 \trianglelefteq S_5$ is normal, we know A_5 is the union of the classes of cycle types

$$(1, 2, 3) \quad \text{and} \quad (1, 2)(3, 4) \quad \text{and} \quad (1, 2, 3, 4, 5)$$

Direct computation shows that the first cycle type class has 20 elements, that the second cycle type class has 15 elements, and that the third cycle type class has 24 elements. It now follows from Lagrange's theorem and from normal subgroups are unions of conjugacy classes that A_5 has no proper nontrivial subgroups. (done)

Let $N \trianglelefteq A_n$, with $\tau \neq e \in N$ and $n > 5$. We are required to show $N = A_n$. Because $n \geq 5$, clearly for any pair of 3-cycles $\{(a_1, a_2, a_3), (b_1, b_2, b_3)\}$, there exists some $\sigma \in A_n$ such that $(b_1, b_2, b_3) = \sigma \circ (a_1, a_2, a_3) \circ \sigma^{-1}$. In other words, the class of 3-cycles forms a conjugacy class of A_n. This together with normality $N \trianglelefteq A_n$ and the fact that A_n is generated by set of 3-cycles reduce the problem into proving N contains a 3-cycle.

Consider A_5 as a subgroup of A_n that fixes a particular set of $n - 5$ numbers. Then clearly we have $N \cap A_5 \trianglelefteq A_5$. Because A_5 is simple and contains a 3-cycle, we now only have to show $N \cap A_5 > 1$, that is, to show N contains an element that fixes at least $n - 5$ elements.

Let (a_1, a_2, a_3) be a 3-cycle such that $\{\tau(a_1), \tau(a_2), \tau(a_3)\}, \{a_1, a_2, a_3\}$ overlap. We now see $\tau \circ (a_1, a_2, a_3) \circ \tau^{-1} \circ (a_1, a_2, a_3)^{-1} \in N$ is an element that fixes at least $n - 5$ elements. $\blacksquare$

Theorem 1.13.7. (A_n is the only proper nontrivial normal subgroup of S_n for $n \geq 5$) Let $n \geq 5$. Then A_n is the only proper nontrivial subgroup of S_n.

Proof. Let N be a proper nontrivial subgroup of S_n. We are required to show $N = A_n$. Because $[S_n : A_n] = 2$, we only have to show $A_n \leq N$. This boils down to showing $N \cap A_n > 1$, since A_n is simple. Assume for a contradiction that $N \cap A_n = 1$. The contradiction $N = 1$ then follows from $A_n = S_n^{(1)}$ and $Z(S_n) = 1$, since normal subgroup that disjoint with the commutator subgroup must be contained by the center. ∎

A group is said to be **complete** if the group has no outer automorphism and centerless. In other words, the natural map $G \longrightarrow \mathrm{Inn}(G)$ forms an isomorphism between G and $\mathrm{Aut}(G)$.

Theorem 1.13.8. (S_n is complete for $n \neq 2$ or 6) Let $n \geq 3$. Then S_n is complete for $n \neq 6$.

Proof. Clearly, automorphism group $\mathrm{Aut}(G)$ in general acts on conjugacy classes of G. That is, we have a group homomorphism $\mathrm{Aut}(G) \longrightarrow \mathrm{Bij}(\mathrm{cl}(G))$.

Let $\alpha \in \mathrm{Aut}(S_n)$. We first show that $\alpha \in \mathrm{Stab}(\mathrm{cl}((1,2))) \implies \alpha \in \mathrm{Inn}(S_n)$. Because S_n is generated by $\{(1,k) \in S_n : 2 \leq k \leq n\}$, we only have to show the existence of some $\sigma \in S_n$ such that

$$\alpha((1,k)) = \sigma(1,k)\sigma^{-1} = (\sigma(1), \sigma(k)), \quad \text{for all } k \geq 2$$

Because of the premise, we already know that $\alpha((1,k))$ is a 2-cycle. Our first task is to show that the intersection of the 2-cycles $\{\alpha((1,k)) : k \geq 2\}$ is nonempty. Write

$$\alpha((1,2)) \triangleq (a, b_2)$$

Because $(1,2)(1,3)$ is a 3-cycle, we know $\alpha((1,2))\alpha((1,3)) = \alpha((1,2)(1,3))$ is of order 3, which is only possible if the 2-cycle $\alpha((1,3))$ share exactly one element with the 2-cycle (a, b_2). WLOG, let that element be a, and write

$$\alpha((1,3)) = (a, b_3), \quad \text{where } b_3 \notin \{a, b_2\}$$

Applying the same logic to $\alpha((1,4))$, we see that the 2-cycle $\alpha((1,4))$ must share exactly one element with (a, b_2) and must share exactly one element with (a, b_3). Therefore, we know $\alpha((1,4))$ either is of the form

$$(a, b_4), \quad \text{with } b_4 \notin \{a, b_2, b_3\}$$

or is of the form (b_2, b_3). To see that the latter is impossible, simply compute the order of $(1,2)(1,3)(1,4)$ and $(a, b_2)(a, b_3)(b_2, b_3)$. Now, we apply the same logic to $\alpha((1,5))$, and this time we can conclude that $\alpha((1,5))$ must be of the form (a, b_5) with $b_5 \notin \{a, b_2, b_3, b_4\}$. Repeating the process, we then see

$$\sigma(1) \triangleq a \quad \text{and} \quad \sigma(k) \triangleq b_k$$

suffices.   (done)

Ir remains to show every $\alpha \in \text{Aut}(S_n)$ fix the class of transposition. Since α must maps a transposition to an element of order 2. We only have to prove

> For $n \neq 6$, the class of transposition has unique cardinality, which is $\binom{n}{2}$, among the conjugacy classes whose elements are of order 2.

Clearly, the conjugacy classes whose elements has order 2 are the classes of product of disjoint 2-cycles. Assume for a contradiction that there really is such a class that has the same cardinality of the class of transposition, says, this class is the class of k product of disjoint 2-cycle. We then would have

$$\binom{n}{2} = \frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2(k-1)}{2}$$

Noticing the RHS is telescoping, we compute

$$\binom{n-2}{2k-2} = \frac{k!(2^{k-1})}{(2k-2)!} \tag{1.5}$$

Because the RHS now is not an integer for $k \geq 4$, we now have $k \in \{1,2,3\}$. Direct computation now shows that for equation 1.5 to holds, we must have $k = 3$ and $n = 6$. (done) ∎

We say a group action $G \longrightarrow \text{Bij}(X)$ is **transitive** if for each $x, y \in X$, there exists some $g \in G$ such that $g \cdot x = y$. We say a subset $S \subseteq S_n$ is **transitive** if for each $i, j \in \{1, \ldots, n\}$ there exists some $s \in S$ such that $s(i) = j$

Theorem 1.13.9. (S_6 is incomplete) S_6 is not complete.

Proof. Sylow theorems shows that S_5 has 6 Sylow 5-subgroups, and the conjugacy action $\phi : S_5 \to \text{Bij}(\text{Syl}_5(S_5)) \cong S_6$ is transitive. In particular, the 6 Sylow 5-subgroups are the cyclic subgroups generated by the 6 distinct 5-cycles. Because A_5 is the only proper nontrivial normal subgroup of S_5, we know $\ker(\phi) \in \{1, A_5, S_5\}$. Clearly it isn't S_5. To see it isn't A_5, just note that if it is, then its images would have all have order 2, which just isn't the case, as one can observe that

$$(1,2,3)^2\langle(2,3,4,5,6)\rangle(1,2,3)^{-2} \neq \langle(2,3,4,5,6)\rangle$$

Therefore, the only possibility is that ϕ is injective. Denote $H \triangleq \phi(S_5) \leq S_6$. The fact that ϕ is transitive now means that $H \leq S_6$ is transitive.

Now, consider the left multiplication action $\sigma : S_6 \to \mathrm{Bij}(S_6 / H)$ on the left coset spaces of H. Because A_6 is the only proper nontrivial normal subgroup of S_6 and $\mathrm{Core}(H) \leq H$, we know σ must be injective. In other words, σ is an automorphism.

Note that all elements of $\sigma(H) \leq S_6$ fix a point, i.e., $H \in S_6 / H$ itself, while $H \leq S_6$, since being transitive, fix no points. If σ is inner, this is clearly impossible, thus the proof. $\blacksquare$

1.14 Commonsense in Finite Group Theory

Abstract

This section develop some commonsense about finite groups.

Theorem 1.14.1. (Classification of semidirect product of $C_q \rtimes C_p$ with $p \mid q - 1$) Let p, q be two primes. If $p \nmid q - 1$, then the semidirect product $C_q \rtimes C_p$ must be a direct product. If $p \mid q - 1$, then the semidirect product $C_q \rtimes C_p$ has exactly two non-isomorphic meanings.

Proof. Clearly, we have

$$\mathrm{Aut}(C_q) \cong \mathbb{Z}_q^\times \cong C_{q-1}$$

Let x and y each be the generators of C_p and C_{q-1}. Let $x \mapsto y^c$ defines a group homomorphism. Because $x^p = e$, we must have $q - 1 \mid pc$. Therefore, if $p \nmid q - 1$, the only action $\varphi \in \mathrm{Hom}(C_p, \mathrm{Aut}(C_q))$ is trivial.

Suppose $p \mid q - 1$. By the universal property of presentation, we now see that the possible group homomorphism $\mathrm{Hom}(C_p, C_{q-1})$ are exactly $x \mapsto y^{\frac{q-1}{p}d}$ for $d \in \mathbb{Z}$. Let φ_d and $\varphi : \mathbb{Z}_p \to \mathbb{Z}_{q-1}$ denote $x \mapsto y^{\frac{q-1}{p}d}$ and $x \mapsto y^{\frac{q-1}{p}}$ with $d \neq 0$. Clearly we have

$$\varphi_d = \varphi \circ \psi$$

where $\psi \in \mathrm{Aut}(C_p)$ is defined by $\psi(x) \triangleq x^d$. Because two actions differs by a automorphism in front induces the same semidirect product, we have shown that there can be at most two distinct semidirect product $C_q \rtimes C_p$.

To see that they are distinct, we claim that the nontrivial one is not abelian, which follows from noting that

$$(n, e) \cdot (e, h) = (n, h) \quad \text{and} \quad (e, h) \cdot (n, e) = (\varphi_h(n), h)$$

in general. ∎

We now have enough tools to state and prove our result. Note that normal Sylow subgroups are clearly characteristic, so we will use the word "characteristic Sylow subgroup" instead.

Theorem 1.14.2. (Analysis of finite group of fixed prime structure) Let p, q, r be three distinct prime. Then,

(i) Groups of order pq, where $p < q$, is always a semidirect product $C_q \rtimes C_p$, and we know there are at most 2 of them, depending on whether $p \mid q - 1$.

(ii) Groups of order $p^2 q$ has a characteristic Sylow subgroup.

(iii) Groups of order $p^3 q$ has a characteristic Sylow subgroup, given that $(p, q) \neq (2, 3)$.

(iv) Groups of order pqr has a characteristic r-Sylow subgroup and a normal subgroup of order qr, where $p < q < r$. If $q \nmid r - 1$, then groups of order pqr moreover has a characteristic q-Sylow subgroup.

(v) Simple groups of order $p^a m$, where $a, m \in \mathbb{N}$ satisfies $p \nmid m > 1$, must satisfies $o(G) \mid n_p!$.

Proof. (i): Clearly $n_q = 1$. Let $P \in \mathrm{Syl}_p(G)$. Clearly $P \cap Q = 1$. This by order formula implies $PQ = G$. The rest then follows from recognition theorem for inner semidirect product.

(ii): If $p > q$, then clearly n_p can only be 1. If $p < q$, then we must have $n_q \in \{1, p^2\}$. If $n_q = 1$, then we are done. If not, then from $n_q \equiv 1 \pmod{q}$, we see $q = p + 1$, which can only happens if $q = 3$ and $p = 2$. We claim that in such case, i.e., $o(G) = 12$, then either $n_3 = 1$ or $G \cong A_4$, which contains a characteristic 2-Sylow subgroup.

If $n_3 = 4$, then for any $P \in \mathrm{Syl}_3(G)$, we have $N_G(P) = P$, since $4 = n_3 = [G : N_G(P)]$. Clearly, the conjugacy action $G \longrightarrow \mathrm{Bij}(\mathrm{Syl}_3(G))$ has kernel contained by $N_G(P) = P$. This by non-normality of P and $o(P) = 3$ implies the conjugacy action $G \hookrightarrow \mathrm{Bij}(\mathrm{Syl}_3(G)) \cong S_4$ is injective. Note that G has 8 elements of order 3. Since A_4 is the only subgroup of S_4 with order 12 and 8 elements of order 3, we now see $G \cong A_4$. [1] The proof then follows from recalling that A_4 has a characteristic 2-Sylow subgroup.

(iii): Suppose G has no characteristic Sylow subgroup. We are required to show $(p, q) = (2, 3)$, which will follows from showing $q = p + 1$.

Now, since G has no characteristic Sylow subgroup, we know $n_p = q$, which by $n_p \equiv 1 \pmod{p}$ implies $p < q$, which further implies $n_q \in \{p^2, p^3\}$. Counting now give us $n_q = p^2$, which by $n_q \equiv 1 \pmod{p}$ and $p < q$ implies $q = p + 1$.

(iv): We first show $n_r = 1$. By counting, we know $1 \in \{n_p, n_q, n_r\}$. If n_p and n_q are both > 1, then we are done. We now show that $n_p = 1 \implies n_r = 1$, and the proof for $n_q = 1 \implies n_r = 1$ is similar.

---

[1]One may argue that the original assertion that groups of order $p^2 q$ all have a normal Sylow subgroup holds true, but we don't know whether it is possible $n_3 = 4$. Such is possible, since A_4 really makes $n_3 = 4$.

Denote P the characteristic Sylow p-subgroup of G. Applying (i) on $\frac{G}{P}$, we see the existence of $H \trianglelefteq G$ with order pr containing P. Applying (i) on H, we see the existence of K char H with $o(K) = r$. It then follows from transitive property of characteristic subgroup that K is the characteristic r-Sylow subgroup of G we are looking for.

To see G has a normal subgroup of order qr, just apply (i) on G/K. Denote that normal subgroup by $T \trianglelefteq G$. If $q \nmid r - 1$, then again by (i), there exists L char T with $o(L) = r$. Because of the transitive property of characteristic subgroup, we now see that L is the characteristic r-Sylow subgroup of G we are looking for.

(v): Let $P \in \mathrm{Syl}_p(G)$. Non-normality of P together with second Sylow theorem implies that the conjugacy action $G \longrightarrow \mathrm{Bij}(\mathrm{Syl}_p(G)) \cong S_{n_p}$ is nontrivial. Simplicity of G then forces the action to be injective, as desired. ∎

Theorem 1.14.3. (Analysis of groups of fixed order) We have:

(i) There are exactly four groups of order 30. Precisely, they are the four possible semidirect product of $C_{15} \rtimes C_2$:

$$\langle x, y \mid x^{15} = y^2 = e, yxy^{-1} = x^n \rangle \quad \text{where } n \in \{1, 4, 11, -1\}$$

(ii) The 11-sylow subgroup of groups of order $231 = 3 \cdot 7 \cdot 11$ lies in the centers.

(iii) The 7-sylow subgroup of groups of order $385 = 5 \cdot 7 \cdot 11$ lies in the centers.

(iv) No group of order $132 = 2^2 \cdot 3 \cdot 11$ is simple.

(v) Groups of order $108 = 2^2 \cdot 3^3$ either has a normal subgroup of order 9, or has a normal subgroup of order 27.

(vi) Simple groups of order 60 must be A_5.

Proof. (i): Since $30 = 2 \cdot 3 \cdot 5$, we know G has a normal subgroup N of order 15. This allows us to write $G \cong N \rtimes C_2$. Since the only group of order 15 is C_{15}, we now see G must be of the form:

$$G \cong C_{15} \rtimes C_2$$

To classify the possible semidirect product, one first compute $\mathrm{Aut}(C_{15}) \cong C_4 \times C_2$, [2] which show us that $\mathrm{Hom}(C_2, \mathrm{Aut}(C_{15}))$ has only 4 elements, which can be easily checked to be $y \mapsto (x \mapsto x^n)$, where $C_2 = \langle y \rangle, C_{15} = \langle x \rangle$ and $n \in \{1, 4, 11, 14\}$. To see that these four

---

[2]This can proved by noting $\mathrm{Aut}(C_{15}) \cong \mathbb{Z}_{15}^\times \cong (\mathbb{Z}_5 \times \mathbb{Z}_3)^\times \cong \mathbb{Z}_5^\times \times \mathbb{Z}_3^\times \cong C_4 \times C_2$. Of course, one can also just brute force the computation.

possibly distinct groups are really pairwise distinct, one can use their presentation to easily compute that the number of elements of order 2 they contain are indeed pairwise different.

(ii): Let R be the characteristic 11-sylow subgroup of G. We are required to prove $C_G(R) = G$. Because $C_G(R)$ is exactly the kernel of the conjugacy action $G = N_G(R) \longrightarrow \text{Aut}(R)$, by first isomorphism theorem, we have an injection $G / C_G(R) \hookrightarrow \text{Aut}(R) \cong C_{10}$. The proof then follows from counting order.

(iii): The proof is similar to that of (ii).

(iv): If G is simple, then $n_2 \geq 3, n_3 \geq 4$, and $n_{11} \geq 12$, which is impossible by counting.

(v): Let $n_3 = 4$. We are required to prove the existence of a normal subgroup of order 9. Let $P \in \text{Syl}_3(G)$. Consider the left multiplicative action $G \longrightarrow \text{Bij}(G / P) \cong S_4$ on the left cosets space G / P. The proof then follows from comparing orders and the observation that the kernel must lies in P.

(vi): Because the only proper nontrivial normal subgroup of S_5 is A_5 and because $o(G) = 60$, to show $G \cong A_5$, we only have to establish an injective group homomorphism $G \hookrightarrow S_5$.

Let $P \in \text{Syl}_2(G)$. By simplicity of G, we always have an injective group homomorphism $G \hookrightarrow \text{Bij}(G / N_G(P)) \cong S_{[G:N_G(P)]}$, the left multiplicative action on the left coset space of $N_G(P)$. Since $[G : N_G(P)] = n_2$, it remains to show $n_2 = 5$.

Because G is simple and $60 \nmid 4!$, from $G / \text{Core}(H) \hookrightarrow \text{Bij}(G / H)$, where G / H is the left coset space of H, we know that G can not have proper subgroup with index < 5. This with $[G : N_G(P)] = n_2$ in particular implies $n_2 \geq 5$. Because G is simple, we now have $n_2 \in \{5, 15\}$.

Assume $n_2 = 15$ for a contradiction. Because $n_5 = 6$, by counting, we see that there must be a pair of distinct 2-Sylow subgroup $Q, R \in \text{Bij}_2(G)$ such that $o(Q \cap R) = 2$. Let $M \triangleq N_G(Q \cap R)$. Since Q and R, of order 4, is abelian, we know $Q, R \leq M$, which implies $4 \mid o(M)$, that is, $o(M) \in \{4, 12, 20, 60\}$. Simplicity of G forces $o(M) \neq 60$, $Q \neq R$ forces $o(M) \neq 4$, and the fact that G has no proper subgroup of index < 5 forces $o(M) \neq 20$. Therefore, we must have $o(M) = 12$. By simplicity of G, we now have an injective group homomorphism $G \hookrightarrow \text{Bij}(G / M) \cong S_5$, the left multiplicative action on the left coset space of M, as desired. ∎

1.15   Simplicity of $\mathrm{PSL}_n(\mathbb{F})$

Abstract

This section shows that for $n \geq 3$, $\mathrm{PSL}_n(\mathbb{F})$ is simple, and for $n = 2$, $\mathrm{PSL}_n(\mathbb{F})$ is simple if $\mathbb{F}$ has ≥ 4 elements.

An action $\varphi : G \longrightarrow \mathrm{Bij}(X)$ is called **transitive** if for all $x, y \in X$, there exist some g that takes x to y. We say φ is **doubly transitive** if the naturally induced action on $G \longrightarrow \mathrm{Bij}(X^2 - D)$, where $D \triangleq \{(x, x) \in X^2 : x \in X\}$ is the diagonal, is transitive.

Theorem 1.15.1. (Property of doubly transitive action) Let $\varphi : G \to \mathrm{Bij}(X)$ be a doubly transitive action and $|X| \geq 2$. Then

(i) $\mathrm{Stab}(x) < G$ is maximal for all $x \in X$.

(ii) For all $N \trianglelefteq G$, the action $\varphi|_N : N \to \mathrm{Bij}(X)$ is either trivial or transitive.

Proof. (i): Denote $H \triangleq \mathrm{Stab}(x)$. We first show that:

$$G = H \cup HgH, \quad \text{for all } g \in G - H, \text{ where } HgH \triangleq \left\{ hg\widetilde{h} \in G : h, \widetilde{h} \in H \right\}$$

Fix $g \in G - H$. Let $\widetilde{g} \in G - H$. We are required to show $\widetilde{g} \in HgH$. Because $g, \widetilde{g} \notin H$, doubly transitivity of φ implies the existence of some element in G that takes (x, gx) to $(x, \widetilde{g}x)$. Such element is clearly in H. One then can check $\widetilde{g} \in hgH$, where h is the element that takes gx to $\widetilde{g}x$. (done)

$H < G$ is clear. To see that H is maximal, just observe that if a subgroup K of G properly contains H, then the subgroup contains $H \cup HgH = G$, where $g \in K - H$.

(ii): Suppose the action $N \longrightarrow \mathrm{Bij}(X)$ is nontrivial. We are required to show it is transitive. Fix $x \neq y \in X$. Because N is nontrivial, we know there exists some $z \in X$ and $n \in N$ such that $nz \neq z$. Doubly transitivity of φ then implies the existence of some $g \in G$ such that $g(z, nz) = (x, y)$. The proof then follows from checking that gng^{-1} takes x to y. ∎

Theorem 1.15.2. (Iwasawa criterion) Let $\varphi : G \to \mathrm{Bij}(X)$ be a doubly transitive action. If

(i) G is **perfect**, i.e., $G^{(1)} = G$.

(ii) There exists some $x \in X$ whose stabilizer subgroup has an abelian normal subgroup U such that $\bigcup_{g \in G} gUg^{-1}$ generates G.

then $G/\ker\varphi$ is simple.

Proof. Denote $K \triangleq \ker\varphi$ and $H \triangleq \text{Stab}(x)$. Let N be a normal subgroup of G that contains K. We are required to prove $N = K$ or G. Maximality of H splits the proof into two cases $NH = H$ or $NH = G$. We will prove that the case $NH = H$ leads to $N = K$, and the case $NH = G$ leas to $N = G$.

Case ($NH = H$): In such case, clearly $N \leq H$, and therefore N acts trivially on X, which implies $N \leq K$, as desired.

Case ($NH = G$): In such case, normality $U \trianglelefteq H$ implies $NU \trianglelefteq G$. This then implies that $gUg^{-1} \leq g(NU)g^{-1} = NU$ for all $g \in G$. Therefore by premise, $NU = G$. Second isomorphism theorem then shows that $G/N \cong NU/N \cong U/N \cap U$ is abelian, which by perfectness of G implies that $N = G$. $\blacksquare$

Let $\mathbb{F}$ be a field. The **general linear group** $\text{GL}_n(\mathbb{F})$ is the group of n-by-n $\mathbb{F}$-valued matrices that has nonzero determinant. Clearly, $\text{GL}_n(\mathbb{F})$ acts naturally on the affine space $\mathbb{A}^n(\mathbb{F})$, and moreover on the projective space $\mathbb{P}^{n-1}(\mathbb{F})$.

Theorem 1.15.3. (Kernel of general linear group acting on projective space) The kernel of the group action $\text{GL}_n(\mathbb{F}) \longrightarrow \text{Bij}(\mathbb{P}^{n-1})$ is exactly the group of scalar diagonal:

$$\left\{ cI \in \text{GL}_n(\mathbb{F}) : c \in \mathbb{F}^\times \right\}$$

coinciding with its center $Z(\text{GL}_n(\mathbb{F}))$.

Proof. We first show that the group of the scalar diagonal = the kernel. Clearly the group of scalar transformations lies in the kernel. To see the converse inclusion holds, let A maps

$$v \mapsto \lambda v \quad \text{and} \quad w \mapsto \mu w$$

and observes that if $\lambda \neq \mu$, then A doesn't fix $[v + w]$.

It remains to show the center = the group of scalar diagonal. Again, clearly the group of scalar diagonal lies in the center. Let $A \in Z(\text{GL}_n(\mathbb{F}))$. To prove that A is scalar diagonal, one simply consider $E_{i,j} \triangleq I_n + e_{i,j}$, where $e_{i,j} \in M_n(\mathbb{F})$ is the **matrix unit**. $\blacksquare$

Because the group action $\text{GL}_n(\mathbb{F}) \to \text{Bij}(\mathbb{P}^{n-1})$ has such kernel, we define the **projective general linear group** $\text{PGL}_n(\mathbb{F})$ to be the quotient group

$$\text{PGL}_n(\mathbb{F}) \triangleq \text{GL}_n(\mathbb{F}) / \left\{ cI_n \in \text{GL}_n(\mathbb{F}) : c \in \mathbb{F}^\times \right\}$$

The **special linear group** $\text{SL}_n(\mathbb{F}) \leq \text{GL}_n(\mathbb{F})$ is the subgroup whose elements has determinant 1, and the kernel of its action on $\mathbb{P}^{n-1}$ is clearly $\{cI_n \in \text{SL}_n(\mathbb{F}) : c^n = 1\}$, so we define the **projective special linear group** $\text{PSL}_n(\mathbb{F})$ to be

$$\text{PSL}_n(\mathbb{F}) \triangleq \text{SL}_n(\mathbb{F}) / \left\{ cI_n \in \text{SL}_n(\mathbb{F}) : c \in \mathbb{F}^\times \text{ is a } n\text{-th root of unity.} \right\}$$

Theorem 1.15.4. (Basic properties of special linear group) Let $\mathbb{F}$ be an arbitrary field and $n \geq 2$. Then,

(i) $\mathrm{SL}_n(\mathbb{F})$ acts doubly transitive on $\mathbb{P}^{n-1}$.

(ii) $\mathrm{SL}_n(\mathbb{F})$ has center $\{cI_n \in \mathrm{SL}_n(\mathbb{F}) : c \in \mathbb{F}^{\times} \text{ is a } n\text{-th root of unity.}\}$, thus equal to the kernel of its action on $\mathbb{P}^{n-1}$.

Proof. (i): Let $([v_1], [v_2]), ([w_1], [w_2]) \in (\mathbb{P}^{n-1})^2$ be two pairs off the diagonal. We are required to show the existence of some $\widehat{L} \in \mathrm{SL}_n(\mathbb{F})$ that send $[v_1]$ to $[w_1]$ and $[w_1]$ to $[w_2]$. The proof then follows from extending them to two bases $\{v_1, \ldots, v_n\}, \{w_1, \ldots, w_n\}$ for $\mathbb{F}^n$ and setting $\widehat{L}(v_i) \triangleq c_i w_i$ with

$$\det(PQ^{-1}) \cdot \left(\prod_{i=1}^{n} c_i\right) = 1$$

where $Q, P \in \mathrm{GL}_n(\mathbb{F})$ are respectively the matrix whose i-th column is v_i, w_i. (ii): The proof that computes $Z(\mathrm{GL}_n(\mathbb{F}))$ applies here, since $E_{i,j} \in \mathrm{SL}_n(\mathbb{F})$. $\blacksquare$

To apply Iwasawa criterion on the projective special linear groups $\mathrm{PSL}_n(\mathbb{F})$, it remains to show

(I) $\mathrm{SL}_n(\mathbb{F})$ is perfect.

(II) There exists some $x \in \mathbb{P}^{n-1}$ whose stabilizer subgroup $H \leq \mathrm{SL}_n(\mathbb{F})$ has an abelian normal subgroup U such that $\bigcup_{g \in G} gUg^{-1}$ generates G.

The reasons why simplicity of $\mathrm{SL}_2(\mathbb{F})$ requires $\mathbb{F}$ to have ≥ 4 elements lies in the fact (I) may fails to be true if $\mathbb{F}$ has ≤ 3 elements.

Example 1.15.5: $\mathrm{SL}_2(\mathbb{F}_2)$ and $\mathrm{SL}_2(\mathbb{F}_3)$ are not perfect

By counting, we know

$$o\left(\mathrm{GL}_n(\mathbb{F}_p)\right) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$$

Since determinant function is a surjective group homomorphism from $\mathrm{GL}_n(\mathbb{F}_p)$ to $\mathbb{F}_p^{\times}$ with kernel $\mathrm{SL}_n(\mathbb{F}_p)$, we know

$$o\left(\mathrm{SL}_n(\mathbb{F}_p)\right) = \frac{1}{p-1} \cdot (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$$

In particular, $\mathrm{SL}_2(\mathbb{F}_2)$ and $\mathrm{SL}_2(\mathbb{F}_3)$ has order 6 and 24. Now, clearly $\mathrm{SL}_2(\mathbb{F}_2)$ has a faithful action on:

$$\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\}$$

So by comparing order, we know $\mathrm{SL}_2(\mathbb{F}_2) \cong S_3$. Therefore non-perfectness of $\mathrm{SL}_2(\mathbb{F}_2)$ then follows from $S_3^{(1)} = A_3$. In fact, since $\mathrm{PSL}_2(\mathbb{F}_2) \cong \mathrm{SL}_2(\mathbb{F}_2)$, we have shown that $\mathrm{PSL}_2(\mathbb{F}_2)$ is non-simple.

Now, recall that $\mathrm{PSL}_2(\mathbb{F}_3)$ acts faithfully on $\mathbb{P}^1(\mathbb{F}_3)$, which has $\frac{3^2-1}{3-1} = 4$ points, so we have an injective group homomorphism $\mathrm{PSL}_2(\mathbb{F}_3) \longhookrightarrow S_4$. Computing that $o\left(\mathrm{PSL}_2(\mathbb{F}_3)\right) = 12$, we see that since the only index 2 subgroup of S_4 is A_4, we have the isomorphism $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$, which is non-simple.

Regardless of whether $n > 2$, the second condition is proved using the same H and U. We pick $x \triangleq [1 : 0 : \cdots : 0]$, and therefore

$$H = \left\{ \begin{pmatrix} a & * \\ \mathbf{0} & M \end{pmatrix} : a \in \mathbb{F}^\times \text{ and } M \in \mathrm{GL}_{n-1}(\mathbb{F}) \right\}$$

and since:

$$\begin{pmatrix} a & * \\ \mathbf{0} & M \end{pmatrix} \begin{pmatrix} b & * \\ \mathbf{0} & J \end{pmatrix} = \begin{pmatrix} ab & * \\ \mathbf{0} & MJ \end{pmatrix}$$

We know

$$U \triangleq \left\{ \begin{pmatrix} 1 & * \\ \mathbf{0} & I_{n-1} \end{pmatrix} \right\} \text{ is normal in } H.$$

U is abelian since

$$\begin{pmatrix} 1 & \mathbf{v} \\ \mathbf{0} & I_{n-1} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{w} \\ \mathbf{0} & I_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{v} + \mathbf{w} \\ \mathbf{0} & I_{n-1} \end{pmatrix}$$

Interestingly, both (I) and (II) requires boring computations within $\mathrm{SL}_n(\mathbb{F})$.

Theorem 1.15.6. (One dimensional projective special linear group is simple over field that has ≥ 4 elements) If $\mathbb{F}$ has ≥ 4 elements, then $\mathrm{PSL}_2(\mathbb{F})$ is simple.

Proof. (II): Since

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}$$

We know the group of the lower triangular matrices:

$$\left\{ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\}$$

56

is a conjugate of U. We prove that $\mathrm{SL}_2(\mathbb{F})$ is generated by U and the lower triangular matrices. To see such, just observe that if any of b, c is nonzero, then by transposing the matrix if necessary, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (d-1)b^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (a-1)b^{-1} & 1 \end{pmatrix}, \quad \text{where } b \neq 0$$

and if both of them are zero, then $d = a^{-1}$ and we have

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (1-a)a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix}$$

(I): Compute

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & b(a^2 - 1) \\ 0 & 1 \end{pmatrix}$$

Because $\mathbb{F}$ has ≥ 4 elements, we know that there exists some $a \in \mathbb{F}^\times$ such that $a^2 \neq 1$ (Consider $x^2 - 1 \in \mathbb{F}[x]$). Fix such a. We then see that $U \leq \mathrm{SL}_2(\mathbb{F})^{(1)}$ by letting b run through $\mathbb{F}$. Normality of $\mathrm{SL}_2(\mathbb{F})^{(1)}$ and (II) then implies $\mathrm{SL}_2(\mathbb{F})^{(1)} = \mathrm{SL}_2(\mathbb{F})$ ∎

Theorem 1.15.7. (≥ 2 dimensional projective special linear groups are all simple) Let $n \geq 3$. Then we have:

(i) $I_n + \lambda e_{ij}$ is conjugate to $I_n + e_{12}$ in $\mathrm{SL}_n(\mathbb{F})$, for all $\lambda \in \mathbb{F}^\times$ and $i \neq j$.

(ii) $\{I_n + \lambda e_{ij} : \lambda \in \mathbb{F} \text{ and } i \neq j\}$ generates $\mathrm{SL}_n(\mathbb{F})$.

Since $I_n + e_{12} \in U$, together they implies (II), and using them we may prove (I).

Proof. (i): We are required to find some $P \in \mathrm{SL}_n(\mathbb{F})$ such that $P(I_n + \lambda e_{ij})P^{-1} = I_n + e_{12}$. Note that $I_n + \lambda e_{ij}$ maps

$$e_j \mapsto e_j + \lambda e_i \quad \text{and } e_k \mapsto e_k \text{ for all } k \neq j$$

The construction of P then follows from letting its first column to be λe_i, its second column to be e_j, and the rest to be other basis vector unchanged by $I_n + \lambda e_{ij}$, where the third column is multiplied by λ^{-1}. (We used the fact $n \geq 3$ here)

(ii): This is proved via induction. We have proved the base case in our proof for simplicity of $\mathrm{PSL}_2(\mathbb{F})$. We now prove the inductive case. Let $A \in \mathrm{SL}_n(\mathbb{F})$. We are required to show that

$$PAQ = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \tilde{A} \end{pmatrix}, \quad \text{for some } P, Q \text{ generated by } I_n + \lambda e_{ij}$$

57

and the rest would follows the inductive hypothesis. The construction of P, Q is obvious once one observe the effect of multiplying $I_n + \lambda e_{ij}$ on a matrix.

(I): By (i), (ii) and normality of commutator subgroup, we only have to prove $I_n + e_{12} \in \mathrm{SL}_n(\mathbb{F})^{(1)}$, which follows from computing

$$I_n + e_{12} = [I_n + e_{13}, I_n + e_{32}]$$

∎

1.16   selection of advanced topics

Theorem 1.16.1. (Burnside's $p^a q^b$ theorem) If $o(G) = p^a q^b$ for some primes p, q, then G is solvable.

Proof. Wikipedia has a detailed proof.   ∎

Theorem 1.16.2. (Schur-Zassenhaus theorem) Let G be a finite group and $N \trianglelefteq G$ be Hall. Then the short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

right splits, and thus G must be a semidirect product of $N \rtimes (G/N)$.

Proof. Wikipedia has a proof sketch that relies on group cohomology   ∎

Theorem 1.16.3. (Thompson's fixed-point-free theorem) Let G be a finite group that admits a fixed-point-free automorphism of prime order. Then G is nilpotent.

Proof. This is Thompson's proof.   ∎

Theorem 1.16.4. (Nielsen-Schreier Theorem) The subgroup of a free group is isomorphic to some free group.

Proof. Wikipedia has a proof based on Algebraic Topology.   ∎

Theorem 1.16.5. (Schreier conjecture, now a theorem) Outer automorphism group of finite simple groups are solvable.

Proof. See this MO post.   ∎

Theorem 1.16.6. (Feit-Thompson theorem) Finite groups of odd order are solvable.

Proof. Wikipedia has a proof sketch.   ∎

Theorem 1.16.7. (Frobenius theorem about equation in group) Let G be a finite group, and let $n \mid o(G)$. The number of solution to the equation

$$g^n = e$$

is a positive multiple of n.

Proof. Isaacs and Robinson gives a relatively simple proof of this.   ∎

Theorem 1.16.8. (Frobenius conjecture) Let G be a finite group, and let $n \mid o(G)$. If the number of solution to the equation $g^n = e$ is exactly n, then these n elements form a normal subgroup of G.

Proof. Iiyori and Yamaki show that this is a corollary of classification of finite simple groups.   ∎

1.17   recreational exercises

> **Question 1: Groups as unions of proper subgroups**
>
> Show that a group can not be written as the union of two proper subgroup.

Proof. Let $G = H \cup K$. We are required to prove $G \in \{H, K\}$. We prove such by showing that one is contained by the other. Assume not for a contradiction. Letting $h \in H - K$ and $k \in K - H$, we see that $hk \in G - H \cup K$, a contradiction. For more on this kind theorems, see the survey article *Groups as unions of proper subgroups,* by Bhargava, M. (2009)   ∎

> **Question 2: $n-1, n, n+1$-abelian implies abelian**
>
> Let $n \in \mathbb{Z}$ satisfies
>
> $$(ab)^n = a^n b^n \quad \text{and} \quad (ab)^{n-1} = a^{n-1} b^{n-1} \quad \text{and} \quad (ab)^{n+1} = a^{n+1} b^{n+1}$$
>
> for all $a, b \in G$. Show that G is abelian.

Proof.

$$a^n b^n ab = (ab)^n (ab) = (ab)^{n+1} = a^{n+1} b^{n+1}$$
$$\implies b^n a = ab^n$$
$$\implies (a^{n-1} b^{n-1}) ba = a^n b^n = (a^{n-1} b^{n-1}) ab$$
$$\implies ba = ab$$

∎

> **Question 3: finite 3-abelian whose order is not divisible by 3 is abelian**
>
> Let G be a finite group whose order is not divisible by 3. Suppose
>
> $$(ab)^3 = a^3 b^3, \quad \text{for all } a, b \in G$$
>
> Show that G is abelian.

Proof. Because $3 \nmid o(G)$, we know if $g^3 = e$, then $g = e$. In other words, the endomorphism $x \mapsto x^3$ is an automorphism. Because of such, we only have to prove $a^3 b^3 = b^3 a^3$ for all

$a, b \in G$. This then follows from

$$(ab)^3 = a^3 b^3, \quad \text{for all } a, b \in G$$
$$\implies baba = a^2 b^2, \quad \text{for all } a, b \in G$$
$$\implies (ba)^2 = a^2 b^2, \quad \text{for all } a, b \in G$$
$$\implies (ab)^4 = [(ab)^2]^2 = [b^2 a^2]^2 = a^4 b^4, \quad \text{for all } a, b \in G$$
$$\implies (ab)^4 = a(ba)^3 b = ab^3 a^3 b, \quad \text{for all } a, b \in G$$
$$\implies a^3 b^3 = b^3 a^3, \quad \text{for all } a, b \in G$$

$\blacksquare$

Question 4

Let $a, b \in G$ satisfies

$$o(a) = 5 \quad \text{and} \quad aba^{-1} = b^2$$

Find $o(b)$.

Proof.

$$aba^{-1} = b^2$$
$$\implies a^2 b a^{-2} = ab^2 a^{-1} = (aba^{-1})^2 = b^4$$
$$\implies b = a^5 a^{-5} = a^4 b^2 a^{-4} = (a^2 b a^{-2})^2 = b^8$$

Therefore $o(b) = 7$. $\blacksquare$

Question 5: Structure theorem for finitely generated abelian group

Let G be an abelian group, and $x, y \in G$ has order m, n. Show that G has an element of order $\operatorname{lcm}(m, n)$.

Proof. The proof follows from noting that the fact that in general, given $(a_1, \ldots, a_n) \in G_1 \times \cdots \times G_n$, we have

$$o((a_1, \ldots, a_n)) = \operatorname{lcm}(o(a_1), \ldots, o(a_n))$$

and the fact that since $x, y \in \langle x \rangle + \langle y \rangle$, in the primary decomposition form of $\langle x \rangle + \langle y \rangle$, there must be a component of high enough power. $\blacksquare$

Question 6: Structure theorem for finitely generated abelian group

Let G be an abelian groups that has subgroups of order m and n. Show that is has a subgroup of order $\text{lcm}(m, n)$.

Proof. Let the subgroups be M, N. The proof then follows from noting that $\text{lcm}(m, n) \mid o(MN)$ and the fact that for every divisor d of the order of a finite abelian group H, there always exists a subgroup $\leq H$ of order d. ∎

Question 7: Structure theorem for finitely generated abelian group

Let G be a finite abelian group in which the number of solution of the equation $x^n = e$ is $\leq n$ for all $n \in \mathbb{N}$. Show that G is cyclic.

Proof. Write G in its primary decomposition form. We are required to show that its p-torsion subgroup has at most one component. This follows from noting that for $d, e \geq 1$, the group $C_{p^d} \times C_{p^e}$ has p^2 number of solution to the equation $x^n = e$. ∎

Question 8

Let $a \in G$. Show that the equation

$$x^2 a x = a^{-1}$$

is solvable for $x \in G$ if and only if a is the cube of some element.

Proof. Suppose $x^2 a x = a^{-1}$ for some $x \in G$. One can show that $a = (xa)^3$. If $a = y^3$, then $x \triangleq y^{-2}$ is a solution. ∎

Chapter 2

Commutative Algebra

2.1   Rings and Modules

The precise meaning of the term **ring** varies across different books. In this note, ring multiplication is always associative, commutative, and has an identity. The additive and multiplicative identity are denoted by 0 and 1. Let A be a ring, clearly we have

$$x \cdot 0 = 0, \quad \text{for all } x \in A$$

Consequently, $1 \neq 0$ unless the ring contain only one element, and we always have the **zero ideal**. If $1 = 0$, we call the ring **zero ring**.

We say $a \in A$ is a **zero-divisor** if $ab = 0$ for some $b \neq 0$. Clearly, both zero-divisors and non-zero-divisors are closed under multiplication, and non-zero-divisors moreover forms a monoid:
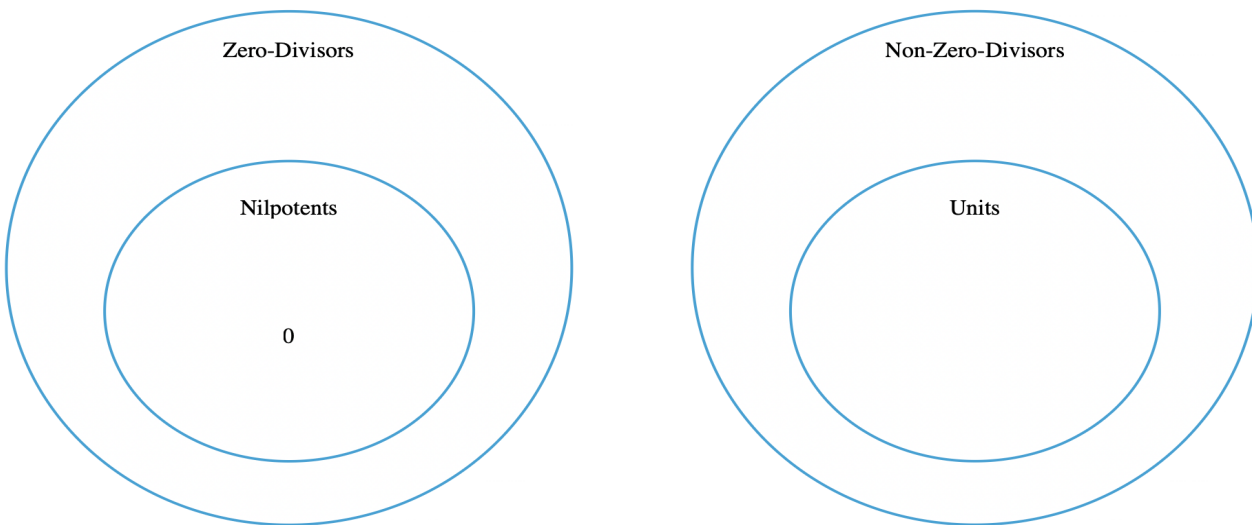
We say $a \in A$ is **nilpotent** if $a^n = 0$ for some $n > 0$, and we call the multiplicative group $A^\times$ of elements that admits an inverse the **unit group** of A.

Theorem 2.1.1. (Sum of nilpotents and unit is always a unit) Let $x \in \mathrm{Nil}(A)$. Then $x + u \in A^\times$ for all $u \in A^\times$.

Proof. Just observe

$$-(x+u)(x-u)(x^2+u^2)(x^4+u^4)\cdots(x^{2^n}+u^{2^n}) = u^{2^{n+1}} - x^{2^{n+1}}$$

for all $n \in \mathbb{N}$, and therefore equals to $u^{2^{n+1}} \in A^\times$ for $n \gg 0$. This then implies $x + u \in A^\times$. ∎

One should always be careful with zero-divising and unital properties, as they clearly depends on the ambient ring:

> **Example 2.1.2: Non-units and non-zero-divisors become units and zero-divisors in larger rings.**
>
> Embedding a ring into a field, all non-units becomes a unit. In particular, $2 \in \mathbb{Z}$ is a unit in $\mathbb{Q}$. Let A be a ring, $a \in A$ be a non-unit non-zero-divisor, and consider the embedding:
>
> $$A \longhookrightarrow A \times (A/\mathfrak{a}) \quad \text{and} \quad x \mapsto (x, x + \mathfrak{a}), \quad \text{where } \mathfrak{a} \triangleq (a)$$
>
> Because a is non-unit, we know $A/\mathfrak{a} \neq 0$, and therefore $(0, 1) \neq (0, 0)$. Since
>
> $$(a, 0) \cdot (0, 1) = (0, 0)$$
>
> We see a is a zero-divisor in $A \times (A/\mathfrak{a})$.

A **ring homomorphisms** $f : A \to B$ is a function that respect $+$, $\times$, and 1. Clearly, f must also respect 0, -1, and units, $f(A)$ forms a subring of B, and if f is injective, then the inverse $f^{-1} : f(A) \to A$ forms a ring homomorphism. An A-**module** M is an abelian group together with a compatible A-scalar structure, or equivalently, a ring homomorphism $A \longrightarrow \mathrm{End}(M)$, where $\mathrm{End}(M)$ is the endomorphism ring of the abelian group M. An A-**module homomorphism** $f : M \to N$ is a function that respect vector addition and multiplication.

Let $f : A \to B$ be a ring homomorphism and N be a B-module. Clearly, we can give N an A-module structure, called **restriction of scalar**, by setting $ax \triangleq f(a)x$ for all $a \in A$ and $x \in N$.

An *A*-**algebra** is an *A*-module *B* together with a compatible ring structure, or equivalently, a ring homomorphism $f : A \to B$ that give *B* an *A*-module structure by scalar restriction. An *A*-**algebra homomorphism** $f : B \to C$ is a function that is both ring homomorphism and *A*-module homomorphism. Clearly, a ring homomorphism $h : B \to C$ is an *A*-algebra homomorphism if and only if it makes the diagram:

$$
\begin{array}{ccc}
 & A & \\
 \swarrow & & \searrow \\
B & \xrightarrow{\quad h \quad} & C
\end{array}
$$

commute. In this note, **subrings, submodules and subalgebra** are then just injective ring (module, algebra) homomorphism.

Let *A* be a ring. An **ideal** $\mathfrak{a} \trianglelefteq A$ is just a submodule. Since they play roughly the same role as normal subgroups in groups, we use the same notation. Let $f : A \to B$ be a ring homomorphism and $\mathfrak{b} \trianglelefteq B$. Notably, since preimage $f^{-1}(\mathfrak{b})$ is the kernel of the ring homomorphism:

$$
A \longrightarrow B \longrightarrow B \big/ \mathfrak{b}
$$

We see that, just like normal subgroups, preimages of ideals are ideals.

Let *M* be an *A*-module and $X \subseteq M$. The set (X) of finite linear combinations of *X* is called the **submodule generated by** *X*. Let $S \subseteq A$. The **ideal** (S) **generated by** *S* is then the submodule generated by *S*. Let *B* be an *A*-algebra and $Y \subseteq B$. The natural image of the polynomial ring $A[Y]$ is called the **subalgebra generated by** *Y*. Clearly, in the case of module, ring, and algebra, the generated objects are the smallest objects that contain the generators.

At this point, we should point out that **finitely generated module** and **finitely generated algebra** are two different notions, and a **ring is finitely generated** if it is finitely generated as a $\mathbb{Z}$-algebra.

Example 2.1.3: Finitely generated algebras need not be finitely generated modules.

Clearly, $A[x]$ is finitely generated as an *A*-algebra, but not finitely generated as an *A*-module.

2.2 Direct Limits

Abstract

This section deals with the very basic properties of direct limit, especially in **Ring** and **Mod**$_A$.

Theorem 2.2.1. (Construction of direct limit in familiar categories) Let A be a ring, I a directed set, and $\{M_i, \varphi_{ij}\}$ a directed system of A-modules. One way to construct its direct limit is to first define the underlying set as:

$$\varinjlim M_i \triangleq \bigsqcup_i M_i \big/ \sim$$

where $x_i \in M_i$ and $x_j \in M_j$ are equivalence when:

$$x_i \sim x_j \overset{\triangle}{\iff} \varphi_{ik}(x_i) = \varphi_{jk}(x_j), \quad \text{for some } k \geq i, j$$

Addition is well-defined by

$$[x_i] + [x_j] \triangleq [\varphi_{ik}(x_i) + \varphi_{jk}(x_j)], \quad \text{for any } k \geq i, j$$

while scalar multiplication is well-defined by

$$c[x_i] \triangleq [cx_i]$$

Lastly, the canonical morphism $\varphi_i : M_i \to M$ maps elements to their equivalence class. One can now check that our construction in fact also shows that direct limit exists in **Set**, **Gp**, and **Ab**. Moreover, in **Ring** and **Alg**$_A$, direct limit also exists if we define vector multiplication the same way we define addition.

Proof. Routine. ∎

Theorem 2.2.2. (Basic properties of direct limit) Let A be a ring, I a directed set, and (M_i, φ) a directed system of A-modules. Then

(i) Every element of $\varinjlim M_i$ can be written in the form $\varphi_i(x_i)$ for some $i \in I$ and $x_i \in M_i$.

(ii) If $\varphi_i(x_i) = 0$, then there exists some $j \geq i$ such that $\varphi_{ij}(x_i) = 0$.

Let (A_i, ψ) be a directed system of ring. Then

(i) $\varinjlim A_i = 0 \implies A_i = 0$ for some i.

(ii) If A_i are integral domain, then $\varinjlim A_i$ is an integral domain.

(iii) We have a natural $\mathbb{Z}$-module isomorphism:

$$\varinjlim \mathrm{Nil}(A_i) \cong \mathrm{Nil}\left(\varinjlim A_i\right), \quad \phi_i(a_i) \mapsto \psi_i(a_i)$$

where the canonical morphism ϕ of directed system of $\mathrm{Nil}(A_i)$ is obtained by restricting ψ.

Proof. The statements for M_i all follow from the construction, so we only prove the statement for A_i.

(i): Fix i. Because ψ_i maps 1_{A_i} to 0, we know there exists some $j \geq i$ such that ψ_{ij} maps 1_{A_i} to 0. Then because ring homomorphism preserve multiplicative identity, we see $A_j = 0$.

(ii): Let $\psi_i(a_i)\psi_j(a_j) = 0$. Then for all $k \geq i, j$, we have $\psi_k(\psi_{ik}(a_i)\psi_{jk}(a_j)) = 0$. It then follows from the premise that A_k is an integral domain that either $\psi_{ik}(a_i)$ or $\psi_{jk}(a_j)$ is 0, which implies that either $\psi_i(a_i) = \psi_k \circ \psi_{ik}(a_i)$ or $\psi_j \circ \psi_{jk}(a_j)$ is 0.

(iii): The reason we may restrict ψ follows from the obvious fact that ring homomorphisms preserve nilpotents. The proposed homomorphism is clearly well-defined and have image lying inside $\mathrm{Nil}\left(\varinjlim A_i\right)$. To see $\mathrm{Nil}\left(\varinjlim A_i\right) \leq \varinjlim \mathrm{Nil}(A_i)$, just observe that if $\psi_i(a_i)^n = 0$, then $\psi_i(a_i^n) = 0$, and therefore for some $j \geq i$, we have $\psi_{ij}(a_i)^n = 0$, which implies $\psi_{ij}(a_i) \in \mathrm{Nil}(A_j)$, and therefore $\psi_i(a_i)$ is the image of $\phi_{ij}(a_i) \in \mathrm{Nil}(A_j)$. ∎

Theorem 2.2.3. (Module sums are direct limits) Let M_i be a collection of submodules of M indexed by I that satisfies

For all $i, j \in I$, there exists some $k \in I$ that makes $M_i + M_j \leq M_k$.

then M_i and M/M_i naturally forms a directed system whose direct limit can be realized as

$$\varinjlim M_i = \sum M_i = \bigcup M_i \quad \text{and} \quad \varinjlim(M/M_i) = M/\sum M_i$$

Therefore, in particular, every module is the direct limit of its finitely generated submodules.

Proof. Routine. ∎

Let A be a ring and I be a directed set. Then we can define a covariant functor $D : \mathrm{Func}(I, \mathbf{Mod}_A) \to \mathbf{Mod}_A$ by

$$D(M_i, \mu) \triangleq \varinjlim M_i \quad \text{and} \quad D(\Phi) \triangleq \varphi$$

where $\varphi : \varinjlim M_i \to \left(\varinjlim N_i, \nu\right)$ is the unique A-module homomorphism such that $\varphi \circ \mu_i = \nu_i \circ \varphi_i$.

Equivalent Definition 2.2.4. (Direct limit is an exact functor) Let A be a ring and I be a directed set. The covariant functor $\varinjlim : \mathrm{Func}(I, \mathbf{Mod}_A) \to \mathbf{Mod}_A$ is exact.

Proof. Routine. ∎

2.3 Ideals

Equivalent Definition 2.3.1. (Sum for modules and ideals) Let A be a ring, and M an A-module. The **sum** $\sum M_i$ **of** *possibly infinite* **submodules** $M_i \leq M$ is the set of finite combinations of elements of M_i. One can check that, in the form of **external direct sum**, coproduct always exists in the category of modules. Moreover, given a collection M_i of submodules of M, if $M_i \cap \sum_{j \neq i} M_j = 0$ for all i, clearly we have a natural module isomorphism:

$$\bigoplus M_i \cong \sum M_i$$

In such case, we say $\sum M_i$ form an **internal direct sum**.

The **sum of** *possibly infinite* **ideals** $\mathfrak{a}_i \trianglelefteq A$ is defined as their sum as submodules. Notably, finite sum of principal ideals satisfies:

$$(x) + (y) = (x + y), \quad \text{for all } x, y \in A$$

Proof. Routine. ∎

Note that in general, condition $M_i \cap M_j = 0$ for all $i \neq j$ isn't strong enough to make $\sum M_i$ an internal direct sum, and that submodules N of $M_1 \times M_2$ need not take the form $N \cap M_1 \times N \cap M_2$. See example 1.8.9 and example 1.8.10.

Equivalent Definition 2.3.2. (Quotient of module and ideals) Let A be a ring and M an A-module. Let $N, P \leq M$ be two submodules. Their **quotient** is the ideal of A defined by:

$$(N : P) \triangleq \{a \in A : aP \leq N\}$$

The **annihilator** of M is then defined by:

$$\text{Ann}(M) \triangleq (0 : M)$$

The **ideal quotient and annihilator** is defined as their quotient and annihilator as submodules. We then have

$$\{d \in A : d \text{ is a zero-divisor}\} = \bigcup_{x \neq 0 \in A} \text{Ann}(x)$$

We say M is a **faithful module** if $\text{Ann}(M) = 0$. Interestingly, if $\text{Ann}(M) \leq \mathfrak{a}$, then M has a well-defined natural $A/\mathfrak{a}$-module structure:

$$\overline{a} \cdot m \triangleq am$$

Proof. Routine. ∎

Theorem 2.3.3. (Basic properties of module quotient) Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \trianglelefteq A$. We have

$$\mathfrak{a} \leq (\mathfrak{a} : \mathfrak{b}) \quad \text{and} \quad (\mathfrak{a} : \mathfrak{b})\mathfrak{b} \leq \mathfrak{a} \quad \text{and} \quad ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$$

For *possibly infinite* set of ideals $\mathfrak{a}_i, \mathfrak{b}_i \leq A$, we have

$$\left(\bigcap \mathfrak{a}_i : \mathfrak{b} \right) = \bigcap (\mathfrak{a}_i : \mathfrak{b}) \quad \text{and} \quad \left(\mathfrak{a} : \sum \mathfrak{b}_i \right) = \bigcap (\mathfrak{a} : \mathfrak{b}_i)$$

Given three submodules M, N, P of some A-module, we have

$$\mathrm{Ann}(M + N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N) \quad \text{and} \quad (N : P) = \mathrm{Ann}\left(N + P \diagup N \right)$$

Proof. Routine. ∎

Equivalent Definition 2.3.4. (Product of ideals and modules) The **product** of a *finite* set of ideals $\mathfrak{a}_i$ is defined to be the set of all finite sums of products of elements:

$$\prod_{i=1}^{n} \mathfrak{a}_i \triangleq \left\{ \sum_{\text{finite}} a_1 \cdots a_n \in A : a_i \in \mathfrak{a}_i \right\}$$

Even though product of two submodules can not be defined, we may define the **product** $\mathfrak{a}M \leq M$ as:

$$\mathfrak{a}M \triangleq \left\{ \sum_{\text{finite}} a_i m_i \in M : a_i \in \mathfrak{a} \text{ and } m_i \in M \right\}$$

Proof. Routine. ∎

Theorem 2.3.5. (Ideals in finite direct product of rings) Let $\mathfrak{a} \trianglelefteq A_1 \times \cdots \times A_n$. Then

$$\mathfrak{a} = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$$

where $\mathfrak{a}_i \trianglelefteq A_i$ is the set of $a_i \in A_i$ such that for some $\prod_{j \neq i} a_j \in \prod_{j \neq i} A_j$, we have $(a_1, \ldots, a_n) \in \mathfrak{a}$.

Proof. Clearly we have $\mathfrak{a} \leq \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$. So we only have to prove the other way around. Let $(a_1, \ldots, a_n) \in \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$. By definition, for all i, there exists some $r^{(i)} \in \mathfrak{a}$ such that $r_i^{(i)} = a_i$. Consider

$$e_i \triangleq (0, \ldots, \overset{i}{1}, \ldots, 0) \in A$$

We then see

$$(a_1, \ldots, a_n) = \sum_{i=1}^{n} e_i r^{(i)} \in \mathfrak{a}$$

∎

We say a ring homomorphism $\pi : A \twoheadrightarrow A/\mathfrak{a}$ satisfies the **universal property of quotient ring** $A/\mathfrak{a}$ if

(i) π vanishes on $\mathfrak{a}$. **(Ring condition)**

(ii) For all ring homomorphism $f : A \to B$ that vanishes on $\mathfrak{a}$ there exist a unique ring homomorphism $\widetilde{f} : A/\mathfrak{a} \to B$ that makes the diagram:

$$
\begin{array}{ccc}
A & \xrightarrow{\ \ \pi\ \ } & A/\mathfrak{a} \\
 & {\scriptstyle f}\searrow & \Big\downarrow {\scriptstyle \widetilde{f}} \\
 & & B
\end{array}
$$

   commute. **(Universality)**

Equivalent Definition 2.3.6. (Prime ideals and integral domains) We say a *nonzero* ring D is an **integral domain** if any of the followings hold true:

(i) D has no nonzero zero divisor.

(ii) The zero ideal (0) is prime.

(iii) For any nonzero $a \in D$, the cancellative law holds: $ab = ac \implies b = c$.

(iv) For any nonzero $a \in D$, the map $D \longrightarrow D; x \mapsto xa$ is injective.

(v) D is isomorphic to a subring of a field.

Let A be a ring, we say $\mathfrak{p} \triangleleft A$ is **prime** if whenever the product of two elements lies in $\mathfrak{p}$, one of them lies in $\mathfrak{p}$. Therefore,

$$\mathfrak{p} \trianglelefteq A \text{ is prime} \iff A/\mathfrak{p} \text{ is an integral domain}$$

Proof. Routine. ∎

Theorem 2.3.7. (Basic properties of prime ideals) Let A be a ring. Then

(i) $\mathrm{Spec}(A)$ has minimal elements. In particular, by correspondence theorem for rings, every ideal $\mathfrak{a} \trianglelefteq A$ admits a **minimal prime ideal over** $\mathfrak{a}$, a prime ideal minimal among the prime ideals containing $\mathfrak{a}$.

(ii) Let Z be the semigroup of zero-divisors of A and Σ be the set of ideals of A that are contained by Z. Then maximal elements of Σ exist and are prime, and their union $= Z$.

(iii) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(A)$. Then

$$\mathfrak{a} \leq \bigcup_{i=1}^{n} \mathfrak{p}_i \implies \mathfrak{a} \leq \mathfrak{p}_i \text{ for some } i$$

(iv) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq A$ and $\mathfrak{p} \in \operatorname{Spec}(A)$. Then

$$\bigcap_{i=1}^{n} \mathfrak{a}_i \leq \mathfrak{p} \implies \mathfrak{a}_i \leq \mathfrak{p} \text{ for some } i$$

and

$$\bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{p} \implies \mathfrak{a}_i = \mathfrak{p} \text{ for some } i$$

Proof. (i): This is an application of Zorn's Lemma. We show that the ideal $\mathfrak{q} \triangleq \bigcap_{i=1}^{\infty} \mathfrak{p}_i$ is prime, where $\{\mathfrak{p}_i\}$ is a decreasing sequence of prime ideals. Let $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$. We are required to show $y \in \mathfrak{q}$. The proof then follows from noting that since $x \notin \mathfrak{p}_i$ for some i, x can't lies in any higher term, which forces y to lie in all higher terms.

(ii): Clearly Σ and $\Sigma_{\geq \mathfrak{a}} \triangleq \{\mathfrak{b} \in \Sigma : \mathfrak{b} \geq \mathfrak{a}\}$ satisfies the hypothesis of Zorn's lemma for all $\mathfrak{a} \in \Sigma$, so we know maximal elements of Σ exist with union $= Z$. Let $\mathfrak{p} \in \Sigma$ be a maximal element. It remains to show $\mathfrak{p}$ is prime.

Let $x, y \notin \mathfrak{p}$. We are required to show $xy \notin \mathfrak{p}$. Because $x, y \notin \mathfrak{p}$, we know $(x) + \mathfrak{p}$ and $(y) + \mathfrak{p}$ both contains some non-zero-divisors. The product of the two non-zero-divisors, which is a non-zero-divisor, then lies in $(xy) + \mathfrak{p}$, which can only happen if $xy \notin \mathfrak{p}$, as desired.

(iii): We prove

$$\mathfrak{a} \not\leq \mathfrak{p}_i \text{ for all } i \implies \mathfrak{a} \not\leq \bigcup_{i=1}^{n} \mathfrak{p}_i$$

by induction. The base case $n = 1$ is clear. We now prove the inductive case. By inductive hypothesis, for all $1 \leq i \leq n$, there exist some $x_i \in \mathfrak{a} - \bigcup_{j \neq i} \mathfrak{p}_j$. If there exists some $x_i \notin \mathfrak{p}_i$, then we are done. If there isn't, then we have

$$y \triangleq \sum_{i=1}^{n} x_1 x_2 \cdots x_{i-1} x_{i+1} x_{i+2} \cdots x_n \in \mathfrak{a} - \bigcup_{i=1}^{n} \mathfrak{p}_i$$

72

(iv): The first statement is proved by assuming for a contradiction that $x_i \in \mathfrak{a}_i - \mathfrak{p}$ for all i, and then observe that $\prod x_i \in \bigcap \mathfrak{a}_i - \mathfrak{p}$ since $\mathfrak{p} \in \mathrm{Spec}(A)$. Let $\bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{p}$. By first statement, $\mathfrak{a}_i \leq \mathfrak{p}$ for some i. We then see that the equality must holds, otherwise $\bigcap \mathfrak{a}_i < \mathfrak{p}$. ∎

Equivalent Definition 2.3.8. (Maximal ideals and fields) A proper ideal $\mathfrak{m} \triangleleft A$ is said to be **maximal** if it is maximal among the proper ideals of A. We say a *nonzero* ring F is a **field** if and of the followings hold true:

(i) Every nonzero element of F is a unit.

(ii) The only ideal of F are 0 and (1).

(iii) Every homomorphism $F \hookrightarrow B \neq 0$ into a ring $\neq 0$ is injective.

Let A be a ring. Therefore, by correspondence theorem for rings,

$$\mathfrak{m} \subseteq A \text{ is maximal} \iff A/\mathfrak{m} \text{ is a field}$$

Because of such, maximal ideals are prime.

Proof. Routine. We prove (iii) $\implies$ (i). Let $x \in F$ be a non-unit. We are required to prove that $x = 0$. Because $(x) \neq (1)$, $F/(x) \neq 0$. Then the canonical projection $\pi : F \to F/(x)$ is injective, which forces $x = 0$, since $\pi(x) = 0$. ∎

Theorem 2.3.9. (Basic properties of maximal ideals) Let A be a ring. Then

(i) Every proper ideal $\mathfrak{a} \neq (1)$ is contained by some maximal ideal.

(ii) Every non-unit is contained by some maximal ideal.

(iii) If for all $x \in A$, there exists some $n > 1$ that makes $x^n = x$, then $\mathrm{Spec}(A) = \mathrm{Max}(A)$.

Proof. (ii) follows from (i), since the ideal generated by a non-unit must be proper. (i) follows from applying *Zorn's lemma* on the set of ideals in $A/\mathfrak{a}$ and correspondence theorem for rings.

(iii): Let $\mathfrak{p} \in \mathrm{Spec}(A)$ and $x \in A - \mathfrak{p}$. We are required to show $(x + \mathfrak{p}) \in A/\mathfrak{p}$ has an inverse. Because $A/\mathfrak{p}$ is an integral domain, we may apply cancellation law on $(x + \mathfrak{p})^n = (x + \mathfrak{p})$ to see $(x + \mathfrak{p})^{n-1} = 1 + \mathfrak{p}$ in $A/\mathfrak{p}$. This implies $(x + \mathfrak{p})^{n-2}$ is the desired inverse of $x + \mathfrak{p}$. ∎

Equivalent Definition 2.3.10. (Comaximal ideal pairs) Let A be a ring with $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$. We say $\mathfrak{a}, \mathfrak{b}$ are **comaximal** if any of the followings hold true:

(i) $\mathfrak{a} + \mathfrak{b} = (1)$.

(ii) $a + b = 1$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq A$, and consider the natural ring homomorphism $A \xrightarrow{\phi} \prod A / \mathfrak{a}_i$. Since $\ker \phi = \bigcap \mathfrak{a}_i$, we know ϕ is injective if and only if $\bigcap \mathfrak{a}_i = 0$. We also have:

$$\phi \text{ is surjective} \iff \mathfrak{a}_i \text{ are pairwise comaximal} \tag{2.1}$$

which implies **Chinese remainder theorem for integers** by counting cardinality. Moreover, we have:

$$\mathfrak{a}_i \text{ are pairwise comaximal} \implies \prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i \tag{2.2}$$

Proof. We first prove Statement 2.1 ($\implies$): We show $\mathfrak{a}_1, \mathfrak{a}_2$ are comaximal. Because ϕ is surjective, we know there exists $x \in A$ such that

$$x \equiv 1 \pmod{\mathfrak{a}_1} \quad \text{and} \quad x \equiv 0 \pmod{\mathfrak{a}_i} \pmod{\mathfrak{a}_i} \text{ for all } i \geq 2 \tag{2.3}$$

We now see that $1 - x \in \mathfrak{a}_1$ and $x \in \mathfrak{a}_2$, as desired.

($\impliedby$): Clearly, we only have to show the existence of some $x \in A$ that satisfies equation 2.3. Because $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are pairwise comaximal, for all $i \geq 2$, we may find $u_i \in \mathfrak{a}_1$ and $v_i \in \mathfrak{a}_i$ that makes $u_i + v_i = 1$. Direct computation shows that $x \triangleq \prod_{i=2}^{n} v_i$ suffices.

We now prove statement 2.2, which relies on induction. Note that we always have $\leq$, so we only have to prove $\geq$. Let $a_1 + a_2 \triangleq 1$ with $a_1 \in \mathfrak{a}_1$ and $a_2 \in \mathfrak{a}_2$. The base case $n = 2$ then follows from noting that

$$x \in \mathfrak{a}_1 \cap \mathfrak{a}_2 \implies x = xa_1 + xa_2 \in \mathfrak{a}_1 \mathfrak{a}_2$$

We now prove the inductive case. Let $x_i + y_i \triangleq 1$ with $x_i \in \mathfrak{a}_i$ and $y_i \in \mathfrak{a}_n$ for all $i \leq n - 1$. We then have

$$\prod_{i=1}^{n-1} x_i \equiv 1 \pmod{\mathfrak{a}_n}$$

which implies $\mathfrak{a}_n$ and $\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}$ are comaximal. Therefore, by inductive hypothesis, we have

$$\prod_{i=1}^{n} \mathfrak{a}_i = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

$\blacksquare$

Theorem 2.3.11. (Isomorphism theorems for rings) Let $f : A \to B$ be a ring homomorphism. The first isomorphism theorem stated that the induced map $\widetilde{f} : A/\ker(f) \hookrightarrow B$ is injective. Let B be a subring of A, and $\mathfrak{a} \trianglelefteq A$. The second isomorphism theorem stated that:

(i) $B + \mathfrak{a} \triangleq \{b + a \in A : b \in B, a \in \mathfrak{a}\}$ forms a subring of A.

(ii) $B \cap \mathfrak{a}$ forms an ideal in B.

(iii) $(B + \mathfrak{a})/\mathfrak{a} \cong B/(B \cap \mathfrak{a})$ as rings.

Let $\mathfrak{a} \trianglelefteq A$ and $\pi : A \twoheadrightarrow A/\mathfrak{a}$ be the canonical ring homomorphism. The third isomorphism theorem stated that for all $\mathfrak{a} \leq \mathfrak{b} \trianglelefteq A$, the subset $\pi(\mathfrak{b}) \trianglelefteq A/\mathfrak{a}$ forms an ideal, and the natural map

$$(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong A/\mathfrak{b}, \quad \text{where } \mathfrak{b}/\mathfrak{a} \triangleq \pi(\mathfrak{b}) \tag{2.4}$$

forms a ring isomorphism. The **spectrum** $\mathrm{Spec}(A)$ is the set of prime ideals in A, and the **maximal spectrum** $\mathrm{Max}(A)$ is the set of maximal ideals in A.

The correspondence theorem for rings stated that equation 2.4 forms a bijection between the collection of ideals of A that contains $\mathfrak{a}$ and ideals of $A/\mathfrak{a}$, a bijection between the collection of prime ideals of A that contains $\mathfrak{a}$ and $\mathrm{Spec}(A/\mathfrak{a})$, and a bijection between the collection of maximal ideals of A that contains $\mathfrak{a}$ and $\mathrm{Max}(A/\mathfrak{a})$.

Also, given arbitrary $\mathfrak{c} \trianglelefteq A$, we always have

$$\pi(\mathfrak{c}) = (\mathfrak{c} + \mathfrak{a})/\mathfrak{a}$$

Proof. Routine. ∎

2.4 Radical Ideals

Equivalent Definition 2.4.1. (Nilradical and Jacobson radical) Let A be a ring. The set $\mathrm{Nil}(A)$ of nilpotents in A clearly forms an ideal, and is called the **nilradical**. We have:

$$\mathrm{Nil}(A) = \bigcap \mathrm{Spec}(A) \tag{2.5}$$

Clearly, $A/\mathrm{Nil}(A)$ has no nilpotent $\neq 0$. We define the **Jacobson radical** $\mathrm{Jac}(A)$ by

$$\mathrm{Nil}(A) \leq \mathrm{Jac}(A) \triangleq \bigcap \mathrm{Max}(A)$$

For all $x \in A$, we have:

$$x \in \mathrm{Jac}(A) \iff 1 - xy \in A^\times, \quad \text{for all } y \in A \tag{2.6}$$

Proof. Equation 2.5: $\mathrm{Nil}(A) \leq \bigcap \mathrm{Spec}\, A$ is clear. Assume $x \in \bigcap \mathrm{Spec}\, A - \mathrm{Nil}(A)$ for a contradiction. Let Σ be the set of ideals $\mathfrak{a}$ such that $x^n \notin \mathfrak{a}$ for all $n > 0$. Because unions of chains in Σ belong to Σ and because $0 \in \Sigma$, by Zorn's Lemma, there exists some maximal element $\mathfrak{a} \in \Sigma$. Because $x \notin \mathfrak{a}$, to close out the proof, we only have to show $\mathfrak{a}$ is prime.

Let $yz \in \mathfrak{a}$. Assume for a contradiction that $y \notin \mathfrak{a}$ and $z \notin \mathfrak{a}$. By maximality of $\mathfrak{a}$, both $\mathfrak{a} + (y), \mathfrak{a} + (z)$ don't belong to Σ. This implies $x^n \in \mathfrak{a} + (y)$ and $x^m \in \mathfrak{a} + (z)$ for some $n, m > 0$, which cause a contradiction to $\mathfrak{a} \in \Sigma$, since $x^{n+m} \in \mathfrak{a} + (yz) = \mathfrak{a}$.

Statement 2.6: ($\implies$): Assume for a contradiction that $1 - xy$ is a non-unit, and therefore contained by some maximal ideal $\mathfrak{m}$. The contradiction then follows from noting that since $x \in \mathfrak{m}$, we have $1 \in \mathfrak{m}$, which is impossible.

($\impliedby$): Assume for a contradiction that $x \notin \mathfrak{m}$ for some $\mathfrak{m} \in \mathrm{Max}(A)$. This forces $\mathfrak{m} + (x) = (1)$, which implies the existence of some $m \in \mathfrak{m}$ and $y \in A$ that makes $m + xy = 1$. Therefore by premise, $m \in A^\times$, which contradicts to $m \in \mathfrak{m}$. ∎

Example 2.4.2: $\mathrm{Nil}(A) = \mathrm{Jac}(A)$ **doesn't require** $\mathrm{Spec}(A) = \mathrm{Max}(A)$.

Let $A \triangleq \mathbb{C}[x]$. Fundamental theorem of algebra implies

$$\mathrm{Spec}(A) = \{(x - \lambda) \trianglelefteq A : \lambda \in \mathbb{C}\} \cup \{(0)\}$$

Therefore, we know

$$\mathrm{Max}(A) = \{(x - \lambda) \trianglelefteq A : \lambda \in \mathbb{C}\}$$

and $\mathrm{Nil}(A) = \mathrm{Jac}(A) = 0$.

Theorem 2.4.3. (Criteria for $\mathrm{Nil}(A) = \mathrm{Jac}(A)$**)** Let A be a ring. If every ideal of A not contained by $\mathrm{Nil}(A)$ contains a nonzero idempotent, then $\mathrm{Nil}(A) = \mathrm{Jac}(A)$.

Proof. Let $x \in A - \mathrm{Nil}(A)$. Clearly $(x) \not\subseteq \mathrm{Nil}(A)$. Therefore, $(1 - xa)xa = 0$ for some $a \in A$ that makes $xa \neq 0$. This implies $1 - xa$ is a zero-divisor, which implies $x \notin \mathrm{Jac}(A)$, as desired. ∎

> **Example 2.4.4: The set of zero-divisors doesn't form an ideal**
>
> Consider the ring $\mathbb{R} \times \mathbb{R}$. The sum of the zero-divisors $(0, 1)$ and $(1, 0)$ isn't a zero-divisor.

Equivalent Definition 2.4.5. (Radical and radical ideal) Let A be a ring and $\mathfrak{a} \trianglelefteq A$. The followings are equivalent:

(i) $\sqrt{\mathfrak{a}} \triangleq \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}$.

(ii) $\{x \in A : x^n \in \mathfrak{a} \text{ for } n \gg 0\}$.

(iii) $\pi^{-1}\left(\mathrm{Nil}(A/\mathfrak{a})\right)$, where $\pi : A \twoheadrightarrow A/\mathfrak{a}$ is the canonical projection.

(iv) $\bigcap V(\mathfrak{a})$, where $V(\mathfrak{a}) \triangleq \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{a} \leq \mathfrak{p}\}$.

We say $\mathfrak{a}$ is a **radical ideal** if any of the followings hold true:

(i) $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

(ii) $\mathfrak{a}$ is an intersection of some set of prime ideals.

Therefore, both nilradical and Jacobson radical are radical ideals.

Proof. The equivalent definition for radical ideal follows from (iv). (i) $\iff$ (ii) $\iff$ (iii) is clear. (iii) $\iff$ (iv) follows from computing

$$
\begin{aligned}
\pi\left(\bigcap \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{a} \leq \mathfrak{p}\}\right) \\
= \bigcap \{\pi(\mathfrak{p}) \in \mathrm{Spec}(A/\mathfrak{p}) : \mathfrak{a} \leq \mathfrak{p} \in \mathrm{Spec}(A)\} \\
= \bigcap \mathrm{Spec}(A/\mathfrak{p}) = \mathrm{Nil}(A/\mathfrak{p})
\end{aligned}
$$

where the second equality follows from correspondence theorem for rings. ∎

Clearly, prime ideals are radical, but radical ideals need not be prime:

Example 2.4.6: Radical ideals need not be prime.

Since $(6) \trianglelefteq \mathbb{Z}$ is the intersection of prime ideals (2) and (3), we know $(6) \trianglelefteq \mathbb{Z}$ is radical, but since $2 \cdot 3 \in (6)$, we see $(6) \trianglelefteq \mathbb{Z}$ isn't prime.

Theorem 2.4.7. (Basic properties of radicals) Let $\mathfrak{a} \trianglelefteq A$. Then

$$V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}}) \tag{2.7}$$

In other words, $\mathfrak{a}$ and $\sqrt{\mathfrak{a}}$ share the same set of prime ideals containing them. Because of such, we also have:

$$V(\mathfrak{a}) \subseteq V(\mathfrak{b}) \iff \sqrt{\mathfrak{a}} \geq \sqrt{\mathfrak{b}}$$

We also have

$$\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}} \quad \text{and} \quad \sqrt{\mathfrak{a}} = (1) \iff \mathfrak{a} = (1)$$

and the followings properties:

(i) $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.

(ii) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$.

(iii) If $\sqrt{\mathfrak{a}}, \sqrt{\mathfrak{b}}$ are comaximal, then $\mathfrak{a}, \mathfrak{b}$ are comaximal.

(iv) Given $\mathfrak{p} \in \mathrm{Spec}(A)$, we have $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n > 0$.

(v) The multiplicative semigroup of zero-divisors $= \bigcup_{x \neq 0} \sqrt{\mathrm{Ann}(x)}$.

Proof. Note that $V(\mathfrak{a}) \supseteq V(\sqrt{\mathfrak{a}})$ follows trivially form $\mathfrak{a} \leq \sqrt{\mathfrak{a}}$, and that $V(\mathfrak{a}) \subseteq V(\sqrt{\mathfrak{a}})$ follows from $\sqrt{\mathfrak{a}} = \bigcap V(\mathfrak{a})$. Note that $V(\mathfrak{a}) \subseteq V(\mathfrak{b}) \implies \sqrt{\mathfrak{a}} \geq \sqrt{\mathfrak{b}}$ follows from $\sqrt{\mathfrak{a}} = \bigcap V(\mathfrak{a})$, while $\sqrt{\mathfrak{a}} \geq \sqrt{\mathfrak{b}} \implies V(\mathfrak{a}) \subseteq V(\mathfrak{b})$ follows trivially from equation 2.7.

(i): We prove $\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} \leq \sqrt{\mathfrak{a}\mathfrak{b}}$. Let $x^n \in \mathfrak{a} \cap \mathfrak{b}$. Then $x^{2n} = x^n x^n \in \mathfrak{a}\mathfrak{b}$.

(ii): We prove $\sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} \leq \sqrt{\mathfrak{a} + \mathfrak{b}}$. Let $x^n \triangleq y + z$ where $y^m \in \mathfrak{a}$ and $z^k \in \mathfrak{b}$. Then $x^{n(m+k)} = (y + z)^{m+k} \in \mathfrak{a} + \mathfrak{b}$.

(iii): This follows from computing $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} = \sqrt{(1)} = (1)$.

(iv): Clearly, we have $\mathfrak{p} \leq \sqrt{\mathfrak{p}^n}$. Let $x \in \sqrt{\mathfrak{p}^n}$. Then $x^m \in \mathfrak{p}^n \leq \mathfrak{p}$ for some m, which implies $x \in \mathfrak{p}$ by primality of $\mathfrak{p}$.

(v): Let $x \neq 0$ and $y^n \in \text{Ann}(x)$ with $y^{n-1} \notin \text{Ann}(x)$. Then $y(y^{n-1}x) = y^n x = 0$ shows that y is a zero-divisor. If $y \neq 0$ is a zero-divisor with $xy = 0$ and $x \neq 0$. Then $y \in \sqrt{\text{Ann}(x)}$. $\blacksquare$

2.5 Finitely Generated Modules

We say an A-module homomorphism $\pi : M \twoheadrightarrow M/N$ satisfies the **universal property of quotient module** M/N if

(i) π vanishes on N. (**Module condition**)

(ii) For all A-module homomorphism $f : M \to P$ that vanishes on $\mathfrak{a}$ there exist a unique ring homomorphism $\widetilde{f} : M/N \to P$ that makes the diagram:

$$
\begin{array}{ccc}
M & \xrightarrow{\ \ \pi\ \ } & M/N \\
 & {\scriptstyle f}\searrow & \downarrow {\scriptstyle \widetilde{f}} \\
 & & P
\end{array}
$$

commute. (**Universality**)

Theorem 2.5.1. (Isomorphism theorems and correspondence theorems for modules) Let $f : M \to N$ be an A-module homomorphism. The first isomorphism theorem for modules stated that

$$M/\ker(f) \cong \operatorname{Im}(f)$$

Let P, Q be two submodules of M. The second isomorphism theorem for modules stated that

$$\frac{P+Q}{Q} \cong \frac{P}{P \cap Q}$$

Let $M \leq L$ be A-modules, and $\pi : L \twoheadrightarrow L/M$ be the canonical A-module homomorphism. Denoting

$$\frac{K}{M} \triangleq \pi(K) \leq \frac{L}{M}$$

for all modules K containing M, the third isomorphism theorem for modules stated that

$$(L/M)/(K/M) \cong L/K$$

The correspondence theorem for modules stated that the third isomorphism theorem induces a bijection between submodules of L/M and submodules of L containing M.

Proof. Routine. ∎

Theorem 2.5.2. (Structure theorem for finitely generated modules) Let M be an A-module. Then

$$M \text{ is finitely generated} \iff M \cong A^n/\mathfrak{a} \text{ for some } n > 0 \text{ and } \mathfrak{a} \leq A^n$$

Proof. ($\implies$): Let $M \triangleq (x_1, \ldots, x_n)$. Define $\phi : A^n \to M$ by $\phi(a_1, \ldots, a_n) \triangleq a_1 x_1 + \cdots + a_n x_n$, which is clearly surjective. Then by first isomorphism theorem for modules, we see $M \cong A^n / \ker(\phi)$.

($\impliedby$): M is clearly generated by $\{e_i \in A^n/\mathfrak{a}\}$, where $e_i \triangleq (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 being in the i-th slot. ∎

Example 2.5.3: Submodules of finitely generated modules need not be finitely generated (over a non-noetherian ring)

Let $A \triangleq \mathbb{R}[X_1, X_2, \ldots]$ and define $\mathfrak{a} \trianglelefteq A$ by

$$\mathfrak{a} \triangleq (X_1, X_2, \ldots)$$

Because $A = (1)$, we know A as an A-module is finitely generated. To see $(X_1, X_2, \ldots)$ isn't finitely generated, assume for a contradiction that $(X_1, X_2, \ldots,) = (f_1, \ldots, f_m)$. Let X_k be a variable that doesn't occur in any of f_i. Then since $X_k \in (f_1, \ldots, f_m)$, we may write $X_k = g_1 f_1 + \cdots + g_m f_m$ for some $\{g_i \in A : 1 \leq i \leq m\}$. Therefore, X_k must occur in some $g_i f_i$, which is only possible if X_k occurs in g_i and f_i has nonzero constant term. This then cause a contradiction to $f_i \in (X_1, X_2, \ldots)$.

Theorem 2.5.4. (Finitely generated modules are closed under extension) Given a short exact sequence of module:

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

If M' and M'' are finitely generated, then M is finitely generated.

Proof. Let $M' \triangleq (x_1, \ldots, x_n)$, $M'' \triangleq (y_1, \ldots, y_m)$, and $x \in M$. To see that x can be generated by x_i and y_i, just observe that since for some b_j we have:

$$x + M' \triangleq \sum b_j y_j + M'$$

we know for some a_i we have

$$x = \sum a_i x_i + \sum b_j y_j$$

∎

Theorem 2.5.5. (Basic properties of finitely generated modules) Let M be a finitely generated A-module $(x_1, \ldots, x_m)$ and $\phi : M \twoheadrightarrow A^n$ be a surjective homomorphism. Then $\ker(\phi)$ is finitely generated.

Proof. Clearly, we have a short exact sequence

$$0 \longrightarrow \ker(\phi) \lhook\joinrel\longrightarrow M \overset{\phi}{\longrightarrow\joinrel\rightarrow} A^n \longrightarrow 0$$

Let $e_1, \ldots, e_n$ be the basis for A^n, and let $u_i \in M$ satisfy $\phi(u_i) = e_i$. We then see that the sequence right splits via $s : A^n \to M$ defined by $s(e_i) \triangleq u_i$. Therefore, by splitting lemma, we have $M \cong \ker(\phi) \oplus A^n$. Write

$$x_i = t_i + \sum_{j=1}^{n} a_j u_j \text{ for all } 1 \leq i \leq m$$

We now see $\ker(\phi) = (t_1, \ldots, t_m)$. ∎

Theorem 2.5.6. (Generalized Cayley-Hamilton theorem) Let M be a finitely generated A-module, $\mathfrak{a} \lhd A$, and ϕ an A-module endomorphism of M such that $\phi(M) \leq \mathfrak{a}M$. Then for some $n \geq 1$, ϕ satisfies an equation of the form

$$\phi^n + a_1 \phi^{n-1} + \cdots + a_n = 0, \quad \text{where } a_i \in \mathfrak{a}$$

Proof. Let $M \triangleq (x_1, \ldots, x_n)$. Because $\phi(M) \leq \mathfrak{a}M$, we may write $\phi(x_i) \triangleq \sum_{j=1}^{n} a_{ij} x_j$ where $a_{i,j} \in \mathfrak{a}$. Therefore, for all i, we have

$$\sum_{j=1}^{n} \left(\delta_{ij} \phi - a_{ij} \right) x_j = 0$$

Multiplying from the left the adjugate of the matrix $\delta_{ij} \phi - a_{ij} \in M_n(A[\phi])$, we now see that $\det(\delta_{ij} \phi - a_{ij}) \in A[\phi]$ is the polynomial we are looking for. ∎

Theorem 2.5.7. (First version of Nakayama lemma) Let M be a finitely generated A-module and $\mathfrak{a} \lhd A$ satisfies $\mathfrak{a}M = M$. Then there exists $x \equiv 1 \pmod{\mathfrak{a}}$ that makes $xM = 0$.

Proof. Because $\mathfrak{a}M = M$, we know $1 \in \text{End}(M)$ satisfies $1(M) \leq \mathfrak{a}M$. Therefore, we may generalized Cayley-Hamilton to see that $x \triangleq 1 + a_1 \cdots + a_n$ suffices. ∎

Theorem 2.5.8. (Second version of Nakayama lemma) Let M be a finitely generated A-module and $\mathfrak{a} \lhd A$ satisfies $\mathfrak{a}M = M$. If $\mathfrak{a} \leq \text{Jac}(A)$, then $M = 0$.

Proof. Because $\mathfrak{a} \leq \text{Jac}(A)$, first version of Nakayama lemma implies the existence of some $x \in A$ such that

$$x \equiv 1 \pmod{\text{Jac}(A)} \quad \text{and} \quad xM = 0$$

By definition of Jacobson radical, $x \equiv 1 \pmod{\text{Jac}(A)}$ implies $x \in A^{\times}$. Therefore, we have $M = x^{-1}xM = 0$, as desired. $\blacksquare$

Theorem 2.5.9. (Third version of Nakayama lemma) Let M be a finitely generated A-module with $N \leq M$ and $\mathfrak{a} \leq \text{Jac}(A)$. If $M = \mathfrak{a}M + N$, then $M = N$.

Proof. By second version of Nakayama lemma, it suffices to show $\mathfrak{a}(M / N) = M / N$, which follows from computing

$$\mathfrak{a}(M / N) = \mathfrak{a}M + N / N = M / N$$

$\blacksquare$

Corollary 2.5.10. (Algebraic consequences of Nakayama lemmas) Let A be a ring. Then

(i) Let $(A, \mathfrak{m}, k)$ be a local ring and M be an A-module. If $\{x_i + \mathfrak{m}M : 1 \leq i \leq n\}$ forms a basis for the k-vector space $M / \mathfrak{m}M$, then $M = (x_1, \ldots, x_n)$.

(ii) Let N, M be two A-modules with M finitely generated and $\mathfrak{a} \leq \text{Jac}(A)$. Let $u : N \to M$ be a homomorphism. If the induced homomorphism $\widetilde{u} : N / \mathfrak{a}N \twoheadrightarrow M / \mathfrak{a}M$ is surjective, then u is surjective.

Proof. (i): Let $N \triangleq (x_1, \ldots, x_n) \leq M$. We are required to prove $N = M$, which follows third version of Nakayama lemma and the fact that $N + \mathfrak{m}M = M$.

(ii): The proof follows from third version of Nakayama lemma and the observation that $M = u(N) + \mathfrak{a}M$. $\blacksquare$

2.6   Tensor Products

Given a *finite* collection $M_1, \ldots, M_n$ of A-modules, their **tensor product** is an A-module $M_1 \otimes \cdots \otimes M_n$ together with a multilinear map $\otimes : M_1 \times \cdots \times M_n \to M_1 \otimes \cdots \otimes M_n$ that satisfies the **universal property for tensor product**: For each multilinear map $f : M_1 \times \cdots \times M_n \to P$, there exists an unique module homomorphism $\widetilde{f} : M_1 \otimes \cdots \otimes M_n \to P$ such that the diagram

$$\prod M_i \xrightarrow{\ \otimes\ } \bigotimes M_i$$

with f to P and $\widetilde{f}$ to P

commutes.

Example 2.6.1: Non-zero modules can have zero tensor product.

Let $m, n \in \mathbb{N}$ be coprime with $am + bn = 1$. Then we have

$$\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = 0$$

since

$$x \otimes y = (am + bn)(x \otimes y) = a(mx \otimes y) + b(x \otimes ny) = 0$$

Given two module homomorphisms $f : M \to M'$ and $g : N \to N'$, clearly we can induce another module homomorphism $f \otimes g : M \otimes N \to M' \otimes N'$ by

$$(f \otimes g)(m \otimes n) \triangleq f(m) \otimes g(n)$$

In particular, for all $M_0 \leq M$ and $N_0 \leq N$, given $x \in M_0$ and $y \in N_0$ that makes $x \otimes y = 0$ in $M_0 \otimes N_0$, the module homomorphism from $M_0 \otimes N_0$ to $M \otimes N$ tell us that $x \otimes y$ must also be 0 in $M \otimes N$. The converse however is not true. That is, given $x \in M_0$ and $y \in N_0$ with $x \otimes y = 0$ in $M \otimes N$, we don't always have $x \otimes y = 0$ in $M_0 \otimes N_0$.

In short, if an expression is zero in a tensor products of submodules, then it must be zero in the parent tensor product, but an expression being zero in the parent tensor product can still be nonzero in the tensor product of submodules.

Example 2.6.2: Zero expression in $M \otimes N$ can be nonzero in $M_0 \otimes N_0$ for $M_0 \le M$ and $N_0 \le N$.

Consider $A \triangleq \mathbb{Z}$, $M \triangleq \mathbb{Z}$, and $N \triangleq \mathbb{Z}_2$. Let $M_0 \triangleq 2\mathbb{Z} \le M$ and $x \in N$ be the nonzero element. Then in $M \otimes N$, we have

$$2 \otimes x = 2(1 \otimes x) = 1 \otimes 2x = 0$$

Yet in $M_0 \otimes N$, we can't have $2 \otimes x = 0$, since if so, then $M_0 \otimes N = 0$, but

$$M_0 \otimes N \cong \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2 \ne 0$$

However, we do have the following existence result.

Theorem 2.6.3. (Existence of finitely generated submodules that makes an expression of zero remain zero) Let A be a ring and M and N two A-modules. Let $\sum x_i \otimes y_i = 0$ in $M \otimes N$. Then there exist two finitely generated submodules $M' \le M$ and $N' \le N$ that respectively contains x_i and y_i and makes

$$\sum x_i \otimes y_i = 0, \quad \text{in } M' \otimes N'$$

Proof. Let M_i and N_j be the directed system of finitely generated submodules of M and N. Then we have a natural isomorphism

$$M \otimes N \cong \left(\varinjlim M_i \right) \otimes \left(\varinjlim N_j \right) \cong \varinjlim (M_i \otimes N_j)$$

Let $M' \le M$ and $N' \le N$ be the submodules generated by x_i and y_i. Clearly, the isomorphism maps $\sum x_i \otimes y_i \in M' \otimes N'$ to $0 \in M \otimes N$ (from the right hand side to left). The proof then follows from the fact that if something in a direct limit is zero then at a fixed stage it is already zero. ∎

Let N be an A-module. If we say N is an (A, B)-**bimodule** we mean that the abelian group N has a B-module structure compatible with its A-module structure in the sense that

$$b \cdot (a \cdot n) = a \cdot (b \cdot n), \quad \text{for all } a \in A, b \in B, n \in N$$

An (A, B)-**bimodule homomorphism** $g : N \to P$ is then a map that is simultaneously an A-module homomorphism and a B-module homomorphism. Let M be an A-module and N an (A, B)-bimodule. Clearly, by universal property, we can give $M \otimes_A N$ a B-module structure by

$$b(m \otimes n) \triangleq m \otimes bn \tag{2.8}$$

which naturally makes $M \otimes_A N$ an (A, B)-bimodule.

Example 2.6.4: Lifting of module structures requires bimodules.

Let k be a field, $A \triangleq k[x]$, $M \triangleq N \triangleq A$, and $B \triangleq k[y]$. Clearly, we may give N a B-module structure by

$$cy^n \cdot f \triangleq cf^{(n)}, \quad \text{for all } c \in k, f \in N$$

It is clear that the A-module structure and the B-module structure on N are not compatible. Therefore, we can't use universal property to give $M \otimes_A N$ a B-module structure as in equation 2.8. To see this *as a hindsight*, first observe

$$1 \otimes x = x(1 \otimes 1) = 1 \otimes x$$

So if there exists a B-module structure on $M \otimes_A N$ that agrees with equation 2.8, then we have

$$1 \otimes 1 = y(1 \otimes x) = y(x \otimes 1) = 0$$

This is clearly impossible, since it suggests $M \otimes N = 0$, but

$$M \otimes N \cong A \otimes A \cong A \neq 0$$

In particular, given a ring homomorphism $f : A \to B$, restriction of scalars makes B an (A, B)-bimodules, and so for all A-module M, we have an (A, B)-bimodule:

$$M_B \triangleq M \otimes_A B$$

called **extension of scalar**.

Theorem 2.6.5. (Criteria for finite generation under extension and restriction of scalars) Let $f : A \to B$ be a ring homomorphism, M an A-module and N a B-module. Then

(i) If N is finitely generated as a B-module and B is finitely generated as an A-module, then N is finitely generated as an A-module.

(ii) If M is finitely generated as an A-module, then M_B is finitely generated as a B-module.

Proof. (i): If $y_1, \ldots, y_m$ generate N over B and $b_1, \ldots, b_n$ generate B over A, then clearly $\{b_i y_j \in N : 1 \leq i \leq n, 1 \leq j \leq m\}$ generate N over A.

(ii): If $x_1, \ldots, x_m$ generate M over A, then $1 \otimes x_i$ generate M_B over B. In particular

$$b \otimes \sum a_i x_i = \sum b \otimes a_i x_i = \sum a_i (b \otimes x_i) = \sum (bf(a_i)) \otimes x_i$$

$\blacksquare$

Because for generic $f' : M' \to M''$ and $g' : N' \to N''$, we clearly have:

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$$

For all (A, B)-bimodule N, the tensor product $- \otimes_A N$ forms a clearly additive *covariant* functor from $\mathbf{Mod}_A$ to $\mathbf{Mod}_{(A,B)}$ with the action

$$f \mapsto f \otimes \mathbf{id}_N \tag{2.9}$$

Theorem 2.6.6. (Basic property of tensor products) Let $M_1, \ldots, M_n$ and N be A-modules. Then

(i) $M_1 \otimes \cdots \otimes M_n$ is generated by **basic elements** $x_1 \otimes \cdots \otimes x_n$.

(ii) There is a natural isomorphism

$$\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, P))$$

called the **tensor-hom adjunction** that maps f to f', where $f'(m)(n) \triangleq f(m \otimes n)$. In particular, they are both naturally bijective to the set of bilinear maps from $M \times N$ to P.

(iii) The covariant functor $- \otimes_A N$ is *right exact*.

Proof. (ii) is routine. We now prove (i). Let $E \leq M_1 \otimes \cdots \otimes M_n$ be the submodule generated by basic elements with quotient map $\pi : M_1 \otimes \cdots \otimes M_n \twoheadrightarrow E$. We are required to prove that $\pi = 0$. This follows from noting that both π and $0 : M_1 \otimes \cdots \otimes M_n \to (M_1 \otimes \cdots \otimes M_n)/E$ makes the diagram:

$$
\begin{array}{ccc}
M_1 \times \cdots \times M_n & \xrightarrow{\quad \otimes \quad} & M_1 \otimes \cdots \otimes M_n \\
& {}_{0} \searrow & \Big\downarrow {\scriptstyle \tilde{0}} \\
& & (M_1 \otimes \cdots \otimes M_n)/E
\end{array}
$$

commutes. Lastly, we prove (iii). Consider the exact sequence of A-modules:

$$M' \xrightarrow{\quad u \quad} M \xrightarrow{\quad v \quad} M'' \longrightarrow 0$$

Let P be an A-module, and denote the contravariant functor $\mathrm{Hom}(-, P) : \mathbf{Mod}_A \longrightarrow \mathbf{Mod}_A$ by G_P. By property of G_P, we only have to prove

$$0 \longrightarrow \mathrm{Hom}(M'' \otimes N, P) \xrightarrow{G_P(v \otimes 1)} \mathrm{Hom}(M \otimes N, P) \xrightarrow{G_P(u \otimes 1)} \mathrm{Hom}(M' \otimes N, P)$$

is exact. Now, because tensor-hom adjunction gives an equivalent sequence:

$$0 \longrightarrow \mathrm{Hom}(M'', \mathrm{Hom}(N, P)) \xrightarrow{\widetilde{v}} \mathrm{Hom}(M, \mathrm{Hom}(N, P)) \xrightarrow{\widetilde{u}} \mathrm{Hom}(M', \mathrm{Hom}(N, P))$$

we only have to prove this sequence is exact. Denote $G_{\mathrm{Hom}(N,P)} \triangleq \mathrm{Hom}(-, \mathrm{Hom}(N, P))$. The proof then follows from property of $G_{\mathrm{Hom}(N,P)}$ and a routine check of $\widetilde{v} = G_{\mathrm{Hom}(N,P)}(v)$. ∎

Example 2.6.7: Tensor product need not be left-exact

Consider the exact sequence of $\mathbb{Z}$-modules:

$$0 \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$$

where $f(x) \triangleq 2x$. To see that the $\mathbb{Z}$-modules sequence

$$0 \longrightarrow 0 \longrightarrow \mathbb{Z} \otimes \mathbb{Z}_2 \xrightarrow{f \otimes 1} \mathbb{Z} \otimes \mathbb{Z}_2$$

isn't exact. Just observe that $1 \otimes 1 \in \mathbb{Z} \otimes \mathbb{Z}_2$ is nonzero, since if so, then $\mathbb{Z} \otimes \mathbb{Z}_2 \cong \mathbb{Z}_2 \neq 0$ is zero, and observe that:

$$(f \otimes \mathbf{id}_{\mathbb{Z}_2})(1 \otimes 1) = 2 \otimes 1 = 2(1 \otimes 1) = 1 \otimes 2 = 0$$

Even though tensor product as a functor lack the functorality we desired, it still has lots of algebraic identities.

Theorem 2.6.8. (Identities for tensor products) Let A be a ring and M an A-module. Then

(i) We have a natural isomorphism

$$A \otimes M \cong M, \quad a \otimes m \mapsto am$$

(ii) Let $\mathfrak{a} \trianglelefteq A$. We have a natural isomorphism

$$(A / \mathfrak{a}) \otimes M \cong M / \mathfrak{a}M, \quad a \otimes m \mapsto am$$

(iii) Let N and P be two A-modules. We have a natural isomorphism

$$(M \otimes N) \otimes P \cong M \otimes N \otimes P, \quad (m \otimes n) \otimes p \mapsto m \otimes n \otimes p$$

(iv) Let N an (A, B)-bimodule, and P a B-module. We have a natural (A, B)-bimodule isomorphism

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P), \quad (m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$$

(v) Let M_i be a directed system of A-modules with canonical morphism φ. Then $M_i \otimes M$ is a directed system with canonical morphism ψ defined by $\psi_{ij} \triangleq \varphi_{ij} \otimes \mathbf{id}_M$, and we have a natural isomorphism:

$$\left(\varinjlim M_i\right) \otimes M \cong \varinjlim (M_i \otimes M), \quad \varphi_i(m_i) \otimes m \mapsto \psi_i(m_i \otimes m)$$

(vi) For *possibly infinite* collection M_i of A-module, we have a natural isomorphism

$$N \otimes \bigoplus M_i \cong \bigoplus (N \otimes M_i), \quad n \otimes (m_1 \oplus \cdots \oplus m_k) \mapsto (n \otimes m_1) \oplus \cdots \oplus (n \otimes m_k)$$

(vii) Let (M_i, φ) be a directed system of A-modules over directed set $\mathcal{P}$ and (N_j, ψ) be a directed system of A-modules over directed set $\mathcal{Q}$. Then, we can make $M_i \otimes N_j$ a directed system with index set $\mathcal{P} \times \mathcal{Q}$ directed by

$$(i, j) \leq (k, l) \overset{\triangle}{\Longleftrightarrow} i \leq k \quad \text{and} \quad j \leq l$$

and canonical homomorphisms λ defined by

$$\lambda_{(i,j)(k,l)} \triangleq \varphi_{ik} \otimes \psi_{jl}$$

Then the natural directed system of $M_i \otimes N_j$ over $\mathcal{P} \times \mathcal{Q}$ has a natural isomorphism

$$\varinjlim_{\mathcal{P} \times \mathcal{Q}} (M_i \otimes N_j) \cong \varinjlim_{\mathcal{P}} (M_i) \otimes \varinjlim_{\mathcal{Q}} (N_j), \quad \lambda_{(i,j)}(m_i \otimes n_j) \mapsto \varphi_i(m_i) \otimes \psi_j(n_j)$$

(viii) Let $M[x]$ denote the formal abelian group of expression of the form

$$m_0 + m_1 x + \cdots + m_r x^r, \quad \text{where } m_i \in M$$

Then we can give $M[x]$ a natural $A[x]$-module structure, and it has a natural $A[x]$-module isomorphism

$$M[x] \cong A[x] \otimes_A M, \quad \sum m_i x^i \mapsto \sum x^i \otimes_A m_i$$

Proof. (i), (iii), (iv), (v), and (vii) are routine. (ii) is essentially a corollary of (i). In short, because tensor product is right exact, tensoring the exact sequence

$$\mathfrak{a} \overset{i}{\longhookrightarrow} A \overset{\pi}{\twoheadrightarrow} A / \mathfrak{a} \longrightarrow 0$$

with M, we get an exact sequence

$$\mathfrak{a} \otimes M \overset{i \otimes 1}{\longrightarrow} A \otimes M \overset{\pi \otimes 1}{\longrightarrow} (A / \mathfrak{a}) \otimes M \longrightarrow 0$$

which implies that

$$(A/\mathfrak{a}) \otimes M \cong (A \otimes M) / \operatorname{Im}(i \otimes 1)$$

The proof for (ii) then follows from checking that the isomorphism $A \otimes M \cong M$ maps $\operatorname{Im}(i \otimes 1)$ to $\mathfrak{a}M$. (vi) should be first proved in finite case, which is also routine. The infinite case then follows from finite case, (iii), and the fact that direct sum is the direct limit of finite direct sums:

$$N \otimes \left(\bigoplus M_i \right) \cong N \otimes \varinjlim \left(\bigoplus_{\text{finite}} M_i \right) \cong \varinjlim \left(N \otimes \left(\bigoplus_{\text{finite}} M_i \right) \right)$$

$$\cong \varinjlim \left(\bigoplus_{\text{finite}} N \otimes M_i \right) \cong \bigoplus (N \otimes M_i)$$

in which one checks that the isomorphism one gets in the end has the desired form. ∎

The rest of this section is dedicated to some non-fundamental results.

Theorem 2.6.9. (Tensoring with ground ring make it a direct sum of itself) Let $f : A \to B$ be a ring homomorphism, N be a B-module, and $N_B \triangleq B \otimes_A N$. Then we have an A-module isomorphism

$$N_B \cong N \oplus N$$

Proof. This is proved by split lemma and constructing a short exact sequence in $\mathbf{Mod}_A$ that splits:

$$0 \longrightarrow N \overset{g}{\hookrightarrow} N_B \overset{p}{\twoheadrightarrow} N \longrightarrow 0$$

In particular, one need to check that we have two A-module homomorphisms $g : N \to N_B$ and $p : N_N \to N$ well-defined by

$$g(x) \triangleq 1 \otimes x \quad \text{and} \quad p(b \otimes y) \triangleq by$$

Then because they clearly satisfy $p \circ g = \mathbf{id}_N$, the short sequence is exact and splits. ∎

Example 2.6.10: g in general isn't an B-module homomorphism

Let $A \triangleq \mathbb{R}$ and $B \triangleq N \triangleq \mathbb{C}$. Then $g \notin \mathbf{Mod}_B$, since

$$g(i1) = 1 \otimes_A i \neq i \otimes_A 1 = ig(1)$$

90

Let B and C be two A-algebras with canonical homomorphisms $f : A \to B$ and $g : A \to C$. Consider the A-module $B \otimes_A C$. From this A-module structure, we see that the A-modules diagram:

$$
\begin{array}{ccc}
 & B & \\
{\scriptstyle f}\nearrow & & \searrow {\scriptstyle b \mapsto b \otimes 1} \\
A & & B \otimes_A C \\
{\scriptstyle g}\searrow & & \nearrow {\scriptstyle c \mapsto 1 \otimes c} \\
 & C &
\end{array}
$$

commutes. Notably, we can define a multiplication on $B \otimes_A C$ to make it a ring:

$$(b \otimes c) \cdot (b' \otimes c') \triangleq bb' \otimes cc'$$

[1]and in fact, an A-algebra, whose A-module structure clearly can be regained via the morphisms in above diagram, which are now ring homomorphisms. The A-algebra $B \otimes_A C$ is called the **tensor product of A-algebra B and** C. The **tensor product of two rings** is then their tensor product as $\mathbb{Z}$-algebras.

Theorem 2.6.11. (Property of tensors over local rings) Let $(A, \mathfrak{m}, k)$ be a local ring, M and N be two finitely generated A-modules. If $M \otimes N = 0$, then $M = 0$ or $N = 0$.

Proof. The first step of the proof is a *routine verification using identities for tensor products* to show that:

$$(M \otimes_A k) \otimes_k (k \otimes_A N) = 0 \tag{2.10}$$

Clearly, there are two ways to give $(M \otimes_A k) \otimes_k (k \otimes_A N)$ an A-module structure, which are identical since:

$$x \otimes_k (ay) = \bar{a}(x \otimes_k y) = ax \otimes_k y$$

This settles an (A, k)-bimodule structure on $(M \otimes_A k) \otimes_k (k \otimes_A N)$. Consider the A-module structure from left. Then by associativity, we have an (A, k)-bimodule isomorphism:

$$(M \otimes_A k) \otimes_k (k \otimes_A N) \cong M \otimes_A X_1 \tag{2.11}$$

where $X_1 \triangleq k \otimes_k (k \otimes_A N)$ is an (A, k)-bimodule whose A-modules structure comes from the k on left. Again, by checking

$$\bar{b} \otimes_k (ax) = \bar{a} \cdot (\bar{b} \otimes_k x) = (a \cdot \bar{b}) \otimes_k x$$

---

[1]It requires some argument to show that this multiplication is well-defined. The fastest way is to first well-define an A-module homomorphism $B \otimes C \otimes B \otimes C \to B \otimes C$, $b \otimes c \otimes b' \otimes c' \mapsto bb' \otimes cc'$, and then use associativity of tensor product and definition to construct the A-bilinear mapping that is our multiplication.

We see that giving X_1 from left or right an A-module structure are identical. Therefore by associativity, we have an (A, k)-bimodule isomorphism:

$$X_1 \cong X_2$$

where $X_2 \triangleq (k \otimes_k k) \otimes_A N$ is an (A, k)-bimodule in which the A-module structure of $k \otimes_k k$ comes from right.[2] Now, since we have a k-module isomorphism $k \otimes_k k \cong k$, which is clearly also an A-module isomorphism, we have an (A, k)-bimodule isomorphism

$$X_2 \cong k \otimes_A N$$

Therefore, by equation 2.11, we have an (A, k)-bimodule isomorphism

$$(M \otimes_A k) \otimes_k (k \otimes_A N) \cong M \otimes_A (k \otimes_A N)$$

This gives us an A-module isomorphism:

$$(M \otimes_A k) \otimes_k (k \otimes_A N) \cong (M \otimes_A N) \otimes_A k \cong 0 \text{ (done)}$$

Now, since tensor product 2.10 is *over a field* with both sides finite dimensional, we know either $M \otimes_A k$ or $N \otimes_A k$ equals to 0. WLOG, let $M \otimes_A k = 0$. Then we have:

$$M / \mathfrak{m} M \cong M \otimes_A k = 0$$

This implies $M = \mathfrak{m} M$, which by Nakayama lemma implies $M = 0$, as desired.

∎

Theorem 2.6.12. (Interesting results that use tensor and generalized Cayley-Hamilton) Let A be a ring and $\phi : A^m \to A^n$ be a module homomorphism. If ϕ is injective, then $m \leq n$. Conversely, if ϕ is surjective, then $m \geq n$.

Proof. The statement about injectivity is proved via generalized Cayley-Hamilton theorem, and the statement about surjectivity is proved by a "tensoring residue field" argument.

Assume for a contradiction that ϕ is injective and $m > n$. Consider the injective morphism $(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n, 0, \ldots, 0)$ denoted by $i : A^n \hookrightarrow A^m$. Then $\psi \triangleq i \circ \phi \in \text{End}(A^m)$ is injective. Note that generalized Cayley-Hamilton theorem implies that

$$\psi^d + a_1 \psi^{d-1} + \cdots + a_d \mathbf{id}_{A^m} = 0$$

for some minimal $d \in \mathbb{N}$ and $a_i \in A$. Because $m > n$, the projection $(a_1, \ldots, a_m) \mapsto a_m$ denoted by $\pi : A^m \twoheadrightarrow A$ makes $\pi \circ \psi = 0$. Taking π on both side of the above equation then shows that $a_d = 0$, which gives us

$$\psi(\psi^{d-1} + a_1 \psi^{d-2} + \cdots + a_{d-1} \mathbf{id}_{A^m}) = 0$$

---

[2]Again, one can check that giving $k \otimes_k k$ an A-module structure from left or right are identical, but that's not necessary here.

The contradiction that ψ is not injective then follows from noting that minimality[3] of d implies that $\psi^{d-1} + a_1\psi^{d-2} + \cdots + a_{d-1}\mathbf{id}_{A^m}$ has nonzero image.

If ϕ is surjective, then $1 \otimes \phi : k \otimes A^m \twoheadrightarrow k \otimes A^n$ is also surjective by right exactness of tensor product, where $k \triangleq A/\mathfrak{m}$ is some residue field. The proof for $m \geq n$ then follows from noting that $k \otimes A^m$ as a k-vector space is m-dimensional[4] and that $1 \otimes \phi$ is k-linear.

■

---

[3]If $d = 1$, then at the step of $a_d = 0$, we already have a contradiction, i.e., $\psi = 0$.

[4]One way to see such is to use the A-module isomorphism $k \otimes A^m \cong A^m/\mathfrak{m}A^m$, in which one need to check that the natural k-vector space structure on $A^m/\mathfrak{m}A^m$ is m-dimensional and that the A-module isomorphism is indeed a k-vector space morphism.

2.7 Localization

2.8 Extended and Contracted Ideals

Unlike prime ideals, contraction of maximal ideals need not be maximal:

> **Example 2.8.1: Contraction of maximal ideals need not be maximal.**
>
> Consider $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Clearly (0) is maximal in $\mathbb{Q}$, but not maximal in $\mathbb{Z}$.

Let $f : A \to B$ be a ring homomorphism. Even though $f^{-1}(\mathfrak{b}) \lhd A$ is always an ideal, in general $f(\mathfrak{a}) \subseteq B$ need not be an ideal:

> **Example 2.8.2: Image of ideals need not be an ideal**
>
> Consider $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Clearly no nonzero ideal in $\mathbb{Z}$ is an ideal in $\mathbb{Q}$.

We then define **extension and contraction ideal** by

$$\mathfrak{a}^e \triangleq (f(\mathfrak{a})) \lhd B \quad \text{and} \quad \mathfrak{b}^c \triangleq f^{-1}(\mathfrak{b}) \lhd A$$

Theorem 2.8.3. (Basic properties of extension and contradiction) Let $f : A \to B$ be a ring homomorphism and $\mathfrak{a} \lhd A$, $\mathfrak{b} \lhd B$. Clearly, we have

$$\mathfrak{a} \leq \mathfrak{a}^{ec} \quad \text{and} \quad \mathfrak{b}^{ce} \leq \mathfrak{b}$$

Because of such, we have

$$\mathfrak{a}^e = \mathfrak{a}^{ece} \quad \text{and} \quad \mathfrak{b}^c = \mathfrak{b}^{cec}$$

Therefore, the set $C \triangleq \{\mathfrak{b}^c \lhd A : \mathfrak{b} \lhd B\}$ of **contracted ideals** in A and the set $E \triangleq \{\mathfrak{a}^c \lhd B : \mathfrak{a} \lhd A\}$ of **extended ideals** in B are

$$C = \{\mathfrak{a} \lhd A : \mathfrak{a}^{ec} = \mathfrak{a}\} \quad \text{and} \quad E = \{\mathfrak{b} \lhd A : \mathfrak{b}^{ce} = \mathfrak{b}\} \tag{2.12}$$

From description 2.12, we see that $\mathfrak{a} \mapsto \mathfrak{a}^e$ forms a bijection $C \longrightarrow E$ with inverse $\mathfrak{b} \mapsto \mathfrak{b}^c$. Moreover, since we always have:

$$\begin{aligned}
(\mathfrak{a}_1 + \mathfrak{a}_2)^e &= \mathfrak{a}_1^e + \mathfrak{a}_2^e, & (\mathfrak{b}_1 + \mathfrak{b}_2)^c &\geq \mathfrak{b}_1^c + \mathfrak{b}_2^c \\
(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e &\leq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e, & (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c &= \mathfrak{b}_1^c \cap \mathfrak{b}_2^c \\
(\mathfrak{a}_1 \mathfrak{a}_2)^e &= \mathfrak{a}_1^e \mathfrak{a}_2^e, & (\mathfrak{b}_1 \mathfrak{b}_2)^c &\geq \mathfrak{b}_1^c \mathfrak{b}_2^c \\
(\mathfrak{a}_1 : \mathfrak{a}_2)^e &\leq (\mathfrak{a}_1^e : \mathfrak{a}_2^e), & (\mathfrak{b}_1 : \mathfrak{b}_2)^c &\leq (\mathfrak{b}_1^c : \mathfrak{b}_2^c) \\
(\sqrt{\mathfrak{a}})^e &\leq \sqrt{\mathfrak{a}^e}, & (\sqrt{\mathfrak{b}})^c &= \sqrt{\mathfrak{b}^c}
\end{aligned}$$

We see that E is closed under taking sum and product, while C is closed under taking intersection, quotient, and radical.

Proof. Routine. ∎

It is worth mentioning that ideal extension have quite ill behavior. Even though contraction of prime ideals are prime, extension of prime ideal need not be prime:

Example 2.8.4: Extension of prime ideals need not be prime.

Consider $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Clearly, $(p)^e = \mathbb{Q}$ for all prime p.

2.9   Local Rings

Equivalent Definition 2.9.1. (Local rings) We say A is a **local ring** if any of the followings hold true:

(i) $\mathrm{Max}(A) = \{\mathfrak{m}\}$. We then call $A/\mathfrak{m}$ the **residue field** of A.

(ii) Non-units of A forms an ideal.

(iii) There exists a proper ideal containing all the non-units.

(iv) There exists some $\mathfrak{m} \in \mathrm{Max}(A)$ such that $1 + \mathfrak{m} \subseteq A^{\times}$.

Proof. (i) $\Longleftrightarrow$ (ii) $\Longleftrightarrow$ (iii) all follow from the fact that every non-unit is contained by some maximal ideal. (ii) $\Longrightarrow$ (iv) since if the non-units form an ideal $\mathfrak{m}$, then $1 + m$ can't be a non-unit, otherwise 1 would have been a non-unit.

We now prove (iv) $\Longrightarrow$ (iii). Let $x \in A - \mathfrak{m}$. We are required to show $x \in A^{\times}$. Because $x \notin \mathfrak{m}$, we know $(x) + \mathfrak{m} = (1)$, which implies $xy = 1 - m \in A^{\times}$ for some $y \in A$ and $m \in \mathfrak{m}$, as desired. ∎

Theorem 2.9.2. (Local ring contains no non-trivial idempotents) Local ring $(A, \mathfrak{m})$ must contains no **idempotent** $\neq 0, 1$.

Proof. Assume for a contradiction that $x \in A - \{0, 1\}$ is an idempotent. Clearly the only idempotent unit is 1. Therefore x is a non-unit. Since $1 - x$ is also an idempotent:

$$(1 - x)^2 = 1 - 2x + x^2 = 1 - x$$

again we know it must be a non-unit, otherwise $x = 0$. Because A is local, we now see $1 = (1 - x) + x \in \mathfrak{m}$ lies in the ideal of non-unit, a contradiction. ∎

Equivalent Definition 2.9.3. (Local ring with $\mathfrak{m} \triangleq \mathrm{Nil}(A)$) If any of the followings hold true:

(i) A has exactly one prime ideal.

(ii) All non-units of A are nilpotent.

(iii) $A/\mathrm{Nil}(A)$ is a field.

then A is a local ring with $\mathfrak{m} = \mathrm{Nil}(A)$. Such ring satisfies $\mathrm{Nil}(A) = \mathrm{Jac}(A)$.

Proof. (i) $\Longrightarrow$ (ii): Because A has exactly one prime ideal, we know $\mathrm{Nil}(A) = \bigcap \mathrm{Spec}(A)$ is prime. Assume for a contradiction that there exists a non-unit $x \notin \mathrm{Nil}(A)$, then since x is contained by some maximal ideal and maximal ideals are prime, we see $\mathrm{Nil}(A)$ isn't the

unique prime ideal, a contradiction.

(ii) $\implies$ (iii): Because non-units forms the nilradical, we know A is local with $\mathfrak{m} = \operatorname{Nil}(A)$.

(iii) $\implies$ (i): The premise implies $\operatorname{Nil}(A)$ is maximal. Therefore, $\operatorname{Nil}(A) = \bigcap \operatorname{Spec}(A)$ implies $\operatorname{Nil}(A)$ is the unique prime of A. ∎

2.10   GCD Domain and Gauss Lemma

Abstract

This section gives a proof of Gauss lemma in the setting of GCD domains. In this section, if we say $f \in D[x_1, \ldots, x_n]$ is irreducible, we mean that it is irreducible as an element of the integral domain $D[x_1, \ldots, x_n]$.

Let D be an integral domain and $x, y \in D$. We say x **divides** y if there exists some $q \in D$ such that $y = xq$. In this section, given $x \mid y$, we write $\frac{y}{x} \in D$ to denote the element that makes

$$x \cdot \frac{y}{x} \triangleq y$$

even if x is a non-unit. A *nonzero non-unit* element $d \in D$ is said to be **irreducible** if

$$d = xy \implies x \text{ or } y \in D^\times$$

A *nonzero non-unit* element $p \in D$ is said to be **prime** if

$$p \mid xy \implies p \mid x \text{ or } p \mid y$$

Given a collection of elements $\{x_i\}$ in D, we say $d \in D$ is a **greatest common divisor** if d is a common divisor divisible by all common divisors of $\{x_i\}$, and we say $l \in D$ is a **least common multiple** if l is a common multiple of $\{x_i\}$ dividing all common multiples of $\{x_i\}$. Two elements $a, b \in D$ are said to be **associated** if $a = bu$ for some $u \in D^\times$. Clearly, the notion of greatest common divisor, least common multiple, primality, and irreducibility are all defined up to the equivalence relation of associations.

Theorem 2.10.1. (Prime elements are irreducible) Let D be an integral domain and $p \in D$ be a prime element. Then p is irreducible.

Proof. Let $p \triangleq xy$. By primality, p divides one of them. If p divides x, then y is a unit with inverse $\frac{x}{p}$. ∎

Theorem 2.10.2. (Basic properties of greatest common divisors) Let D be an integral domain and $x, y \in D$ be nonzero. Then

(i) GCD is *associative and homogeneous*, that is, for all nonzero $z \in D$, we have

$$\mathrm{GCD}(x, y, z) = \mathrm{GCD}(\mathrm{GCD}(x, y), z)$$

and

$$\mathrm{GCD}(zx, zy) \in D \implies \mathrm{GCD}(x, y) = \frac{\mathrm{GCD}(zx, zy)}{z} \in D$$

99

(ii) We have

$$\text{LCM}(x, y) \text{ exists} \iff \text{GCD}(cx, cy) \text{ exists for all nonzero } c \in D$$

In particular, if $\text{LCM}(x, y)$ exists, then we have

$$\text{GCD}(x, y) = \frac{xy}{\text{LCM}(x, y)}$$

Proof. (i) is routine. We prove (ii). ($\implies$): We first show that

$$\text{GCD}(x, y) \text{ exists}$$

Clearly, $d \triangleq \frac{xy}{\text{LCM}(x,y)} \in D$ exists. Our goal is to prove $d = \text{GCD}(x, y)$. Let d_0 be a common divisor of x and y. Because $d_0 \mid x$, we know $x \cdot \frac{y}{d_0}$ is a common multiple of x and y, so we have

$$\text{LCM}(x, y)d_0 \mid x \cdot \frac{y}{d_0} \cdot d_0 = xy = \text{LCM}(x, y)d, \quad \text{(done)}$$

It remains to show

$$\text{LCM}(cx, cy) \text{ exists and equal } c\,\text{LCM}(x, y)$$

Clearly $c\,\text{LCM}(x, y)$ is a common multiple of cx and cy. Let m be a common multiple of cx and cy. Then $\frac{m}{c} \in D$ exists. Cancellation then shows $\frac{m}{c}$ is a common multiple of x and y, so $\text{LCM}(x, y) \mid \frac{m}{c}$. This implies

$$c\,\text{LCM}(x, y) \mid c \cdot \frac{m}{c} = m, \quad \text{(done)}$$

($\impliedby$): Let m be a common multiple of a and b. Clearly, ab is a common divisor of ma and mb. Therefore by homogeneous property of greatest common divisor, we have:

$$ab \mid \text{GCD}(ma, ma) = m\,\text{GCD}(a, b)$$

which by cancellation implies $\frac{ab}{\text{GCD}(a,b)} \mid m$, as desired. ∎

Equivalent Definition 2.10.3. (GCD domain) We say an integral domain D is a **GCD domain** if any of the followings hold true:

(i) Every pair of elements of D admits a greatest common divisor.

(ii) Every pair of elements of D admits a least common multiple.

Proof. This follows from the relationship between GCD and LCM. ∎

Theorem 2.10.4. (Basic properties of GCD domains) Let D be a GCD domain. Then

(i) D is integrally closed.

(ii) Every irreducible element of D is prime.

(iii) Let $x, y, z \in D$ be nonzero. If $\text{GCD}(x, y) = 1$ and $x \mid yz$, then $x \mid z$. **(Euclid Lemma)**

(iv) Let $x, y, z \in D$ be nonzero. Then $\text{GCD}(x, y) = \text{GCD}(x, z) = 1 \implies \text{GCD}(x, yz) = 1$.

Proof. (iii): Since $\text{GCD}(x, y) = 1$, we have $\text{LCM}(x, y) = xy$. The proof then follows from noting that since yz is a common multiple of x and y, we have

$$xy = \text{LCM}(x, y) \mid yz$$

(iv): Let g be a common divisor of x and yz. Because common divisors of g and y must also be common divisors of x and y, from $\text{GCD}(x, y) = 1$, we know $\text{GCD}(g, y) = 1$. Therefore, by Euclid lemma, g is a divisor of z, thus a common divisor of x and z, which by $\text{GCD}(x, z) = 1$ implies $g = 1$. ∎

Theorem 2.10.5. (Polynomial rings are integral domain if and only if ground rings are integral domain) Let A be a ring. Then

$$A[x] \text{ is an integral domain} \iff A \text{ is an integral domain}$$

Proof. Left to right follows from noting that A is a subring of $A[x]$. Right to left follows from noting that the leading term of the product is the product of leading terms. ∎

Let A be a ring and $f \in A[x_1, \ldots, x_n]$. The **content of** f is the ideal of A generated by the coefficients of f, and we say f is **primitive** if $\text{cont}(f) = (1)$. Clearly, we may give a well-ordering on the set of monomials of $A[x_1, \ldots, x_n]$ by first comparing their powers on x_1, and if tie, then comparing their powers on x_2 and so on. Such ordering is called the **lexicographical monomials ordering**. Clearly, lexicographical monomials ordering satisfies

$$m_1 > m_2 \implies m_1 m_3 > m_2 m_3$$

Theorem 2.10.6. (Divisors of monomials over integral domains must be either constants or monomials) Let D be an integral domain and $m \in D[x_1, \ldots, x_n]$ a monomial. The divisors of m are either constants or monomials.

Proof. Consider lexicographical monomials ordering. ∎

Theorem 2.10.7. (Gauss lemma: primitive statement) Let A be a ring and $f, g \in A[x_1, \ldots, x_n]$. Then

$$\operatorname{cont}(fg) \le \operatorname{cont}(f) \operatorname{cont}(g) \le \sqrt{\operatorname{cont}(fg)}$$

In particular, since $\sqrt{\mathfrak{a}} = (1) \implies \mathfrak{a} = (1)$, we see that

$$f, g \text{ are both primitive} \iff fg \text{ is primitive}$$

Proof. The first inequality is clear. Let $\mathfrak{p} \ge \operatorname{cont}(fg) \trianglelefteq A$. The second inequality requires us to prove that $\mathfrak{p} \ge \operatorname{cont}(f) \operatorname{cont}(g)$. Because $\operatorname{cont}(fg) \le \mathfrak{p}$, we know fg is 0 in $(A/\mathfrak{p})[x_1, \ldots, x_n]$. Then because $(A/\mathfrak{p})[x_1, \ldots, x_n]$ is an integral domain, we know either f or g is 0 in $(A/\mathfrak{p})[x_1, \ldots, x_n]$. The proof then follows from noting that if f is 0 in $(A/\mathfrak{p})[x_1, \ldots, x_n]$, then $\operatorname{cont}(f) \le \mathfrak{p}$. ∎

Theorem 2.10.8. (Gauss lemma: irreducibility statement, part 1) Let D be a GCD domain and $f, g \in D[x_1, \ldots, x_n]$. Then

$$c(fg) = c(f)c(g)$$

where $c(f) \triangleq$ the greatest common divisor of nonzero coefficients of f.

Proof. The first step of the proof is noting that since GCD is homogeneous, we may reduce the proof to the case $c(f) = c(g) = 1$. The rest of the proof relies on induction on number n of terms in fg. The base case $n = 1$ follows from noting that divisors of monomials over integral domains must be either constants or monomials.

We now prove the inductive case. Let f_0 and g_0 be the highest degree term of f and g with respect to lexicographical ordering. Clearly, $f_0 g_0$ is also the highest degree term of fg. Therefore, $c(fg)$ divides $c(f_0 g_0)$. Because of such, we only have to prove

$$\gcd(c(fg), c(f_0 g_0)) = 1$$

In particular, we only have to prove:

$$\gcd\left(c(fg), c(f_0)\right) = \gcd\left(c(fg), c(g_0)\right) = 1$$

Assume $\gcd\left(c(fg), c(f_0)\right) = d \notin D^\times$ for a contradiction. Clearly, we have

$$d \mid c(fg - f_0 g) = c\left(g(f - f_0)\right) = c(g)c(f - f_0) = c(f - f_0)$$

where the second last equality follows from inductive hypothesis. Because $d \mid c(f_0)$, this implies $d \mid c(f) = 1$, a contradiction. ∎

Theorem 2.10.9. (Gauss lemma: irreducibility statement, part 2) Let D be a GCD domain, $K \triangleq \text{Frac}(D)$ its field of quotient, and $f \in D[x]$ be non-constant. Then

$$f \in D[x] \text{ is irreducible} \iff c(f) = 1 \text{ and } f \in K[x] \text{ is irreducible}$$

Proof. ($\impliedby$) is routine. We only prove ($\implies$). $c(f) = 1$ is clear. Assume for a contradiction that $f \triangleq gh \in K[x]$ where $g, h \in K[x]$ are non-units and thus non-constants. Clearly, there exists $d, \tilde{d} \in D$ such that $dg, \tilde{d}h \in D[x]$. We then have

$$f = gh = \frac{b}{a} \cdot g'h', \quad \text{with } g', h' \in D[x] \text{ non-constant and primitive}$$

where $b \triangleq c(dg)c(\tilde{d}h) \in D$ and $a \triangleq d\tilde{d} \in D$. Because $g', h' \in D[x]$ are non-constant, to cause a contradiction to irreducibility of $f \in D[x]$, we only have to show $a \mid b$. Because g', h' are primitive, this follows from part 1 of irreducibility statement of Gauss lemma and taking content on both side of $af = bg'h'$. ∎

Theorem 2.10.10. (Eisenstein's criteria) Let D be an integral domain and

$$f \triangleq a_n x^n + \cdots + a_0 \in D[x]$$

If there exists a prime ideal $\mathfrak{p} \trianglelefteq D$ such that

(i) $a_i \in \mathfrak{p}$ for all $i < n$.

(ii) $a_n \notin \mathfrak{p}$.

(iii) $a_0 \notin \mathfrak{p}^2$.

then f can't be written as a product of two non-constant polynomials $\in D[x]$.

Proof. Assume for a contradiction that $f = gh \in D[x]$ with $g, h \in D[x]$ non-constant. Because the leading coefficient of f is not in $\mathfrak{p}$, we know the leading coefficients of both g and h are not in $\mathfrak{p}$. Therefore, we know $g, h \in (D/\mathfrak{p})[x]$ are non-constants.

Now, since $f \in (D/\mathfrak{p})[x]$ is a monomial and divisors of monomials over integral domains must be either constants or monomials, we see both $g, h \in (D/\mathfrak{p})[x]$ are non-constant monomial, which implies that their constant terms are both in $\mathfrak{p}$, causing a contradiction to $a_0 \notin \mathfrak{p}^2$. ∎

Theorem 2.10.11. (Consequences of Eisenstein's criteria) Let D be an integral domain and $f \in D[x]$ be a non-constant polynomial that can't be written as a product of two non-constant polynomials. Then

(i) If f is primitive, then $f \in D[x]$ is irreducible.

(ii) If D is a GCD domain with $K \triangleq \text{Frac}(D)$, then $f \in K[x]$ is irreducible.

Proof. (i) is clear. By Gauss lemma and (i), $f/c(f)$ is irreducible in $K[x]$, and therefore f is irreducible in $K[x]$. ∎

2.11   UFD PID ED

Equivalent Definition 2.11.1. (UFD) An integral domain D is an **unique factorization domain** if any of the followings hold true:

(i) Every *nonzero non-unit* element of D can be written as finite product of irreducible elements, unique up to permutation and association.

(ii) Every *nonzero non-unit* element of D can be written as finite product of irreducible elements, and every irreducible element of D is prime.

(iii) Every nonzero $\mathfrak{p} \neq 0 \in \mathrm{Spec}(D)$ contains a prime element.

Proof. (i) $\implies$ (ii): Let $a \in D$ be irreducible and $a \mid xy$. To prove a is prime, we are required to prove a divides one of x, y. Write

$$a\pi_1 \cdots \pi_n = (p_1 \cdots p_m)(q_1 \cdots q_k) = xy, \quad \text{where } p_i, \pi_i, q_i \text{ are irreducible}$$

The proof then follows from noting that by premise, a must lies one of p_i, q_i, up to association.

(ii) $\implies$ (i): Consider two factorizations of same element:

$$p_1 \cdots p_n = q_1 \cdots q_m, \quad \text{where } p_i, q_i \text{ are irreducible}$$

WLOG, we only need to prove that, up to association, $p_1 \in \{q_1, \ldots, q_m\}$. Primality of p_1 implies that $p_1 \mid q_i$ for some i. Write $q_i = p_1 s$. Because p_1 is non-unit, irreducibility of q_i implies $s \in D^\times$, as desired.

(ii) $\implies$ (iii): Because $\mathfrak{p}$ is prime and nonzero, existence of factorization implies that $\mathfrak{p}$ contains an irreducible element, which is prime by premise.

(iii) $\implies$ (ii): We first prove a lemma:

> Let $S \subseteq A$ be a be multiplicatively closed subset with $0 \notin S$. If $\mathfrak{a} \trianglelefteq A$ is disjoint with S, then
> $$\Sigma \triangleq \{\mathfrak{b} \trianglelefteq A : \mathfrak{a} \leq \mathfrak{b} \text{ and } \mathfrak{b} \cap S = \varnothing\}$$
> has maximal elements, which are all prime.

The fact that Σ has maximal elements is a consequence of Zorn's lemma. Let $\mathfrak{b}$ be a maximal element of Σ. Assume for a contradiction that $\mathfrak{b}$ is not prime. Then there exists $xy \in \mathfrak{b}$ such that $x, y \notin \mathfrak{b}$. Maximality of $\mathfrak{b}$ then implies that both $\mathfrak{b} + (x)$ and $\mathfrak{b} + (y)$ intersect with S. Let $s_1 \in (\mathfrak{b} + (x)) \cap S$ and $s_2 \in (\mathfrak{b} + (y)) \cap S$. Because $xy \in \mathfrak{b}$, direct computation

then shows $s_1 s_2 \in \mathfrak{b} \cap S$, a contradiction. (done)

Let

$$S \triangleq \{p_1 \cdots p_n \in D : n \geq 0 \text{ and } p_i \text{ are prime}\}$$

where $n = 0$ means unit, so $D^\times \subseteq S$. Because prime elements are irreducible, to prove the existence of factorization, we only have to prove that S contains all nonzero element of D. Before such, we first prove that

$$S \text{ is divisor-closed. That is, if } s \in S \text{ and } d \mid s, \text{ then } d \in S.$$

Let $s \triangleq p_1 \cdots p_n$. This is proved via induction on n. Let $s \triangleq dq$. The base case is $n = 0$, where $s \in D^\times$. In such case, we have $dqs^{-1} = 1$, so $d \in D^\times \subseteq S$. We now prove the inductive case. Because we clearly have $p_1 \mid dq$, primality of p_1 split the proof into two cases:

$$p_1 \mid d \quad \text{or} \quad p_1 \mid q$$

Case ($p_1 \mid d$): Let $d \triangleq p_1 q'$. Our goal is to prove $q' \in S$. Because D is an integral domain, we have

$$p_1 \cdots p_n = dq = p_1 q' q \implies d' \mid p_2 \cdots p_n$$

which by inductive hypothesis implies $q' \in S$.

Case ($p_1 \mid q$): Let $q \triangleq p_1 q''$. Again, because D is an integral domain, we have

$$p_1 \cdots p_n = dq = dp_1 p'' \implies d \mid p_2 \cdots p_n$$

The proof then follows from inductive hypothesis. (done)

We may now prove easily that S contains all nonzero elements of D. Assume for a contradiction that $a \neq 0 \in D - S$. Because S is divisor-closed, this implies $(a) \cap S = \varnothing$. Therefore by our earlier lemma, there exists some prime ideal $\mathfrak{p} \geq (a)$ such that $\mathfrak{p} \cap S = \varnothing$. This is impossible, since by premise, there exists some prime $p \in \mathfrak{p}$.

Let $\pi \in D$ be irreducible. The fact that π is prime then follows from factorizing $\pi = p_1 \cdots p_n$ into prime elements and observing that by irreducibility of π, we must have $n = 1$. ∎

Theorem 2.11.2. (Polynomial ring over UFD is UFD) If D is a UFD, then $D[x]$ is a UFD.

Proof. We first prove the existence of factorization. Let $f \in D[x]$. Because D is a UFD and irreducibles in D remain irreducible in $D[x]$, to factorize f, we only have to factorize $\frac{f}{c(f)}$. In other words, we may suppose f is primitive.

Clearly, $f \in D[x]$ can be written as a finite product of non-constant polynomials $\in D[x]$ that can't be written as products of two non-constant polynomial. By Gauss lemma, these polynomials must be primitive, and therefore irreducibles.

We now prove that every irreducible $f \in D[x]$ must be prime. Clearly, f must be primitive.

Let $g, h \in D[x]$ and gh be divisible by f in $D[x]$. Let $K \triangleq \mathrm{Frac}(D)$. Because $K[x]$ is an Euclidean domain, we know $f \in K[x]$ is prime. Therefore, f divides either g or h in $K[x]$. Suppose $fq = g$ with $q \in K[x]$. Write $q \triangleq \frac{Q}{d}$ with $Q \in D[x], d \in D$. Then

$$fQ = dg$$

Taking contents on both side, again by Gauss lemma, we see

$$c(Q) = dc(g)$$

Therefore, $d \mid c(Q)$, and $q \in D[x]$. ∎

Example 2.11.3: $\mathbb{Z}[\sqrt{5}i]$ isn't UFD.

Because $\mathbb{Z}[\sqrt{5}i]$ is a subring of $\mathbb{C}$, we know it is an integral domain. If $\mathbb{Z}[\sqrt{5}i]$ is an UFD, then all irreducibles are prime. We prove this isn't the case by showing $2 \in \mathbb{Z}[\sqrt{5}i]$ is irreducible but not prime. To see $2 \in \mathbb{Z}[\sqrt{5}i]$ is prime, just observe

$$2 \mid 6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$$

and that 2 clearly doesn't divide neither $1+\sqrt{5}i$ nor $1-\sqrt{5}i$. The proof that $2 \in \mathbb{Z}[\sqrt{5}i]$ is irreducible is more tricky: Let

$$2 \triangleq (a + b\sqrt{5}i)(c + d\sqrt{5}i)$$

Then we have

$$\begin{cases} ac - 5bd = 2 \\ bc + ad = 0 \end{cases} \implies \begin{cases} acd - 5bd^2 = 2d \\ ad = -bc \end{cases} \implies 2d = -b(c^2 + 5d^2)$$

Then by comparing order of absolutes values of each side, we see that we must have $d = 0$. This then implies $b = 0$ and therefore $ac = 2$, as desired.

An integral domain is said to be **PID** if in which all ideals are principal.

Theorem 2.11.4. () $A[x]$ is a PID if and only if A is a field.

Proof. Clearly, we have an ring isomorphism

$$A[x]/(x) \cong A, \quad f \mapsto f(0)$$

∎

Example 2.11.5: $A[x, y]$ is not a PID

Consider (x, y).

Theorem 2.11.6. (Basic properties of principal ideal in integral domain) Let D be an integral domain and $\mathfrak{a} \trianglelefteq D$ an nonzero principal ideal. Clearly, the possible generators of $\mathfrak{a}$ forms an associative class, moreover

(i) $\mathfrak{a} \in \mathrm{Spec}(D) \iff$ the generator class is prime.

(ii) $\mathfrak{a}$ is maximal among proper principal ideals $\iff$ the generator class is irreducible.

In particular, because of (i), we know PID are UFD, and because prime elements are irreducible, from (ii) we see that if D is a PID, then $\mathrm{Spec}(D) = \mathrm{Max}(D)$.

Proof. Let $\mathfrak{a} \triangleq (a)$. We prove (ii). ($\Longrightarrow$): Let $a \triangleq xy$. If x and y are both non-units, then $(a) = (xy) < (y) < D$.

($\Longleftarrow$): Let $(b) \geq (a)$ be a proper ideal, so $a = bq$ for some $q \in D$. Because (b) is a proper ideal, we know the unit is q, so $a \sim q$ and $(b) = (a)$. ∎

We say a divisor $x \in A$ of $a, b \in A$ is a **greatest common divisor** if x is divided by all common divisors of a, b.

Example 2.11.7

Consider $6, 2(1+\sqrt{5}i) \in \mathbb{Z}[\sqrt{-5}]$. 6 has divisors $1, 2, 3, 1 \pm \sqrt{5}i$, so they have common divisors $2, 1 + \sqrt{5}i$, but no greatest common divisor.

Theorem 2.11.8. (Properties of $\mathbb{Z}[\sqrt{-d}]$ for square-free $d \geq 3$) Let $d \geq 3$ be square free. If $d + 1$ is not prime, but divisible by prime p, then

(i) $p \in \mathbb{Z}[\sqrt{-d}]$ is irreducible but isn't prime.

(ii) $\gcd(p, 1 + \sqrt{-d}) = 1$, but $\mathrm{lcm}(p, 1 + \sqrt{-d})$ doesn't exist.

107

If $d+1$ is prime, then

(i) $2 \in \mathbb{Z}[\sqrt{-d}]$ is irreducible but isn't prime.

(ii) $\gcd(2, 2+\sqrt{-d}) = 1$, but $\operatorname{lcm}(2, 2+\sqrt{-d})$ doesn't exist.

Proof. See this note. ∎

Let D be an integral domain. We say D is an **Euclidean domain** if there exists some function $f : D - \{0\} \to \mathbb{Z}_0^+$ that satisfies **division-algorithm property**: For all $a \in D$ and nonzero $b \in D$, there exists some $q, r \in D$ such that $a = qb + r$ and either $r = 0$ or $f(r) < f(q)$. If f moreover satisfies

$$f(a) \le f(ax) \text{ for all nonzero } a, x \in D$$

then we say f is a **Euclidean norm**.

Theorem 2.11.9. (Every Euclidean domain admits an Euclidean norm) If D is a Euclidean domain with $g : D - \{0\} \to \mathbb{Z}_0^+$ satisfying the division-algorithm property, then $f : D - \{0\} \to \mathbb{Z}_0^+$ defined by

$$f(a) \triangleq \min_{x \in D - \{0\}} g(ax)$$

is an Euclidean norm.

Proof. Let $a, b \in D$ with b nonzero satisfying $b \nmid a$. Let $f(b) \triangleq g(bc)$. Applying g-division algorithm on ac and bc, we get

$$ac = q \cdot bc + rc, \quad \text{where } r \triangleq a - qb \ne 0$$

which satisfies

$$f(r) \le g(rc) < g(bc) = f(b)$$

∎

Clearly, Euclidean domains are PID, since every ideal in Euclidean domain can be generated by any of its element of smallest norm.

$\mathbb{Z}$ is a Euclidean domain with Euclidean function $f(x) \triangleq |x|$. Gaussian integers ring $\mathbb{Z}[i]$ is a Euclidean domain with Euclidean function $f(a+bi) \triangleq a^2 + b^2$. For each field K, $K[x]$ has Euclidean function deg. K itself is also Euclidean domain with Euclidean function $x \mapsto 1$.

Example 2.11.10: $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ is a PID that isn't Euclidean

Chapter 3

Algebraic Geometry

3.1 Spectrum

Equivalent Definition 3.1.1. (Zariski topology on spectrum) Let A be a ring. For all $E \subseteq A$ and $f \in A$, we define

$$V(E) \triangleq \{\mathfrak{p} \in \operatorname{Spec}(A) : E \subseteq \mathfrak{p}\} \quad \text{and} \quad U_f \triangleq \{\mathfrak{p} \in \operatorname{Spec}(A) : f \in \mathfrak{p}\}$$

Since

(i) $\operatorname{Spec}(A) = V(0)$ and $\varnothing = V(1)$.

(ii) $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$.

(iii) $\bigcap_{i \in I} V(\mathfrak{a}_i) = V(\bigcup \mathfrak{a}_i) = V(\sum \mathfrak{a}_i)$ for possibly infinite I.

We see that the **Zariski topology** on $\operatorname{Spec}(A)$ is well-defined. Because

$$V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}}), \quad \text{where } \mathfrak{a} \triangleq (E)$$

Topology of $\operatorname{Spec}(A)$ is determined by ideals $\trianglelefteq A$. Moreover, we have

$$\mathfrak{a} \leq \operatorname{Nil}(A) \iff V(\mathfrak{a}) = \operatorname{Spec}(A), \quad \text{for all } \mathfrak{a} \trianglelefteq A$$

Proof. Clearly, we have

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$$

The inequality $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$ follows from $\mathfrak{a} \cap \mathfrak{b} \leq \mathfrak{p}$ implies one of them is contained by $\mathfrak{p}$. ∎

Theorem 3.1.2. (Property of basic open sets) Because

$$\operatorname{Spec}(A) - V(\mathfrak{a}) = \bigcup_{f \in \mathfrak{a}} U_f$$

we know $\{U_f \subseteq \mathrm{Spec}(A) : f \in A\}$ form a basis for $\mathrm{Spec}(A)$, thus the name **basic open sets**. Basic open sets have the properties:

(i) $U_f = \varnothing \iff f \in \mathrm{Nil}(A)$.

(ii) $U_f = \mathrm{Spec}(A) \iff f \in A^\times$.

(iii) $U_{fg} = U_f \cap U_g$ for all $f, g \in A$.

Proof. The first property of basic open sets follows from $\mathrm{Nil}(A) = \bigcap \mathrm{Spec}(A)$. The second property of basic open sets follows from the fact every non-unit must be contained by some maximal ideal. The third property of basic open sets follows from definition of prime ideals. $\blacksquare$

Theorem 3.1.3. (Topological property of $\mathrm{Spec}(A)$**)** Let $Y \subseteq \mathrm{Spec}(A)$. Then clearly we have:

$$\overline{Y} = \bigcap_{Y \subseteq V(\mathfrak{a})} V(\mathfrak{a}) = \bigcap_{\mathfrak{a} \leq \bigcap Y} V(\mathfrak{a}) = V\left(\sum_{\mathfrak{a} \leq \bigcap Y} \mathfrak{a}\right) = V\left(\bigcap Y\right)$$

In particular,

$$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}), \qquad \text{for all } \mathfrak{p} \trianglelefteq A$$

Because of such, we know:

$$\mathfrak{q} \in \overline{\{\mathfrak{p}\}} \iff \mathfrak{p} \leq \mathfrak{q} \tag{3.1}$$

for all $\mathfrak{q} \in \mathrm{Spec}(A)$. In general, given a topological space X, we say $x \in X$ is a **closed point** if $\{x\}$ is closed, we say X is a T_0**-space** if for any pair $x \neq y \in X$, there exists an open set containing exactly of them, and we say X is **irreducible** if X can not be written as union of two proper closed subset of X. Then,

(i) $\mathfrak{p} \in \mathrm{Spec}(A)$ is a closed point $\iff \mathfrak{p} \in \mathrm{Max}(A)$.

(ii) $\mathrm{Spec}(A)$ is T_0.

(iii) $\mathrm{Spec}(A)$ is irreducible $\iff \mathrm{Nil}(A) \trianglelefteq A$ is prime.

(iv) The irreducible closed subspaces of $\mathrm{Spec}(A)$ is exactly $\{V(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Spec}(A)\}$. Therefore, since $V(\mathfrak{a}) \subseteq V(\mathfrak{b}) \iff \sqrt{\mathfrak{a}} \geq \sqrt{\mathfrak{b}}$, the irreducible components of $\mathrm{Spec}(A)$ is exactly $\{V(\mathfrak{p}) : \mathfrak{p} \text{ is a minimal prime ideal over } 0\}$.

Proof. (i) follows from statement 3.1. For (ii), just observe that if $\mathfrak{p} \not\leq \mathfrak{q}$, then $\mathrm{Spec}(A) - V(\mathfrak{p})$ is an open set containing $\mathfrak{q}$ but not $\mathfrak{p}$. We now prove (iii). Because $V(\mathfrak{a}) \cup V(\mathfrak{b}) =$

$V(\mathfrak{a} \cap \mathfrak{b})$ and because $V(\mathfrak{a}) = \mathrm{Spec}(A) \iff \mathfrak{a} \leq \mathrm{Nil}(A)$, we know $\mathrm{Spec}(A)$ is irreducible if and only if:

$$\mathfrak{a} \cap \mathfrak{b} \leq \mathrm{Nil}(A) \implies \mathfrak{a} \text{ or } \mathfrak{b} \leq \mathrm{Nil}(A), \quad \text{for all } \mathfrak{a}, \mathfrak{b} \trianglelefteq A \tag{3.2}$$

This is apparently true if $\mathrm{Nil}(A) \trianglelefteq A$ is prime. Conversely, if statement 3.2 holds, then since $\mathfrak{a}\mathfrak{b} \leq \mathfrak{a} \cap \mathfrak{b}$, by considering principal ideals, we see $\mathrm{Nil}(A)$ is prime.

(iv): Because we have homeomorphisms $V(\mathfrak{a}) \cong \mathrm{Spec}(A/\mathfrak{a})$, by (iii), we know $V(\mathfrak{a})$ is irreducible if and only if $\mathrm{Nil}(A/\mathfrak{a})$ is prime. By correspondence theorem for rings, we know $\mathrm{Nil}(A/\mathfrak{a})$ is prime if and only if $\sqrt{\mathfrak{a}} \trianglelefteq A$ is prime. Therefore, the set of irreducible closed subspaces of $\mathrm{Spec}(A)$ is

$$\{V(\mathfrak{a}) : \mathfrak{a} \trianglelefteq A \text{ and } \sqrt{\mathfrak{a}} \in \mathrm{Spec}(A)\} = \{V(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Spec}(A)\}$$

∎

Theorem 3.1.4. (Basic properties of pullback) Let $\phi : A \to B$ be a ring homomorphism, because preimage of prime ideals are prime, the **pullback** $\phi^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ defined by $\phi^*(\mathfrak{b}) \triangleq \mathfrak{b}^c$ is well-defined. Denote $X \triangleq \mathrm{Spec}(A)$ and $Y \triangleq \mathrm{Spec}(B)$. Then

(i) Because $(\phi^*)^{-1}(X_f) = Y_{\phi(f)}$, we see $\phi^* : Y \to X$ is continuous.

(ii) $(\phi^*)^{-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$.

(iii) $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$.

(iv) If ϕ is surjective, then ϕ^* is a homeomorphism of Y onto $V(\ker(\phi))$. In particular, for all $\mathfrak{a} \trianglelefteq A$, we have a homeomorphism

$$V(\mathfrak{a}) \cong \mathrm{Spec}(A/\mathfrak{a})$$

(v) $\phi^*(Y)$ is dense in $X \iff \ker(\phi) \leq \mathrm{Nil}(A)$.

Proof. (i) and (ii) are clear. For (iii), use the fact that contraction comutes with taking intersection and radical to compute:

$$\overline{\phi^*(V(\mathfrak{b}))} = V\left(\bigcap \phi^*(V(\mathfrak{b}))\right)$$

$$= V\left(\bigcap_{\mathfrak{b} \leq \mathfrak{q}} \mathfrak{q}^c\right) = V\left(\left(\bigcap_{\mathfrak{b} \leq \mathfrak{q}} \mathfrak{q}\right)^c\right) = V\left((\sqrt{\mathfrak{b}})^c\right) = V(\sqrt{\mathfrak{b}^c}) = V(\mathfrak{b}^c)$$

(iv): The fact that $\phi^* : Y \to V(\ker(\phi))$ is bijective follows from correspondence theorem for rings, and the fact that ϕ^* is a closed map follows from using correspondence theorem for rings to compute:

$$\phi^*(V(\mathfrak{b})) = V\left(\phi^{-1}(\mathfrak{b})\right), \quad \text{for all } \mathfrak{b} \trianglelefteq B$$

111

(v): Because $\mathrm{Nil}(A) = \bigcap \mathrm{Spec}(A)$, the proof follows from using (iii) to compute:

$$\overline{\phi^*(Y)} = \overline{\phi^*(V(0))} = V(0^c) = V(\ker(\phi))$$

∎

Theorem 3.1.5. (Connectedness of spectrums) Let $A \triangleq A_1 \times \cdots \times A_n$. Then we have a homeomorphism:

$$\mathrm{Spec}(A) \cong \coprod_{i=1}^n \mathrm{Spec}(A_i) \tag{3.3}$$

Moreover, for any ring B, the followings are equivalent:

(i) $\mathrm{Spec}(B)$ is disconnected.

(ii) $B \cong B_1 \times B_2$ where neither B_1 nor B_2 is the zero ring.

(iii) B contains no idempotent $\neq 0, 1$.

In particular, by (iii), the spectrum of a local ring is always connected.

Proof. Denote $\mathfrak{a}_i \triangleq \ker(\pi_i)$, where $\pi_i : A \twoheadrightarrow A_i$ are the canonical projection. Because we have homeomorphisms $\pi_i^* : \mathrm{Spec}(A_i) \longrightarrow V(\mathfrak{a}_i)$, proof of statement 3.3 boils down to showing that $\mathrm{Spec}(A)$ is the disjoint union of $V(\mathfrak{a}_i)$. This is then clear from the forms of $\mathfrak{a}_i$, as we can compute

$$V(\mathfrak{a}_i) \cap V(\mathfrak{a}_j) = V(\mathfrak{a}_i + \mathfrak{a}_j) = V(A) = \varnothing, \quad \text{for all } i \neq j$$

and compute

$$\bigcup V(\mathfrak{a}_i) = V(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) = V(0) = \mathrm{Spec}(A)$$

We have already shown (ii) $\Longrightarrow$ (i). We now prove (i) $\Longrightarrow$ (iii). Write

$$\mathrm{Spec}(B) = V(\mathfrak{a}) \coprod V(\mathfrak{b})$$

where $V(\mathfrak{a}), V(\mathfrak{b})$ are nonempty. On one hand, by correspondence theorem, from

$$\varnothing = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b})$$

we know $\mathfrak{a} + \mathfrak{b} = (1)$, which by definition of comaximal ideal pair implies $1 = a + b$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. On the other hand, from

$$\mathrm{Spec}(B) = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$$

112

we know $\mathfrak{ab} \leq \mathrm{Nil}(B)$, which implies $a^n b^n = 0$ for some $n > 0$. Now, since $(a + b)^{2n} = 1^{2n} = 1$, we see $(a^n) + (b^n) = (1)$, which implies the existence of some $e \in (a^n)$ and $\widetilde{e} \in (b^n)$ that makes $e + \widetilde{e} = 1$. Computing:

$$e - e^2 = e\widetilde{e} \in (a^n b^n) = (0)$$

we see that e is idempotent. To see $e \neq 0, 1$, just observe that if so, then one of $V(\mathfrak{b}), V(\mathfrak{a})$ would be $\mathrm{Spec}(B)$.

(iii) $\implies$ (i): Let $e \neq 0, 1$ be idempotent. Clearly, $1 - e$ is also idempotent. Because the only idempotent unit is 1, we know both e and $1 - e$ are non-units. Therefore, (e) and $(1 - e)$ is a comaximal pair of proper ideals. Clearly, we have

$$(e) \cap (1 - e) \leq (e)(1 - e) = 0$$

Therefore, by definition of comaximal ideals, we have an isomorphism

$$B \cong B/(e) \times B/(1 - e)$$

as desired. $\blacksquare$

Theorem 3.1.6. (Spectrums are compact) Let A be a ring and $X \triangleq \mathrm{Spec}(A)$. Then open subset $U \subseteq X$ is compact if and only if U is a finite union of basic open sets. In particular, $X = U_0$ and U_f are compact.

Proof. ($\implies$) is clear. Let $f \in A$. Because finite union of compact set is compact, to prove ($\impliedby$), we only have to prove that U_f is compact. This is proved by a sequence of observation of equivalence. Trivially, $\{X - V(\mathfrak{a}_i) : i \in I\}$ covers U_f if and only if

$$V\left(\sum_{i \in I} \mathfrak{a}_i\right) = \bigcap_{i \in I} V(\mathfrak{a}_i) \subseteq V(f)$$

This is then equivalent to:

$$\sqrt{(f)} \leq \sqrt{\sum_{i \in I} \mathfrak{a}_i} \tag{3.4}$$

Since $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$, we know equation 3.4 is equivalent to:

$$f^n \in \sum_{i \in I} \mathfrak{a}_i \text{ for some } n > 0$$

The proof then follows from noting that we may select a finite subset $J \subseteq I$ such that $f^n \in \sum_{i \in J} \mathfrak{a}_i$ still holds. $\blacksquare$

Theorem 3.1.7. (Compact Hausdorff space X is naturally homeomorphic to the maximal spectrum of $C(X)$) Let X be a compact Hausdorff space and $C(X)$ the ring of continuous real-valued function on X. Give $\text{Max}(C(X))$ the subspace topology of $\text{Spec}(C(X))$. Because for all $x \in X$ the ring homomorphism $C(X) \to \mathbb{R}$ defined by $x \mapsto f(x)$ is surjective with kernel

$$\mathfrak{m}_x \triangleq \{f \in C(X) : f(x) = 0\}$$

We have a natural map

$$X \longrightarrow \text{Max}(C(X)); \quad x \mapsto \mathfrak{m}_x$$

Such map is a homeomorphism.

Proof. Let $x \neq y$. To prove injectivity, we are required to prove $\mathfrak{m}_x \neq \mathfrak{m}_y$. Because X is Hausdorff, we know $\{x\}, \{y\}$ are both closed in X. Therefore, by Urysohn's lemma, there exists some $f \in C(X)$ such that $f \in \mathfrak{m}_x - \mathfrak{m}_y$.

Let $\mathfrak{m} \in \text{Max}(C(X))$. To prove surjectivity, we are required to find $x \in X$ such that $\mathfrak{m} = \mathfrak{m}_x$. Define

$$V \triangleq \{x \in X : f(x) = 0 \text{ for all } f \in \mathfrak{m}\}$$

Clearly, if V is nonempty, then for all $x \in V$, we have $\mathfrak{m} \leq \mathfrak{m}_x$, which by maximality of $\mathfrak{m}$ implies $\mathfrak{m} = \mathfrak{m}_x$. Therefore, we only have to prove V is nonempty. Assume for a contradiction that V is empty. Then for all $x \in X$ there exists some $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Because X is compact, this gives us some

$$f \triangleq f_{x_1}^2 + \cdots + f_{x_n}^2 \in \mathfrak{m}$$

such that $f(x) \neq 0$ for all $x \in X$. Such f is clearly a unit in $C(X)$, a contradiction.

It remains to prove that the natural map is continuous and an open map. For all $f \in C(X)$, define

$$U_f \triangleq \{x \in X : f(x) \neq 0\} \quad \text{and} \quad \widetilde{U}_f \triangleq \{\mathfrak{m} \in \text{Max}(C(X)) : f \notin \mathfrak{m}\}$$

Because $\text{Max}(C(X))$ is given the subspace topology, we know that $\left\{\widetilde{U}_f\right\}$ is a basis for $\text{Max}(C(X))$. By Urysohn's lemma, for all $x \in X$ with neighborhood W, there exists some $f \in C(X)$ such that $f(\{x\}) = 1$ and $f(X - W) = 0$. In other words, $x \in U_f \subseteq W$. We have shown that $\{U_f\}$ form a basis for X. The rest of the proof then follows from computing:

$$x \in U_f \iff f(x) \neq 0 \iff f \notin \mathfrak{m}_x \iff \mathfrak{m}_x \in \widetilde{U}_f$$

■

Let k be an algebraically closed field. An **affine algebraic variety** $X \subseteq k^n$ is simply the solution set to some subset of $k[x_1, \ldots, x_n]$. The **ideal $I(X)$ of the variety** X is just the set of polynomial functions $f \in k[x_1, \ldots, x_n]$ that vanishes identically on X. The **coordinate function** ξ_i is simply the image of $x_i \in k[x_1, \ldots, x_n]$ onto the **coordinate ring** $P(X) \triangleq k[x_1, \ldots, x_n]/I(X)$.

For all $x \in X$, because the ideal

$$\mathfrak{m}_x \triangleq \{f \in P(X) : f(x) = 0\}$$

is the kernel of the natural surjective ring homomorphism $P(X) \twoheadrightarrow k$, we know $\mathfrak{m}_x$ are maximal. Therefore, we have a natural map $X \longrightarrow \mathrm{Max}(P(X))$. Such map is clearly injective, since if $x \neq y$, then $x_i \neq y_i$ for some i, which implies

$$\xi_i - x_i \in \mathfrak{m}_x - \mathfrak{m}_y$$

3.2　Boolean rings

A **Boolean ring** is a ring A that makes $x^2 = x$ for all $x \in A$.

Theorem 3.2.1. (Basic properties of Boolean rings) Let A be a Boolean ring. Then

(i) $2x = 0$ for all $x \in A$.

(ii) $\mathrm{Spec}(A) = \mathrm{Max}(A)$, and moreover, $A/\mathfrak{p} \cong \mathbb{Z}_2$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$.

(iii) Every finitely generated ideals $\trianglelefteq A$ is principal.

Proof. (i) is a consequence of $(x+1)^2 = x+1$. We now prove (ii). Because $0 = x^2 - x = x(x-1)$ for all $x \in A$ and because $A/\mathfrak{p}$ is an integral domain, we see that for all $x \in A$, either $x + \mathfrak{p} = 0$ or $(x-1) + \mathfrak{p} = 0 \in A/\mathfrak{p}$. In other words, there are only two elements in $A/\mathfrak{p}$, that is, $\mathfrak{p}$ and $1 + \mathfrak{p}$.

(iii) is proved by induction on number of generators. The base case of single generator is trivial. Let $\mathfrak{a} \triangleq (x_1, \ldots, x_n, y) \trianglelefteq A$. Inductive hypothesis stated that $(x_1, \ldots, x_n) = (x)$ for some $x \in A$. Let $z \triangleq x + y - xy$. Because $x = xz$ and $y = yz$, we have

$$\mathfrak{a} = (x, y) = (z)$$

as desired. ∎

Theorem 3.2.2. (Basic properties of spectrums of Boolean rings) Let A be a Boolean ring. Denote $X \triangleq \mathrm{Spec}(A)$. Then:

(i) The clopen subsets of X are exactly the basic open subsets.

(ii) For all $f_1, \ldots, f_n \in A$, there exists some $f \in A$ such that $X_f = X_{f_1} \cup \cdots \cup X_{f_n}$.

(iii) X is compact Hausdorff.

Proof. (ii) is a consequence of the fact that finitely generated ideals of Boolean rings are principal. In particular, given $(f) \triangleq (f_1, \ldots, f_n)$, we have

$$\bigcup X_{f_i} = X - \bigcap V(f_i) = X - V\left(\sum f_i\right) = X - V(f) = X_f$$

(i): To see basic open subsets X_f are clopen, one simply use the fact that $2f = 0$ to compute

$$X = X_f \coprod X_{1+f}$$

It remains to use (ii) to show all clopen subsets $Y \subseteq X$ are basic open subset. Because Y is closed in compact X, we know Y is also compact, which implies that Y is a finite union

116

of basic open subsets, which by (ii) implies that Y is a basic open subset.

(iii): Recall that X is compact even if A is not Boolean, so we only have to prove X is Hausdorff. Let $\mathfrak{p}, \mathfrak{q} \in X$ be two points such that every open set containing $\mathfrak{p}$ must also contains $\mathfrak{q}$. We are required to prove $\mathfrak{p} = \mathfrak{q}$, which follows from noting that for all $f \in A$, since $X = X_f \coprod X_{1+f}$, we have

$$f \notin \mathfrak{p} \iff \mathfrak{p} \in X_f \iff \mathfrak{q} \notin X_{1+f} \iff 1 + f \in \mathfrak{q} \iff f \notin \mathfrak{q}$$

where the last equivalence follows from the fact $A/\mathfrak{q} \cong \mathbb{Z}_2$. ∎

A **partial order** on a set L is a relation $\leq$ such that:

(i) $x \leq x$ for all $x \in L$ (**Reflexive**)

(ii) $x \leq y$ and $y \leq x \implies x = y$ (**Antisymmetry**)

(iii) $x \leq y \leq z \implies x \leq z$ (**Transitive**)

A **lattice** L is then just a partial ordered set such that every pair of element x, y of L there exists a **least upper bound** $x \wedge y$ and a **maximal lower bound** $x \vee y$. We say L is a **Boolean lattice** if

(i) L has a smallest element and a greatest element, denoted by 0 and 1.

(ii) $\wedge$ and $\vee$ are distributive over each other.

(iii) Every $x \in L$ has a unique **complement** x' such that $x \wedge x' = 1$ and $x \vee x' = 0$.

Theorem 3.2.3. (One-to-one correspondence between Boolean lattice and Boolean rings) Let L be a Boolean lattice. We may define addition and multiplication on L by:

$$x + y \triangleq (x \wedge y') \vee (x' \wedge y) \quad \text{and} \quad xy \triangleq x \wedge y$$

so that L becomes a Boolean ring. Conversely, given a Boolean ring A, we may define an ordering on A by

$$a \leq b \overset{\triangle}{\iff} a = ab$$

so that A become a Boolean lattice. The two correspondence are inverse to each other.

Proof. Routine. ∎

Corollary 3.2.4. (Stone's theorem for Boolean lattice) Every Boolean lattice L is isomorphic to the lattice of clopen subsets of some compact Hausdorff space.

Proof. Let A be the Boolean ring induced by L. It then follows from properties of spectrum of Boolean ring that $\mathrm{Spec}(A)$ is the compact Hausdorff space we are looking for. ∎

3.3 Topological Preliminary

Equivalent Definition 3.3.1. (Normal space) We say a topological space X is **normal** if any of the followings hold true:

(i) For every two disjoint closed subsets $A, B \subseteq X$, there exists a disjoint pair of open subsets $\widetilde{A}, \widetilde{B} \subseteq X$ such that $A \subseteq \widetilde{A}$ and $B \subseteq \widetilde{B}$.

(ii) For every two disjoint closed subsets $A, B \subseteq X$, there exists some continuous $f : X \to [0, 1]$ such that $f(A) = 0$ and $f(B) = 1$.

The proof of their equivalence is called the **Urysohn's lemma**.

Proof. Wikipedia has a detailed proof. ∎

Theorem 3.3.2. (Compact Hausdorff spaces are normal) Let X be a compact Hausdorff topological space. Then X is normal.

Proof. See this proof on MSE. ∎

Chapter 4

Homological Algebra

4.1 General Categories

In this note, a **category** $\mathcal{C}$ is

(i) A *class* $\mathrm{ob}(\mathcal{C})$ of **objects**.

(ii) For each two objects $A, B \in \mathcal{C}$, a *set* $\mathrm{Hom}(A, B)$ of **morphism**.

(iii) For every three objects $A, B, C \in \mathcal{C}$, a map

$$\mathrm{Hom}_{\mathcal{C}}(B, C) \times \mathrm{Hom}_{\mathcal{C}}(B, A) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C)$$

called the **composition**.

that satisfies two conditions:

(i) For all $A \in \mathcal{C}$, there exists an **identity morphism** $1_A \in \mathrm{End}(A)$ that makes $f = f \circ 1_A$ and $g = 1_B \circ g$ for all $f : A \to B$ and $g : B \to C$. (**Identity**)

(ii) $(f \circ g) \circ h = f \circ (g \circ h)$ (**Associativity**)

Let $\mathcal{C}$ be a category and $f : A \to B$ and $g : B \to A$ be two morphisms in $\mathcal{C}$. We say g is a **left inverse of** f if

$$g \circ f = 1_A$$

and say g is a **right inverse of** f if

$$f \circ g = 1_B$$

If simultaneously g is both a left and right inverse of f, then we say f and g are **inverse to each other**, that they are both **isomorphisms**, and A, B are **isomorphic**. Let $\mathcal{C}$ be a

category. A morphism $f : A \hookrightarrow B$ is said to be a **monomorphism** if for all $g, h : C \to A$, we have

$$f \circ g = f \circ h \implies g = h$$

A morphism $f : A \twoheadrightarrow B$ is said to be an **epimorphism** if for all $g, h : B \to C$, we have

$$g \circ f = h \circ f \implies g = h$$

Theorem 4.1.1. (Basic properties of morphisms) Let $\mathcal{C}$ be a category and $f : A \to B$ be a morphism in $\mathcal{C}$. Then

(i) If f is a right inverse of some $g : B \to A$, then f is a monomorphism.

(ii) If f is a left inverse of some $g : B \to A$, then f is an epimorphism.

(iii) Compositions of monomorphisms are monomorphisms.

(iv) Compositions of epimorphisms are epimorphisms.

Proof. Routine. $\blacksquare$

Let $B \in \mathcal{C}$. A **subobject of** B is an object A together with a monomorphism $i : A \hookrightarrow B$, and a **quotient of** B is an object C with an epimorphism $\pi : B \twoheadrightarrow C$. An **initial object** $I \in \mathcal{C}$ is an object such that for all $A \in \mathcal{C}$, there exists exactly one morphism from I to A. A **terminal object** $T \in \mathcal{C}$ is an object such that for all $A \in \mathcal{C}$, there exists exactly one morphism from A to T. Clearly, initial objects and terminal objects, even though may not always exists, are unique up to isomorphisms. A **zero object** is an object that is both an initial and terminal object.

Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. A **covariant functor** (or simply, a **functor**) $F : \mathcal{C} \to \mathcal{D}$ is a map of objects $F : \mathrm{ob}(\mathcal{C}) \to \mathrm{ob}(\mathcal{D})$ together with a map of morphisms:

$$F : \mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$$

that satisfies

$$F(1_A) = 1_{F(A)} \quad \text{and} \quad F(g \circ h) = F(g) \circ F(h)$$

Let $\mathcal{X}$ be an arbitrary category and $F : \mathcal{X} \to \mathcal{C}$ a covariant functor. A **cone to** F is an object $N \in \mathcal{C}$ together with a family of morphisms $\psi_X : N \to F(X)$ indexed by $\mathcal{X}$ such that for all $f : X \to Y$, the diagram

commutes. A cone $(\lim F, \phi)$ to F is said to satisfy the **universal property of limit** if for all cones (N, ψ) to F there exists a unique morphism $u : N \to \lim F$ that makes the diagram

commutes for all $f : X \to Y$. A **directed set** is a partially ordered set in which every two elements have an upper bound. Let I be a directed set and $\mathcal{C}$ a category. By an **inverse system in** $\mathcal{C}$, we mean a collection of object A_i in $\mathcal{C}$ indexed by I together with each relation $i \leq j$ (*note the order*) a morphism $f_{ij} : A_j \to A_i$ in $\mathcal{C}$ such that:

(i) f_{ii} are the identities on A_i.

(ii) $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$

Clearly, an inverse system in $\mathcal{C}$ itself forms a category $\mathcal{I}$ the obvious way, and we have an obvious covariant functor $F : \mathcal{I} \to \mathcal{C}$. The limit of F is then called the **inverse limit of** A_i denoted by $\varprojlim A_i$ and $f_i : \varprojlim A_i \to A_i$.

Let $\mathcal{X}$ be an arbitrary category and $F : \mathcal{X} \to \mathcal{C}$ a covariant functor. A **co-cone to** F is an object $N \in \mathcal{C}$ together with a family of morphisms $\psi_X : F(X) \to N$ indexed by $\mathcal{X}$ such that for all $f : X \to Y$, the diagram

commute. A co-cone $(\operatorname{colim} F, \phi)$ to F is said to satisfy the **universal property of colimit** if for all co-cones (N, ψ) to F there exists a unique morphism $u : \operatorname{colim} F \to N$ that makes

the diagram

$$
\begin{array}{ccc}
F(X) & \xrightarrow{\;F(f)\;} & F(Y)
\end{array}
$$

$$
\phi_X \qquad \phi_Y
$$

$$
\mathrm{colim}\,F
$$

$$
\psi_X \qquad\qquad u \qquad\qquad \psi_Y
$$

$$
N
$$
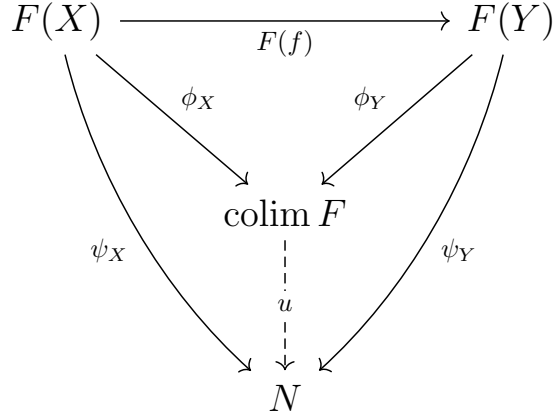
commute for all $f : X \to Y$. Let I be a directed set. By a **directed system in** $\mathcal{C}$, we mean a collection of object A_i in $\mathcal{C}$ indexed by I together with each relation $i \leq j$ (again, *note the order*) a morphism $f_{ij} : A_i \to A_j$ in $\mathcal{C}$ such that:

(i) f_{ii} are the identities on A_i.

(ii) $f_{ik} = f_{jk} \circ f_{ij}$ for all $i \leq j \leq k$

Clearly, a directed system in $\mathcal{C}$ forms a category $\mathcal{I}$ the obvious way, and we have an obvious covariant functor $F : \mathcal{I} \to \mathcal{C}$. The colimit of F is then called the **direct limit of** A_i denoted by $\varinjlim A_i$ and $f_i : A_i \to \varinjlim A_i$.

Let A_i be a collection of objects in $\mathcal{C}$. Clearly, we can make it a category $\mathcal{J}$ by requiring it to have only the identity morphisms, and doing such, we have an obvious covariant functor $F : \mathcal{J} \to \mathcal{C}$. Its *limit* is called the **product of** A_i denoted by $\prod A_i$, with canonical morphism $p_i : \prod A_i \to A_i$ called the **projection map**, and its *colimit* is called the **coproduct of** A_i denoted by $\coprod A_i$, whose canonical morphism $A_i \to \coprod A_i$ are often called the **coprojection map**.

Theorem 4.1.2. (Existence of products and coproduct in familiar categories) Let A be a ring. Product and coproduct always exists

(i) in **Set** and **Top**, in the form of Cartesian product and disjoint union.

(ii) in **Gp**, in the form of direct product and free product.

(iii) in **Ring**, in the form of direct product and tensor product as $\mathbb{Z}$-algebras.

(iv) in **Mod**$_A$ and **Ab**, in the form of direct product and direct sum.

Proof. Routine. ∎

Note that by the **free product $A_1 * A_2$ of two groups**, we mean the group defined by presentation

$$A_1 * A_2 \triangleq \langle S_{A_1} \cup S_{A_2} \mid R_{A_1} \cup R_{A_2} \rangle$$

given that

$$A_1 = \langle S_{A_1} \mid R_{A_1} \rangle \quad \text{and} \quad A_2 = \langle S_{A_2} \mid R_{A_2} \rangle$$

Let $A, B \in \mathcal{C}$ and f and g be morphism from A to B. Again, they form a category $\mathcal{I}$:

$$A \underset{g}{\overset{f}{\rightrightarrows}} B$$

whose limit is called the **equalizer** $\mathrm{eq}(f, g)$ and whose colimit is called the **coequalizer** $\mathrm{coeq}(f, g)$. Clearly, if the equalizer exists and the canonical morphism from $\mathrm{eq}(f, g)$ to A is h, then we must have $f \circ h = g \circ h$, since they are both the morphism of the right hand side arrow of the commutative diagram:

Similar statement holds true for coequalizer. If the canonical morphism from B to $\mathrm{coeq}(f, g)$ is k, then the canonical morphism from A to $\mathrm{coeq}(f, g)$ is $k \circ g = k \circ f$

Theorem 4.1.3. (Equalizer and coequalizer in familiar categories) Let R be a ring. In $\mathbf{Set}, \mathbf{Gp}, \mathbf{Ab}, \mathbf{Ring}$, and $\mathbf{Mod}_R$, the equalizer of two morphisms $f, g : A \to B$ is simply

$$\mathrm{eq}(f, g) = \{a \in A : f(a) = g(a)\}$$

In $\mathbf{Gp}$, their coequalizer is the quotient

$$\mathrm{coeq}(f, g) = B \big/ \mathrm{ncl}_B \left(\{f(a)g(a)^{-1} \in B : a \in A\} \right)$$

In **Ring**, their coequalizer is

$$\mathrm{coeq}(f, g) = B / \mathfrak{b}$$

where $\mathfrak{b} \trianglelefteq B$ is the ideal generated by $\{f(a) - g(a) \in B : a \in A\}$. In **Ab** and $\mathbf{Mod}_R$, we don't have to take normal closure. Their coequalizer is then

$$\mathrm{coeq}(f, g) = \mathrm{Coker}(f - g)$$

Proof. Routine. ∎

Theorem 4.1.4. (Canonical morphism of equalizer is a monomorphism, and the canonical morphism of coequalizer is an epimorphism) Let $\mathcal{C}$ be a category in which we have a diagram

$$A \xrightarrow[\;\;g\;\;]{\;\;f\;\;} B$$

If the equalizer $\mathrm{eq}(f, g)$ exists, then the canonical morphism $h : \mathrm{eq}(f, g) \to A$ is a monomorphism. If the coequalizer $\mathrm{coeq}(f, g)$ exists, then the canonical morphism $k : B \to \mathrm{coeq}(k)$ is an epimorphism.

$$\mathrm{eq}(f, g) \hookrightarrow A \xrightarrow[\;\;g\;\;]{\;\;f\;\;} B \twoheadrightarrow \mathrm{coeq}(f, g)$$

Proof. Routine. ∎

Theorem 4.1.5. (Finite limit theorem) Let $\mathcal{C}$ be a category. Then the following two statements are equivalent

  (i) All finite (including the arrows) diagrams in $\mathcal{C}$ have a limit.

 (ii) All finite product and equalizer exist.

The following two statements are also equivalent

  (i) All finite (including the arrows) diagrams in $\mathcal{C}$ have a colimit.

 (ii) All finite coproduct and coequalizer exist.

Proof. Because the proofs for two equivalence are dual to each other, we only prove the first one. Clearly (i) $\Longrightarrow$ (ii). We now prove (ii) $\Longrightarrow$ (i). Let a diagram in $\mathcal{C}$ consists of objects M_i indexed by $i \in I$ and arrows a indexed by A. For all $a \in A$, denote its source and target by $s(a)$ and $t(a)$. Denote the canonical morphism by

$$p_i : \prod_{i \in I} M_i \to M_i \quad \text{and} \quad \widetilde{p}_a : \prod_{a \in A} M_{t(a)} \to M_{t(a)}$$

124

By universal property, we then know there exist $\phi, \psi : \prod_{i \in I} M_i \to \prod_{a \in A} M_{t(a)}$ that makes

$$\widetilde{p}_a \circ \phi = p_{t(a)} \quad \text{and} \quad \widetilde{p}_a \circ \psi = a \circ p_{s(a)}$$

The proof then follows from verifying that the equalizer $\text{eq}(\phi, \psi)$ together with $p \circ_i \circ h$ satisfies the universal property of limit of the diagram, where $h : \text{eq}(\phi, \psi) \to \prod_{i \in I} M_i$ is the canonical morphism of equalizer. ∎

Let $\mathcal{C}$ be a category in which we have a diagram:

$$A_1 \qquad\qquad A_2$$
$$f_1 \searrow \qquad \swarrow f_2$$
$$B$$
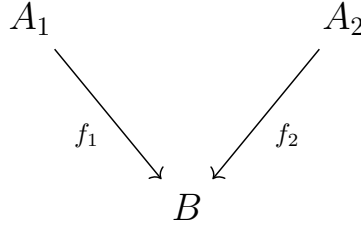
Clearly, this form a category $\mathcal{I}$ with an obvious covariant functor $F : \mathcal{I} \to \mathcal{C}$. The limit of this covariant functor is then called the **fiber product** $A_1 \times_B A_2$ **over** B, or by some author, the **pullback of** A_1 **and** A_2 **over** B.

$$A_1 \times_B A_2$$

with morphisms p_1, p_2 to A_1, A_2 and f_1, f_2 to B.
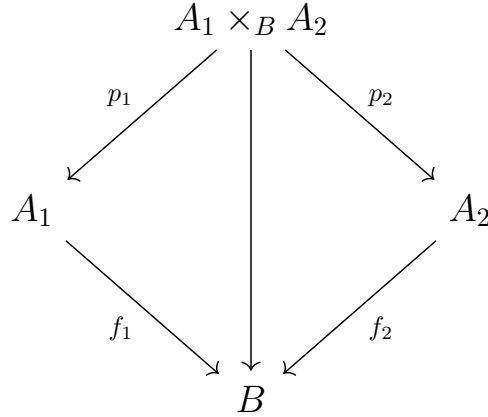
Theorem 4.1.6. (Existence of fiber product in familiar categories) Let R be a ring. In **Set**, **Gp**, **Ab**, **Ring**, and $\textbf{Mod}_R$, the fiber product of $f_1 : A_1 \to B$ and $f_2 : A_2 \to B$ can be constructed as a subobject of the product $A_1 \times A_2$ by

$$A_1 \times_B A_2 = \{(a_1, a_2) \in A_1 \times A_2 : f_1(a_1) = f_2(a_2)\}$$

Proof. Routine. ∎

Let $\mathcal{C}$ be a category in which we have a diagram:

$$B$$
$$f_1 \swarrow \qquad \searrow f_2$$
$$A_1 \qquad\qquad A_2$$
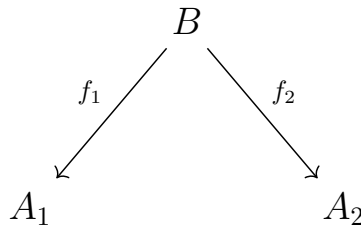
The diagram clearly forms a category $\mathcal{I}$ with an obvious covariant functor $F : \mathcal{I} \to \mathcal{C}$. The colimit of this covariant functor is then called the **fiber coproduct $A_1 +_B A_2$ over B**, or by some author, the **pushout of A_1 and A_2 over B**

$$
\begin{array}{ccc}
 & B & \\
f_1 \swarrow & \downarrow & \searrow f_2 \\
A_1 & & A_2 \\
i_1 \searrow & \downarrow & \swarrow i_2 \\
 & A_1 +_B A_2 &
\end{array}
$$
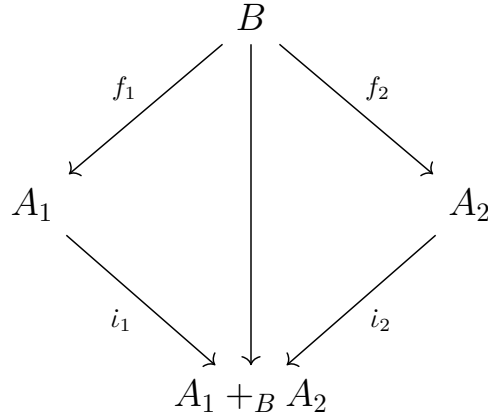
Theorem 4.1.7. (Existence of fiber coproduct in familiar categories) Let R be a ring. In **Gp**, the fiber coproduct of $f_1 : B \to A_1$ and $f_2 : B \to A_2$ is

$$ A_1 +_B A_2 = A_1 * A_2 \big/ \mathrm{ncl}_{A_1 * A_2}\left(\left\{ f_1(b)f_2(b)^{-1} \in A_1 * A_2 : b \in B \right\}\right) $$

where $A_1 * A_2$. In **Ab** and $\mathbf{Mod}_R$, their fiber coproduct can be constructed as a quotient of their direct product

$$ A_1 +_B A_2 = A_1 \times A_2 \big/ \left\{ (f_1(b), -f_2(b)) \in A_1 \times A_2 : b \in B \right\} $$

In **Ring**, their fiber coproduct is their tensor product as B-algebras:

$$ A_1 +_B A_2 = A_1 \otimes_B A_2 $$

Proof. Routine. ∎

Given two covariant functors $F, F' : \mathcal{C} \to \mathcal{D}$, by a **natural transformation $\eta : F \rightsquigarrow F'$**, we mean a class of morphisms $\eta_A : F(A) \to F'(A)$ in $\mathcal{D}$ indexed by $\mathcal{C}$ that makes the diagram:

$$
\begin{array}{ccc}
F(A) & \xrightarrow{\eta_A} & F'(A) \\
F(f) \downarrow & & \downarrow F'(f) \\
F(B) & \xrightarrow{\eta_B} & F'(B)
\end{array}
$$

commutes for all $f : A \to B$ in $\mathcal{C}$. The **functor category** $\mathrm{Func}(\mathcal{C}, \mathcal{D})$ is then the category whose objects is the class of covariant functors from $\mathcal{C}$ to $\mathcal{D}$ and whose morphisms are natural transformations. We say a category $\mathcal{C}$ is **small** if the class $\mathrm{ob}(\mathcal{C})$ is a set.

4.2 Additive Categories

An **additive category** $\mathcal{A}$ is a category such that $\mathrm{Hom}(A, B)$ is an abelian group (thus a set) for all $A, B \in \mathcal{A}$ that satisfies

$$(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g \quad \text{and} \quad f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$$

and

(i) $\mathcal{A}$ admits zero object.

(ii) $\mathcal{A}$ admits *finite* coproducts.

Let $f : A \to B$ be a morphism in an additive category $\mathcal{A}$. We say a morphism $i : \ker(f) \hookrightarrow A$ satisfies the **universal property of kernel** if

(i) $f \circ i = 0$.

(ii) For all $h : C \to A$ that makes $f \circ h = 0$, there exists a unique morphism $u : C \to \ker(f)$ that makes the diagram:

commutes.

We say a morphism $\pi : B \twoheadrightarrow \mathrm{Coker}(f)$ satisfies the **universal property of cokernel** if

(i) $\pi \circ f = 0$.

(ii) For all $h : B \to C$ that makes $h \circ f = 0$, there exists a unique morphism $u : \mathrm{Coker}(f)$ that makes the diagram:

commutes.

127

Note that the notion of kernel and cokernel can be generalized to categories that are not additive, as long as the category admits zero morphism. Therefore, even though **Gp** isn't additive due to the lack of abelian group structure on Hom-set, **Gp** still have categorical kernel. On the other hand, **Ring** isn't additive and there isn't a good way to define zero morphism in it, so **Ring** has no categorical kernel. Indeed, the "kernel" of a group homomorphism forms a group, and the "kernel" of a ring homomorphism don't always form a ring.

Theorem 4.2.1. (Basic properties of additive categories) Let $\mathcal{A}$ be an additive category. Then

(i) Let A and B be a pair of objects in $\mathcal{A}$, and Z be a zero object in $\mathcal{A}$ with

$$A \xrightarrow{f} Z \xrightarrow{g} B$$

Then $g \circ f$ is the zero in the abelian group $\mathrm{Hom}(A, B)$.

(ii) Given a *finite* collection of objects $A_1, \ldots, A_n \in \mathcal{A}$ and a object A together with a collection of morphism $A_i \xrightarrow{i_i} A \xrightarrow{p_i} A_i$ that satisfies

$$p_i \circ i_j \triangleq \begin{cases} \mathbf{id}_{A_i} & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases} \quad \text{and} \quad \sum i_i \circ p_i = \mathbf{id}_A$$

then the morphisms i_i and p_i respectively satisfies the universal property of coproduct and product. In particular, any finite product and finite coproduct can be made a coproduct and product this way.

(iii) $Z \in \mathcal{A}$ is a zero object $\iff$ $\mathbf{id}_Z$ is the zero in $\mathrm{Hom}(Z, Z)$.

(iv) Canonical morphisms of *finite* products and coproducts in $\mathcal{A}$ are respectively epimorphisms and monomorphisms.

(v) Let $f : A \to B$ be a morphism in $\mathcal{A}$ that has both $i : \ker(f) \hookrightarrow A$ and $\pi : B \twoheadrightarrow \mathrm{Coker}(f)$. Then i is indeed a monomorphism, and π is indeed an epimorphism.

Proof. They are all routine. Note that (iv) follows from (ii) and the fact that left inverses are epimorphisms and right inverses are monomorphisms. ∎

Clearly, given an additive category $\mathcal{A}$ and a small category $\mathcal{C}$, the functor category $\mathrm{Func}(\mathcal{C}, \mathcal{A})$ form an additive category the obvious way. Also, if all kernels and cokernels exists in $\mathcal{A}$, we may construct kernels and cokernels in $\mathrm{Func}(\mathcal{C}, \mathcal{A})$ component wise.

Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A **contravariant functor** $G : \mathcal{C} \to \mathcal{D}$ is a map of objects $G : \mathrm{ob}(\mathcal{C}) \to \mathrm{ob}(\mathcal{D})$ together with a map of morphisms:

$$G : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(G(B), G(A))$$

such that

$$G(\mathbf{id}_A) = \mathbf{id}_{G(A)} \quad \text{and} \quad G(g \circ h) = G(h) \circ G(g)$$

Let $F : \mathcal{A} \to \mathcal{B}$ and $G : \mathcal{A} \to \mathcal{B}$ be respectively covariant and contravariant functors between additive categories. We say F and G are **additive** if for all $A, B \in \mathcal{A}$, respectively, the map $\mathrm{Hom}_{\mathcal{A}}(A, B) \to \mathrm{Hom}_{\mathcal{B}}(F(A), F(B))$ and the map $\mathrm{Hom}_{\mathcal{A}}(A, B) \to \mathrm{Hom}_{\mathcal{B}}(G(B), G(A))$ are group homomorphisms.

Theorem 4.2.2. (Basic property of additive functor) Let $F : \mathcal{A} \to \mathcal{B}$ and $G : \mathcal{A} \to \mathcal{B}$ be additive covariant and additive contravariant additive functor between additive categories. Then

(i) F and G both map zero object to zero objects.

(ii) If *finite* $A_i \longrightarrow A$ satisfies universal property of coproduct, then $F(A_i) \longrightarrow F(A)$ satisfies universal property of coproduct. Dually, if *finite* $A \longrightarrow A_i$ satisfies universal property of product, then $F(A) \longrightarrow F(A_i)$ satisfies universal property of product.

Proof. (i) follows from the characterization of zero objects in additive categories. (ii) and (iii) follows from the characterization of biproduct. $\blacksquare$

4.3   Abelian Categories

Suppose the *additive* category $\mathcal{A}$ admits all kernels and cokernels. We then define the **image** and **coimage** of a morphism $f : A \to B$ to be

$$\mathrm{Im}(f) \triangleq \ker(B \twoheadrightarrow \mathrm{Coker}(f)) \quad \text{and} \quad \mathrm{Coim}(f) \triangleq \mathrm{Coker}(\ker(f) \hookrightarrow A)$$

In other word, given the canonical morphisms:

$$\ker(f) \overset{i}{\longrightarrow} A \overset{f}{\longrightarrow} B \overset{\pi}{\twoheadrightarrow} \mathrm{Coker}(f)$$

The morphism $\pi' : A \twoheadrightarrow \mathrm{Im}(f)$ satisfies the **universal property of coimages** if

(i) $\pi' \circ i = 0$.

(ii) For all $h : A \to C$ that makes $h \circ i = 0$, there exists a unique morphism $u : \mathrm{Coim}(f) \to C$ that makes the diagram:

$$
\begin{array}{ccccc}
\ker(f) & \overset{i}{\lhook\joinrel\longrightarrow} & A & \overset{\pi'}{\longrightarrow\!\!\!\twoheadrightarrow} & \mathrm{Coim}(f) \\
 & & & \overset{h}{\searrow} & \Big\downarrow{\scriptstyle u} \\
 & & & & C
\end{array}
$$

commutes.

and the morphism $i' : \mathrm{Im}(f) \hookrightarrow B$ satisfies the **universal property of image** if

(i) $\pi \circ i' = 0$.

(ii) For all $h : C \to B$ that makes $\pi \circ h = 0$, there exists a unique morphism $u : C \to \mathrm{Im}(f)$ that makes the diagram:

$$
\begin{array}{ccccc}
\mathrm{Im}(f) & \overset{i'}{\lhook\joinrel\longrightarrow} & B & \overset{\pi}{\longrightarrow\!\!\!\twoheadrightarrow} & \mathrm{Coker}(f) \\
\Big\uparrow{\scriptstyle u} & \overset{h}{\nearrow} & & & \\
C & & & &
\end{array}
$$

commutes.

Theorem 4.3.1. (Existence and uniqueness of the canonical morphism from coimage to image) Let $\mathcal{A}$ be an additive category that admits all kernels and cokernels and $f : A \to B$ be a morphism in $\mathcal{A}$. Then there exists a unique morphism

$u : \operatorname{Coim}(f) \to \operatorname{Im}(f)$ that makes the diagram:

$$
\begin{array}{ccc}
A & \xrightarrow{\ \ f\ \ } & B \\
\pi' \downarrow & & \uparrow i' \\
\operatorname{Coim}(f) & \xrightarrow{\ \ u\ \ } & \operatorname{Im}(f)
\end{array}
$$

commute.

Proof. Note that the uniqueness of u follows from the fact that i' is a monomorphism and π' is an epimorphism. We now prove its existence. Because $f \circ i = 0$, by universal property of coimage, there exists a unique morphism $u' : \operatorname{Coim}(f) \to B$ such that $f = u' \circ \pi'$. Therefore, we can deduce

$$
\pi \circ f = 0 \implies \pi \circ u' \circ \pi' = 0
$$

Then, because $0 \circ \pi' = 0$ and because π' is an epimorphism, we see $\pi \circ u' = 0$. This then by universal property of images implies the existence of some $u : \operatorname{Coim}(f) \to \operatorname{Im}(f)$ that makes $u' = i' \circ u$. Therefore,

$$
f = u' \circ \pi' = i' \circ u \circ \pi'
$$

as desired. ∎

We say f is **strict** if such canonical morphism $u : \operatorname{Coim}(f) \to \operatorname{Im}(f)$ is an isomorphism, and we say this *additive* category $\mathcal{A}$ is **abelian** if all of its morphisms are strict. Note that clearly, given an abelian category $\mathcal{A}$ and an small category $\mathcal{C}$, the functor category $\operatorname{Func}(\mathcal{C}, \mathcal{A})$ is also abelian, and the image and coimages can be constructed componentwise.

Theorem 4.3.2. (Basic properties of abelian categories) Let $\mathcal{A}$ be an abelian category. Then

(i) All finite (including the arrows) diagrams in $\mathcal{A}$ have limits and colimits.

(ii) Fiber products of $f_1 : A_1 \to B$ and $f_2 : A_2 \to B$ exist in $\mathcal{A}$ in the form of

$$
A_1 \times_B A_2 \triangleq \ker\left((f_1, -f_2) : A_1 \oplus A_2 \to B\right)
$$

(iii) Fiber coproducts of $g_1 : B \to A_1$ and $g_2 : B \to A_2$ exists in $\mathcal{A}$ in the form of

$$
A_1 +_B A_2 \triangleq \operatorname{Coker}((g_1, -g_2) : B \to A_1 \oplus A_2)
$$

Proof. (i) is a corollary of finite limit theorem, in which one construct equalizer and co-equalizer by

$$\mathrm{eq}(f,g) \triangleq \ker(f-g) \quad \text{and} \quad \mathrm{coeq}(f,g) \triangleq \mathrm{Coker}(f-g)$$

(ii) and (iii) are routine checking. ∎

Theorem 4.3.3. (Existence and uniqueness of the canonical morphism for homologies) Let $\mathcal{A}$ be an abelian category in which we have morphisms $f : A \to B$ and $g : B \to C$ that satisfies $g \circ f = 0$. Denote the canonical morphisms of coimage and image of f by $\pi' : A \twoheadrightarrow \mathrm{Coim}(f)$ and $i' : \mathrm{Im}(f) \hookrightarrow B$, and let $u : \mathrm{Coim}(f) \to \mathrm{Im}(f)$ be the unique isomorphism that satisfies $f = i' \circ u \circ \pi'$, which we have proved to exist uniquely. Denote $\widetilde{f} \triangleq u \circ \pi' : A \to \mathrm{Im}(f)$. Then there exists a unique morphism $\widetilde{u} : \mathrm{Im}(f) \to \ker(g)$ such that

$$f = i \circ \widetilde{u} \circ \widetilde{f}$$

where $i : \ker(g) \to B$ is the canonical morphism of kernel of g.

Proof. Because u is an isomorphism and π' is an epimorphism, we know $\widetilde{f}$ is an epimorphism. The uniqueness of $\widetilde{u}$ then follows from the fact that i is a monomorphism. We now prove its existence.

Denote the canonical morphism of cokernel of f by $\pi : B \twoheadrightarrow \mathrm{Coker}(f)$. Because $g \circ f = 0$, by the universal property of cokernel of f, there exists a unique morphism $\widetilde{g} : \mathrm{Coker}(f) \to C$ that makes $g = \widetilde{g} \circ \pi$. Therefore, because $\pi \circ i' = 0$ by definition of image of f, we have:

$$g \circ i' = \widetilde{g} \circ \pi \circ i' = g \circ 0 = 0$$

This then by universal property of kernel of g induce a unique morphism $\widetilde{u} : \mathrm{Im}(f) \to \ker(g)$ that makes $i' = i \circ \widetilde{u}$. By premise, we now see

$$i \circ \widetilde{u} \circ \widetilde{f} = i' \circ u \circ \pi' = f$$

as desired. ∎

Let $\mathcal{A}$ be an abelian category in which we have morphisms $f : A \to B$ and $g : B \to C$ that satisfies $g \circ f = 0$. The **(co) homology** at this point is then defined to be $\mathrm{Coker}(\widetilde{u})$ where $\widetilde{u} : \mathrm{Im}(f) \to \ker(g)$ is from theorem 4.3.3.

We shall make an important remark here. Let A be a ring. For completeness, the theorems in the rest of this chapter will still be stated in the language of abelian categories, but the proof will only be done for $\mathbf{Mod}_A$, since a proof for the latter can always be easily modified to be a proof for the former. Moreover, for the sake of style, we will use $\oplus$ in place of $\coprod$.

132

Theorem 4.3.4. (Split lemma) Let

$$0 \longrightarrow A \overset{q}{\hookrightarrow} B \overset{r}{\twoheadrightarrow} C \longrightarrow 0$$

be a short exact sequence in an abelian category $\mathcal{A}$. The followings are equivalent:

(i) There exists a morphism $t : B \to A$ such that $t \circ q = \mathbf{id}_A$. **(Left Splits)**

(ii) There exists a morphism $u : C \to B$ such that $r \circ u = \mathbf{id}_C$. **(Right Splits)**

(iii) There exists an isomorphism $h : B \to A \oplus C$ such that $h \circ q : A \to A \oplus C$ and $r \circ h^{-1} : A \oplus C \to C$ are the canonical morphism. **(Direct sum)**

Proof. Routine. ∎

Theorem 4.3.5. (Snake lemma) Let

be a commutative diagram in an abelian category $\mathcal{A}$ with rows exact. Then we have a *canonical* exact sequence:

$$\ker(f') \overset{u}{\longrightarrow} \ker(f) \overset{v}{\longrightarrow} \ker(f'') \overset{d}{\longrightarrow} \mathrm{Coker}(f') \overset{\widetilde{u}'}{\longrightarrow} \mathrm{Coker}(f) \overset{\widetilde{v}'}{\longrightarrow} \mathrm{Coker}(f'')$$

where

(i) The morphism $u : \ker(f') \to \ker(f)$ is injective if $u : M' \to M$.

(ii) The morphism $\widetilde{v}' : \mathrm{Coker}(f) \to \mathrm{Coker}(\widetilde{f}'')$ is surjective if $v' : N' \to N''$ is.

Proof. Routine. Here, we give an outline for inducing of the **boundary homomorphism** $d : \ker(f'') \to \mathrm{Coker}(f')$. Let $x'' \in \ker(f'')$. Because v is surjective, we know $x'' = v(x)$ for some $x \in M$. Therefore, $v' \circ f(x) = f'' \circ v(x) = 0$, which implies $f(x) \in \ker(v') = \mathrm{Im}(u')$, that is, $f(x) = u'(y')$ for some $y' \in N'$. The boundary homomorphism can be induced by

$$d(x'') \triangleq y' + \mathrm{Im}(f')$$

∎

Let $\mathcal{A}$ be an abelian category and $\mathcal{C}$ be a subclass of $\mathcal{A}$ that contains a zero object. A function $\lambda : \mathcal{C} \to \mathbb{Z}$ is said to be **additive** if for all short exact sequence

$$0 \longrightarrow A' \lhook\joinrel\longrightarrow A \longrightarrow\!\!\!\!\!\rightarrow A'' \longrightarrow 0$$

in $\mathcal{C}$, the function λ satisfies

$$\lambda(A') - \lambda(A) + \lambda(A'') = 0 \quad \text{and} \quad \lambda(0) = 0$$

Theorem 4.3.6. (Additive functions on long exact sequences) Let $\mathcal{A}$ be an abelian category, $\mathcal{C}$ a subclass of $\mathcal{A}$ that contains a zero object, and an additive function $\lambda : \mathcal{C} \to \mathbb{Z}$. Given an exact sequence

$$0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow \cdots \longrightarrow M_n \longrightarrow 0$$

whose all terms, including the kernels, are in $\mathcal{C}$, we have

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$$

Proof. Let $N_i \leq M_i$ be the kernels. Then the proof follows from noting that for all $0 \leq i \leq n$, we have a short exact sequence

$$0 \longrightarrow N_i \lhook\joinrel\longrightarrow M_i \longrightarrow\!\!\!\!\!\rightarrow N_{i+1} \longrightarrow 0$$

$\blacksquare$

4.4 Homologies and Cohomologies

Let $\mathcal{A}$ be an abelian category. A **chain** $A_\bullet$ in $\mathcal{A}$ is a sequence of the form:

$$\cdots \longleftarrow A_{i-1} \xleftarrow{\ d_i\ } A_i \xleftarrow{\ d_{i+1}\ } A_{i+1} \longleftarrow \cdots$$

in which $d_i \circ d_{i+1} = 0$ for all $i \in \mathbb{Z}$, and a **cochain** $A^\bullet$ in $\mathcal{A}$ is a sequence of the form:

$$\cdots \longrightarrow A^{i-1} \xrightarrow{\ d^{i-1}\ } A^i \xrightarrow{\ d^i\ } A^{i+1} \longrightarrow \cdots$$

in which $d^i \circ d^{i-1} = 0$ for all $i \in \mathbb{Z}$. The **homology** $H_\bullet(A_\bullet)$ and the **cohomology** $H^\bullet(A^\bullet)$ are then defined by:

$$H_i(A_\bullet) \triangleq \frac{\ker(d_i)}{\mathrm{Im}(d_{i+1})} \quad \text{and} \quad H^i(A^\bullet) \triangleq \frac{\ker(d^i)}{\mathrm{Im}(d^{i-1})}$$

Clearly, we can make the class $\mathbf{Ch}(\mathcal{A})$ of chains in $\mathcal{A}$ an abelian category by requiring the morphisms $f_\bullet : A_\bullet \to B_\bullet$ to be sets $f_i : A_i \to B_i$ of morphisms that makes

$$d_i \circ f_i = f_{i-1} \circ d_i$$

In other words, f_i make the diagram:

$$
\begin{array}{ccccccccc}
\cdots & \longleftarrow & A_{i-1} & \xleftarrow{\ d_i\ } & A_i & \xleftarrow{\ d_{i+1}\ } & A_{i+1} & \longleftarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{i-1}} & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f_{i+1}} & & \\
\cdots & \longleftarrow & B_{i-1} & \xleftarrow[\ d_i\ ]{} & B_i & \xleftarrow[\ d_{i+1}\ ]{} & B_{i+1} & \longleftarrow & \cdots
\end{array}
$$

commute. Similarly, we have the abelian category $\mathbf{cCh}(\mathcal{A})$ of cochains in $\mathcal{A}$ in which the morphisms $f^\bullet : A^\bullet \to B^\bullet$ satisfies:

$$d_i \circ f_i = f_{i+1} \circ d_i$$

Given a morphism $f_\bullet : A_\bullet \to B_\bullet$ between two chains, clearly, for each i we have a natural morphism

$$f_i^* : H_i(A_\bullet) \to H_i(B_\bullet) \quad \text{and} \quad f_i^*(\overline{x}) \triangleq \overline{f_i(x)}$$

Similarly, given a morphism $f^\bullet : A^\bullet \to B^\bullet$ between two cochains, for each i we have a natural morphism

$$f_*^i : H^i(A^\bullet) \to H^i(B^\bullet) \quad \text{and} \quad f_*^i(\overline{x}) \triangleq \overline{f^i(x)}$$

Therefore, for each $i \in \mathbb{Z}$, *the i-th homology and cohomology are in nature functors*:

$$H_i : \mathbf{Ch}(\mathcal{A}) \to \mathcal{A} \quad \text{and} \quad H^i : \mathbf{cCh}(\mathcal{A}) \to \mathcal{A}$$

Note that sequences in $\mathbf{Ch}(\mathcal{A})$ and $\mathbf{cCh}(\mathcal{A})$ are exact if and only if it is exact componentwise.

Theorem 4.4.1. (Short exact sequence of complexes induce a long exact sequence of (co) homologies) Let $\mathcal{A}$ be an abelian category. Given a short exact sequence of chains

$$0 \longrightarrow A_\bullet \xrightarrow{f_\bullet} B_\bullet \xrightarrow{g_\bullet} C_\bullet \longrightarrow 0$$

in $\mathcal{A}$, we have a *canonical* long exact sequence of homologies:

$$\cdots \longrightarrow H_i(A_\bullet) \xrightarrow{f_i^*} H_i(B_\bullet) \xrightarrow{g_i^*} H_i(C_\bullet) \xrightarrow{\partial_i} H_{i-1}(A_\bullet) \longrightarrow \cdots$$

Dually, given a short exact sequence of cochains

$$0 \longrightarrow A^\bullet \xrightarrow{f^\bullet} B^\bullet \xrightarrow{g^\bullet} C^\bullet \longrightarrow 0$$

in $\mathcal{A}$, we have a *canonical* long exact sequence of cohomologies:

$$\cdots \longrightarrow H^i(A^\bullet) \xrightarrow{f_*^i} H^i(B^\bullet) \xrightarrow{g_*^i} H^i(C^\bullet) \xrightarrow{\partial^i} H^{i+1}(A^\bullet) \longrightarrow \cdots$$

Proof. Routine. The inducing of the boundary homomorphisms is done the same way as in snake lemma. ∎

Let $f_\bullet, g_\bullet : A_\bullet \to B_\bullet$ be two morphisms from one chain to another. A **chain homotopy** $s_\bullet : f_\bullet \to g_\bullet$ is a set of morphisms $s_i : A_i \to B_{i+1}$:

that make

$$f - g = d \circ s + s \circ d \tag{4.1}$$

136

Dually, given two morphisms $f^\bullet, g^\bullet : A^\bullet \to B^\bullet$ from one cochain to another, a **cochain homotopy** $s^\bullet : f^\bullet \to g^\bullet$ is a set of morphisms $s^i : A^i \to B^{i-1}$

$$
\begin{array}{ccccccccc}
\cdots & \xrightarrow{\ d\ } & A_{i-1} & \xrightarrow{\ d\ } & A_i & \xrightarrow{\ d\ } & A_{i+1} & \xrightarrow{\ d\ } & \cdots \\
& & \downarrow & \overset{s_i}{\nearrow} & \downarrow {\scriptstyle f_i - g_i} & \overset{s_{i+1}}{\nearrow} & \downarrow & & \\
\cdots & \xrightarrow{\ d\ } & B_{i-1} & \xrightarrow{\ d\ } & B_i & \xrightarrow{\ d\ } & B_{i+1} & \xrightarrow{\ d\ } & \cdots
\end{array}
$$

that satisfies equation 4.1. Clearly, chain and cochain homotopic are respectively equivalence relation in the Hom-sets of $\mathbf{Ch}(\mathcal{A})$ and $\mathbf{cCh}(\mathcal{A})$.

Theorem 4.4.2. (Basic property of homotopic) Let $\mathcal{A}$ be an abelian category and $f_\bullet, g_\bullet : A_\bullet \to B_\bullet$ be two morphisms from one chain in $\mathcal{A}$ to another. If they are homotopic, then

$$
f_i^* = g_i^* : H_i(A_\bullet) \to H_i(B_\bullet)
$$

Dually, given two morphisms $f^\bullet, g^\bullet : A^\bullet \to B^\bullet$ from one cochain in $\mathcal{A}$ to another. If they are homotopic, then

$$
f_*^i = g_*^i : H^i(A^\bullet) \to H^i(B^\bullet)
$$

Proof. Routine. ∎

4.5 Exact Functors

Equivalent Definition 4.5.1. (Exactness of functors) Let $\mathcal{A}$ and $\mathcal{B}$ be two abelian categories. An *additive* (both covariant and contravariant) functor $F : \mathcal{A} \to \mathcal{B}$ is said to be an **exact functor** if any of the followings hold true

(i) F maps exact sequence to exact sequence.

(ii) F maps short exact sequence to short exact sequence.

Proof. Because the proof for contravariant functors is dual to the proof for covariant functors, we only prove for covariant functors. (i) $\implies$ (ii) is clear, so we only have to prove (ii) $\implies$ (i). This is done by **breaking up a long exact sequence into multiple short exact sequences**. That is, given an exact sequence:

$$A \xrightarrow{f} B \xrightarrow{g} C$$

in $\mathcal{A}$, we construct a commutative diagram:
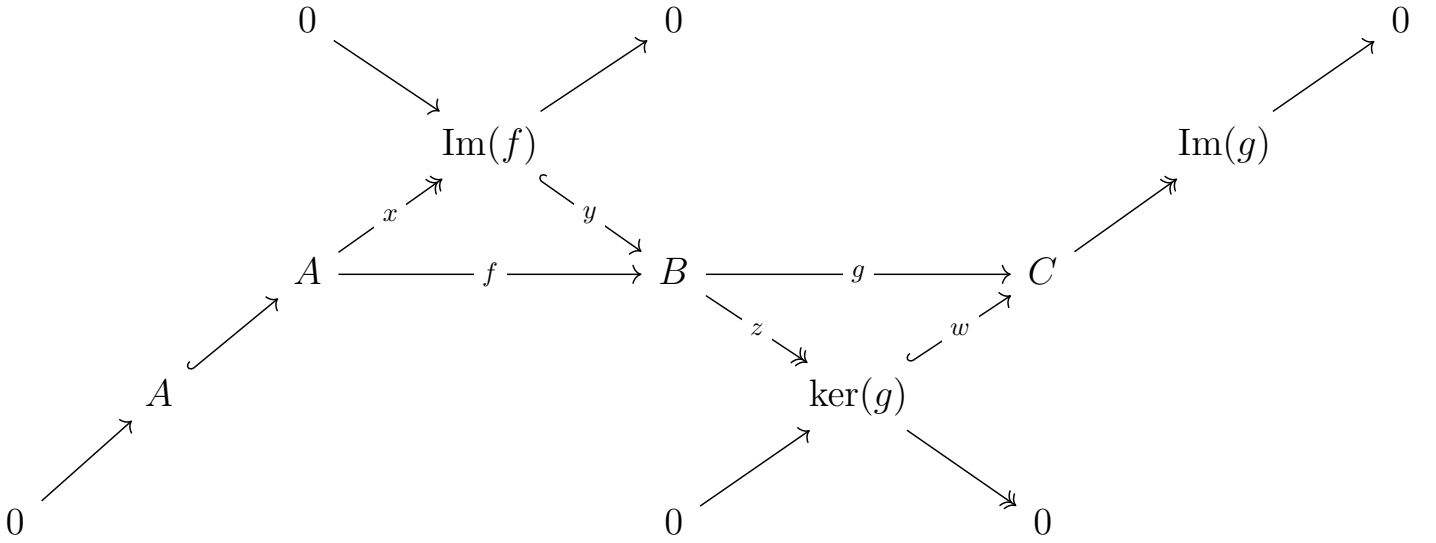
Now, because F preserves short exact sequence, we know $F(x)$ is surjective, so from $F(f) = F(y \circ x) = F(y) \circ F(x)$, we know $\operatorname{Im}(F(f)) = \operatorname{Im}(F(y))$. Similarly, we can show $\ker(F(g)) = \ker(F(z))$. Then because F preserves the middle short exact sequence, we have

$$\operatorname{Im}(F(f)) = \operatorname{Im}(F(y)) = \ker(F(z)) = \ker(F(g))$$

as desired. ∎

Equivalent Definition 4.5.2. (Left and right exactness of functors) Let $\mathcal{A}, \mathcal{B}$ be two abelian categories. An additive covariant functor $F : \mathcal{A} \to \mathcal{B}$ is said to be **right exact** if any of the followings hold true

(i) $A \longrightarrow B \twoheadrightarrow C \longrightarrow 0$ is exact $\implies F(A) \longrightarrow F(B) \twoheadrightarrow F(C) \longrightarrow 0$ is exact.

(ii) $0 \longrightarrow A \hookrightarrow B \twoheadrightarrow C \longrightarrow 0$ is exact $\implies F(A) \longrightarrow F(B) \twoheadrightarrow F(C) \longrightarrow 0$ is exact.

Also, $F : \mathcal{A} \to \mathcal{B}$ is said to be **left exact** if any of the followings hold true

(i) $0 \longrightarrow A \hookrightarrow B \longrightarrow C$ is exact $\implies 0 \longrightarrow F(A) \hookrightarrow F(B) \longrightarrow F(C)$ is exact.

(ii) $0 \longrightarrow A \hookrightarrow B \twoheadrightarrow C \longrightarrow 0$ is exact $\implies 0 \longrightarrow F(A) \hookrightarrow F(B) \longrightarrow F(C)$ is exact.

An additive contravariant functor $G : \mathcal{A} \to \mathcal{B}$ is said to be **right exact** if any of the followings hold true

(i) $0 \longrightarrow A \hookrightarrow B \longrightarrow C$ is exact $\implies G(C) \longrightarrow G(B) \twoheadrightarrow G(A) \longrightarrow 0$ is exact.

(ii) $0 \longrightarrow A \hookrightarrow B \twoheadrightarrow C \longrightarrow 0$ is exact $\implies G(C) \longrightarrow G(B) \twoheadrightarrow G(A) \longrightarrow 0$ is exact.

Also, $G : \mathcal{A} \to \mathcal{B}$ is said to be **left exact** if any of the followings hold true

(i) $A \longrightarrow B \twoheadrightarrow C \longrightarrow 0$ is exact $\implies 0 \longrightarrow G(C) \hookrightarrow G(B) \longrightarrow G(A)$ is exact.

(ii) $0 \longrightarrow A \hookrightarrow B \twoheadrightarrow C \longrightarrow 0$ is exact $\implies 0 \longrightarrow G(C) \hookrightarrow G(B) \longrightarrow G(A)$ is exact.

Proof. Routine. See this MSE post. ∎

Let $\mathcal{A}$ be an abelian category. Clearly, for all $N \in \mathcal{A}$ we have an additive *covariant* functor $\mathrm{Hom}(N, -) : \mathcal{A} \to \mathbf{Ab}$ defined by

$$A \mapsto \mathrm{Hom}(N, A) \quad \text{and} \quad g \xmapsto{F(f)} f \circ g$$

and an additive *contravariant* functor $\mathrm{Hom}(-, N) : \mathcal{A} \to \mathbf{Ab}$ defined by

$$A \mapsto \mathrm{Hom}(A, N) \quad \text{and} \quad g \xmapsto{G(f)} g \circ f$$

The memorization here is that the Hom is covariant in the second variable and contravariant in the first variable.

Theorem 4.5.3. (Both Hom functors are left exact) Let $\mathcal{A}$ be an abelian category. Then

(i) The sequence:

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

in $\mathcal{A}$ is exact $\iff$ For all $N \in \mathcal{A}$, the sequence:

$$0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{G(v)} \mathrm{Hom}(M, N) \xrightarrow{G(u)} \mathrm{Hom}(M', N)$$

in $\mathbf{Ab}$ is exact, where G is the contravariant functor $\mathrm{Hom}(-, N) : \mathcal{A} \to \mathbf{Ab}$.

(ii) The sequence:

$$0 \longrightarrow M' \overset{u}{\lhook\joinrel\longrightarrow} M \overset{v}{\longrightarrow} M''$$

in $\mathcal{A}$ is exact $\iff$ For all $N \in \mathcal{A}$, the sequence:

$$0 \longrightarrow \mathrm{Hom}(N, M') \overset{F(u)}{\longrightarrow} \mathrm{Hom}(N, M) \overset{F(v)}{\longrightarrow} \mathrm{Hom}(N, M'')$$

in $\mathbf{Ab}$ is exact, where F is the covariant functor $\mathrm{Hom}(N, -) : \mathcal{A} \to \mathbf{Ab}$.

Proof. Since the two proofs are dual to each other, we only prove for the contravariant functor G. The direction ($\implies$) is to say that G is left exact. We first prove this direction. The fact that functors preserve chain complex is clear, so we only have to prove

$$\ker(G(v)) \leq 0 \quad \text{and} \quad \ker(G(u)) \leq \mathrm{Im}(G(v))$$

Let $g \in \ker(G(v))$. It then follows from surjectivity of v and $g \circ v = G(v)(g) = 0$ that $g = 0$. Let $f \in \ker(G(u))$. Because $f \circ u = 0$, we know $\ker(f) \leq \mathrm{Im}(u) = \ker(v)$. This then by universal property induces a unique morphism $\widetilde{f} : M'' \to N$ that makes $f = G(v)(\widetilde{f})$. (done)

($\impliedby$): To prove $v \circ u = 0$, one set $N \triangleq M''$ and consider $\mathbf{id}_{M''}$. It remains to prove

$$\pi : M'' \twoheadrightarrow \mathrm{Coker}(v) \text{ is zero in } \mathrm{Hom}(M'', \mathrm{Coker}(v)) \quad \text{and} \quad \ker(v) \leq \mathrm{Im}(u)$$

For the first statement, set $N \triangleq \mathrm{Coker}(v)$. Because $G(v)(\pi) = \pi \circ v = 0$ by definition, we see $\pi \in \ker(G(v))$, which implies $\pi = 0$. For the second statement, set $N \triangleq \mathrm{Coker}(u)$ and let $p : M \twoheadrightarrow \mathrm{Coker}(u)$ be the canonical morphism. Because $\ker(p) = \mathrm{Im}(u)$, we only have to prove $\ker(v) \leq \ker(p)$. Now, since $p \in \ker(G(u)) = \mathrm{Im}(G(v))$, we know $p = \psi \circ v$, which implies $\ker(v) \leq \ker(p)$. (done) ∎

4.6 Resolutions

Let $\mathcal{C}$ be a category. We say $I \in \mathcal{C}$ is an **injective object** if for all monomorphism $m : M \hookrightarrow X$ and morphism $f : M \to I$, there exists a unique morphism $\widetilde{f} : X \to I$ that makes the diagram:

$$
\begin{array}{ccc}
M & \xrightarrow{\ \ m\ \ } & X \\
 & {}_{f}\searrow & \ \ \Big\downarrow{\widetilde{f}} \\
 & & I
\end{array}
$$

commutes. We say $P \in \mathcal{C}$ is a **projective object** if for all epimorphism $e : E \twoheadrightarrow X$ and morphism $f : P \to X$ there exists a unique morphism $\widetilde{f} : P \to E$ that makes the diagram:

$$
\begin{array}{ccc}
X & \xleftarrow{\ \ f\ \ } & P \\
\ \ \nwarrow{}_{e} & & \Big\downarrow{\widetilde{f}} \\
 & & E
\end{array}
$$

commutes. In other words, every morphism to an injective object factors through every monomorphism from its source, and every morphism from a projective object factors through every epimorphism to its target.

Equivalent Definition 4.6.1. (Injective and projective objects in abelian categories) Let $\mathcal{A}$ be an abelian category and $I, P \in \mathcal{A}$. Then the followings are equivalent:

(i) I is an injective object.

(ii) The contravariant functor $\mathrm{Hom}(-, I) : \mathcal{A} \to \mathbf{Ab}$ is exact.

(iii) Every short exact sequence of the form

$$
0 \longrightarrow I \hookrightarrow M \twoheadrightarrow M'' \longrightarrow 0
$$

splits.

Also, the followings are equivalent:

(i) P is a projective object.

(ii) The covariant functor $\mathrm{Hom}(P, -) : \mathcal{A} \to \mathbf{Ab}$ is exact.

(iii) Every short sequence of the form

$$0 \to M' \lhook\joinrel\longrightarrow M \longrightarrow\mkern-18mu\rightarrow P \longrightarrow 0$$

splits.

Proof. Because the proof for projective object is dual to the proof for injective object, we only prove for injective object.

(i) $\implies$ (ii): Because $G \triangleq \mathrm{Hom}(-, I) : \mathcal{A} \to \mathbf{Ab}$ is left exact, we only have to prove that for injective $u : M' \to M$, the morphism $G(u) : \mathrm{Hom}(M, I) \to \mathrm{Hom}(M', I)$ is surjective. Let $f \in \mathrm{Hom}(M', I)$. It then follows from universal property of injective object that there exists some (unique) $\widetilde{f} : M \to I$ that makes

$$f = u \circ \widetilde{f} = G(u)(\widetilde{f})$$

(ii) $\implies$ (iii): Denote the injective morphism by $m : I \to M$. The proof then follows from noting that because $G(m) : \mathrm{Hom}(M, I) \to \mathrm{Hom}(I, I)$ is surjective, there exists some $r : \mathrm{Hom}(M, I)$ that makes the sequence left splits:

$$\mathbf{id}_I = G(m)(r) = r \circ m$$

(iii) $\implies$ (i): Clearly, given the diagram:

we may form their pushout:

where g can be easily checked to be injective from the construction of pushouts in abelian category. Then from premise, there exists some $h : X +_M I \to I$ that makes $h \circ g = \mathbf{id}_I$. We now see that $h \circ j$ is the morphism we are looking for:

$$h \circ j \circ m = h \circ g \circ f = \mathbf{id}_I \circ f = f$$

$\blacksquare$

Theorem 4.6.2. (Projective objects are closed under coproduct and injective objects are closed under product) Let $\mathcal{C}$ be a category.

(i) If *possibly infinite* $A_i \in \mathcal{C}$ are projective and coproduct $\bigoplus A_i$ exists, then $\bigoplus A_i$ is projective.

(ii) If *possibly infinite* $A_i \in \mathcal{C}$ are injective and product $\prod A_i$ exists, then $\prod A_i$ is injective.

Proof. Routine. ∎

Let $\mathcal{C}$ be a category. We say $\mathcal{C}$ **has enough injective** if for all $X \in \mathcal{C}$ there exists a monomorphism $X \hookrightarrow I$ from X to an injective object $I \in \mathcal{C}$, and we say $\mathcal{C}$ **has enough projective** if for all $X \in \mathcal{C}$ there exists an epimorphism $P \twoheadrightarrow X$ from a projective object $P \in \mathcal{C}$ to X. Given an abelian category $\mathcal{A}$ with enough injective, for each $X \in \mathcal{A}$, we may form an exact cochain:

called **an injective resolution of** X. Dually, given an abelian category $\mathcal{A}$ with enough projective, for each $X \in \mathcal{A}$, we may form an exact chain:

called **a projective resolution of** X.

Theorem 4.6.3. (Morphisms induce (co) chain morphism unique up to homotopy) Let $\mathcal{A}$ be an abelian category. Given two injective resolutions $X \to I^\bullet$ and $Y \to Q^\bullet$ in $\mathcal{A}$ and a morphism $f : X \to Y$, there exists a cochain morphism $f^\bullet : I^\bullet \to Q^\bullet$ that makes $f^{-1} = f$, unique up to homotopy. Dually, given two projective resolution $X \leftarrow P_\bullet$ and $Y \leftarrow Q_\bullet$ in $\mathcal{A}$ and a morphism $f : X \to Y$, there exists a chain morphism $f_\bullet : P_\bullet \to Q_\bullet$ that makes $f_{-1} = f$, unique up to homotopy.

Proof. Because the two proofs are dual to each other, we only prove for injective resolutions.

We first prove the existence, so we start with the diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & X & \xrightarrow{\;d^{-1}\;} & I^0 & \xrightarrow{\;d^0\;} & I^1 & \longrightarrow & \cdots \\
& & \big\downarrow{\scriptstyle f} & & & & & & \\
0 & \longrightarrow & Y & \xrightarrow{\;\epsilon^{-1}\;} & Q^0 & \xrightarrow{\;\epsilon^0\;} & Q^1 & \longrightarrow & \cdots
\end{array}
$$

Because $d^{-1} : X \hookrightarrow I^0$ is by definition injective, we may construct f using the universal property of I^0, giving us a commutative diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & X & \xrightarrow{\;d^{-1}\;} & I^0 & \xrightarrow{\;d^0\;} & I^1 & \longrightarrow & \cdots \\
& & \big\downarrow{\scriptstyle f} & & \big\downarrow{\scriptstyle f^0} & & & & \\
0 & \longrightarrow & Y & \xrightarrow{\;\epsilon^{-1}\;} & Q^0 & \xrightarrow{\;\epsilon^0\;} & Q^1 & \longrightarrow & \cdots
\end{array}
$$

Then because

$$
\epsilon^0 \circ f^0 \circ d^{-1} = \epsilon^0 \circ \epsilon^{-1} \circ f = 0
$$

By universal property of $\mathrm{Coker}(d^{-1})$, there exist a morphism $u : \mathrm{Coker}(d^-1) \to Q^0$ that makes the diagram:

commutes. The construction of f^1 then follows from universal property of I^1 :

The construction of f^n for $n \geq 2$ are similar to that of f^1. We now prove its uniqueness up to homotopic. Clearly, it suffices to show that given $f \triangleq 0$, the induced chain morphism $f^\bullet$ is homotopic to $0^\bullet$. In other words, we only have to construct $s^i : I^i \to Q^{i-1}$ to satisfies

$$0 = s \circ d + d \circ s$$

Clearly, $s^i \triangleq 0$ for $i \leq 0$ satisfies

$$0^i = s \circ d + d \circ s, \quad \text{for all } i \leq -1$$

We now construct s^1. Because

$$f^0 \circ d^{-1} = \epsilon^{-1} \circ f = 0$$

By universal property of $\operatorname{Coker}(d^{-1})$ induces a commutative diagram:

which by injectivity of I^1 induces a commutative diagram:

$$
\begin{array}{c}
X \\
\downarrow{\scriptstyle d^{-1}} \\
I^0 \\
\end{array}
$$

Because $s^0 = 0$, such s^1 clearly is what we are looking for. Let

$$h^1 \triangleq f^1 - \epsilon^0 \circ s^1 \in \mathrm{Hom}(I^1, Q^1)$$

We are then require to construct $s^2 : I^2 \to Q^1$ that makes $h^1 = s^2 \circ d^1$. First, because $f^0 = s^1 \circ d^0$, we have

$$
\begin{aligned}
h^1 \circ d^0 &= f^1 \circ d^0 - \epsilon^0 \circ s^1 \circ d^0 \\
&= \epsilon^0 \circ f^0 - \epsilon^0 \circ s^1 \circ d^0 = \epsilon^0 \circ (f^0 - s^1 \circ d^0) = 0
\end{aligned}
$$

This then by universal property of $\mathrm{Coker}(d^0)$ induces a commutative diagram:

$$
\begin{array}{c}
\mathrm{Coker}(d^0) \\
I^0 \xrightarrow{\ d^0\ } I^1 \\
Q^1
\end{array}
$$

which by injectivity of I^1 induces a commutative diagram:

as desired. The construction of s^n for $n \geq 3$ is similar to that of s^2, so we win. ∎

Theorem 4.6.4. (Horseshoe Lemma) Let $\mathcal{A}$ be an abelian category with enough projective and

$$0 \longrightarrow A' \overset{f}{\longrightarrow} A \overset{g}{\longrightarrow} A'' \longrightarrow 0$$

be an exact sequence in $\mathcal{A}$. Then for all projective resolutions $P'_\bullet \to A'$ and $P''_\bullet \to A''$ for A' and A'', there exists a projective resolution $P_\bullet \to A$ and a short exact sequence

$$0 \longrightarrow (P'_\bullet \to A') \longrightarrow (P_\bullet \to A) \longrightarrow (P''_\bullet \to A) \longrightarrow 0$$

in $\mathbf{Ch}(\mathcal{A})$. More precisely, we can construct a projective resolution of A by

$$P_i \triangleq P'_i \oplus P''_i, \quad \text{for all } i$$

with the natural morphisms $P'_i \longrightarrow P_i \longrightarrow P''_i$ respectively forming a lift of f and g. In

other words, the natural morphisms give rise to a commutative diagram:

$$
\begin{array}{ccccccc}
& & 0 & & 0 & & 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
\cdots \longrightarrow & P_1' & \longrightarrow & P_0' & \longrightarrow\!\!\!\!\twoheadrightarrow & A' & \longrightarrow 0 \\
& \big\uparrow & & \big\uparrow & & \big\uparrow f & \\
\cdots \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow 0 \\
& \big\downarrow & & \big\downarrow & & \big\downarrow g & \\
\cdots \longrightarrow & P_1'' & \longrightarrow & P_0'' & \longrightarrow & A'' & \longrightarrow 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
& 0 & & 0 & & 0 &
\end{array}
$$

Dually, the same statement holds for abelian categories with enough injective.

Proof. Let $P_i \triangleq P_i' \oplus P_i''$. We start with the diagram:

$$
\begin{array}{ccc}
P_0' & \overset{\epsilon'}{\longrightarrow\!\!\!\!\twoheadrightarrow} & A' \longrightarrow 0 \\
\big\uparrow i_0 & & \big\uparrow f \\
P_0 & & A \longrightarrow 0 \\
\big\downarrow \pi_0 & & \big\downarrow g \\
P_0'' & \underset{\epsilon''}{\longrightarrow\!\!\!\!\twoheadrightarrow} & A'' \longrightarrow 0
\end{array}
$$

Because g is surjective, projectivity of P_0'' gives us a commutative diagram:

$$
\begin{array}{ccccc}
P_0' & \xrightarrow{\;\epsilon'\;} & A' & \longrightarrow & 0 \\
\downarrow{\scriptstyle i_0} & & \downarrow{\scriptstyle f} & & \\
P_0 & & A & \longrightarrow & 0 \\
\downarrow{\scriptstyle \pi_0} & \nearrow{\scriptstyle t} & \downarrow{\scriptstyle g} & & \\
P_0'' & \xrightarrow{\;\epsilon''\;} & A'' & \longrightarrow & 0
\end{array}
$$

Because $P_0 = P_0' \oplus P_0$, universal property of coproduct gives us a commutative diagram:

$$
\begin{array}{ccccc}
P_0' & \xrightarrow{\;\epsilon'\;} & A' & \longrightarrow & 0 \\
\downarrow{\scriptstyle i_0} & & \downarrow{\scriptstyle f} & & \\
P_0 & \xdashrightarrow{\;\epsilon \triangleq t + f\circ\epsilon'\;} & A & \longrightarrow & 0 \\
\downarrow{\scriptstyle \pi_0} & \nearrow{\scriptstyle t} & \downarrow{\scriptstyle g} & & \\
P_0'' & \xrightarrow{\;\epsilon''\;} & A'' & \longrightarrow & 0
\end{array}
$$

Note that the reason we have $\epsilon = t \circ \pi_0$ is that by definition we have

$$t \circ \pi_0 \circ i = t = \epsilon \circ i$$

where $i : P_0'' \hookrightarrow P_0$ is the canonical morphism for coproduct, which is a monomorphism.
Applying snake lemma on the two columns, we have a commutative diagram:

$$
\begin{array}{ccccccccc}
P_1' & \twoheadrightarrow & \ker(\epsilon') & \longrightarrow & P_0' & \xrightarrow{\;\epsilon'\;} & A' & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle i_0} & & \downarrow{\scriptstyle f} & & \\
P_1 & & \ker(\epsilon) & \longrightarrow & P_0 & \xtwoheadrightarrow{\;\epsilon\;} & A & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle \pi_0} & \nearrow{\scriptstyle t} & \downarrow{\scriptstyle g} & & \\
P_1'' & \twoheadrightarrow & \ker(\epsilon'') & \longrightarrow & P_0'' & \xtwoheadrightarrow{\;\epsilon''\;} & A'' & \longrightarrow & 0
\end{array}
$$

in which ϵ is surjective because in the application of snake lemma we have a exact sequence

$$\text{Coker}(\epsilon') = 0 \longrightarrow \text{Coker}(\epsilon) \longrightarrow\!\!\!\!\!\rightarrow \text{Coker}(\epsilon'') = 0$$

which implies $\text{Coker}(\epsilon) = 0$. Lastly, the proof follows from noting that the rest of construction can be done the same way we construct ϵ. ∎

4.7 δ-Functors

Let $\mathcal{A}$ and $\mathcal{B}$ be two abelian categories. A **homological covariant δ-functor from $\mathcal{A}$ to $\mathcal{B}$** consists of the followings datum

(i) a sequence of additive functors $F_i : \mathcal{A} \to \mathcal{B}$.

(ii) For every short exact sequence in $\mathcal{A}$:

$$0 \longrightarrow A \xrightarrow{\;f\;} B \xrightarrow{\;g\;} C \longrightarrow 0$$

a sequence of morphisms $\delta_i : F_i(C) \to F_{i-1}(A)$ that gives rise to a long exact sequence in $\mathcal{A}$:

$$\cdots \longrightarrow F_i(A) \xrightarrow{F_i(f)} F_i(B) \xrightarrow{F_i(g)} F_i(C) \xrightarrow{\delta_i} F_{i-1}(A) \longrightarrow \cdots$$

natural in the sense that for each morphism of short exact sequences in $\mathcal{A}$:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
  &   & \downarrow &   & \downarrow &   & \downarrow &   &   \\
0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0
\end{array}
$$

we have a morphism of long exact sequences in $\mathcal{A}$:

$$
\begin{array}{ccccccccc}
\cdots \longrightarrow & F_i(A) & \longrightarrow & F_i(B) & \longrightarrow & F_i(C) & \longrightarrow & F_{i-1}(A) & \longrightarrow \cdots \\
 & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\
\cdots \longrightarrow & F_i(A') & \longrightarrow & F_i(B') & \longrightarrow & F_i(C') & \longrightarrow & F_{i-1}(A') & \longrightarrow \cdots
\end{array}
$$

Dually, a **cohomological covariant δ-functor from $\mathcal{A}$ to $\mathcal{B}$** consists of:

(i) a sequence of additive functors $F_i : \mathcal{A} \to \mathcal{B}$.

(ii) For every short exact sequence in $\mathcal{A}$:

$$0 \longrightarrow A \xrightarrow{\;f\;} B \xrightarrow{\;g\;} C \longrightarrow 0$$

a sequence of morphisms $\delta_i : F_i(C) \to F_{i+1}(A)$ that gives rises to a long exact sequence in $\mathcal{A}$:

$$\cdots \longrightarrow F_i(A) \xrightarrow{F_i(f)} F_i(B) \xrightarrow{F_i(g)} F_i(C) \xrightarrow{\delta_i} F_{i+1}(A) \longrightarrow \cdots$$

natural in the sense that for each morphism of short exact sequences in $\mathcal{A}$:

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$
$$\downarrow \qquad\quad \downarrow \qquad\quad \downarrow$$
$$0 \longrightarrow A' \longrightarrow B' \longrightarrow C' \longrightarrow 0$$

we have a morphism of long exact sequences in $\mathcal{A}$:

$$\cdots \longrightarrow F_i(A) \longrightarrow F_i(B) \longrightarrow F_i(C) \longrightarrow F_{i+1}(A) \longrightarrow \cdots$$
$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$
$$\cdots \longrightarrow F_i(A') \longrightarrow F_i(B') \longrightarrow F_i(C') \longrightarrow F_{i+1}(A') \longrightarrow \cdots$$

Clearly, we have the **category of homological covariant δ-functors from $\mathcal{A}$ to $\mathcal{B}$**, in which the morphisms from (F_i, δ_i) to (G_i, δ_i') is a family of natural transformation $\eta_i : F_i \rightsquigarrow G_i$ such that for all short exact sequence in $\mathcal{A}$:

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

the diagram:

$$\begin{array}{ccc} F_i(C) & \xrightarrow{\ \ \delta_i\ \ } & F_{i-1}(A) \\ \downarrow{\scriptstyle (\eta_i)_C} & & \downarrow{\scriptstyle (\eta_{i-1})_A} \\ G_i(C) & \xrightarrow{\ \ \delta_i'\ \ } & G_{i-1}(A) \end{array}$$

commutes. A homological covariant δ-functor (F_i, δ_i) from $\mathcal{A}$ to $\mathcal{B}$ is then said to be **universal** if given

(i) any δ-functor (G_i, δ_i')

(ii) any natural transformation $\eta_0 : F_0 \rightsquigarrow G_0$ from F_0 to G_0

there exists a unique sequence of natural transformations $\eta_i : F_i \rightsquigarrow G_i$ that gives us a morphism $\eta : (G_i, \delta_i') \to (F_i, \delta_i)$ of homological covariant δ-functors.

Clearly, universal homological covariant δ-functors from $\mathcal{A}$ to $\mathcal{B}$ are unique up to the 0-th functor in the sense that given any two universal homological covariant δ-functor (F_i, δ_i) and (G_i, δ_i') from $\mathcal{A}$ to $\mathcal{B}$, if F_0 and $G_0 : \mathcal{A} \to \mathcal{B}$ are isomorphic, then F_i and G_i are all isomorphic.[1]

---

[1]To prove such, just induce the two natural transformation $F_0 \rightsquigarrow G_0$ and $G_0 \rightsquigarrow F_0$ inverse to each other to each F_i and G_i.

4.8 Derived Functors

Abstract

In this section, we show that derived functors are well-defined and they are universal δ-functors.

Let $F : \mathcal{A} \to \mathcal{B}$ be a *covariant additive* functor from an abelian category $\mathcal{A}$ with enough injective to an arbitrary abelian category $\mathcal{B}$. Let $X \in \mathcal{A}$ and $X \to I^\bullet$ be an injective resolution. Truncate the $F(X)$ in its image, we have a cochain:

$$0 \longrightarrow F(I^0) \longrightarrow F(I^1) \longrightarrow \cdots$$

For now we denote

$$R^i F(X) \triangleq H^i(F(I^\bullet))$$

Theorem 4.8.1. ($R^i F(X)$ **is well-defined**) Let $\mathcal{A}$ be an abelian category with enough injective and $\mathcal{B}$ an abelian category. Let $F : \mathcal{A} \to \mathcal{B}$ be a covariant additive functor. Given two injective resolutions $X \to I^\bullet$ and $X \to Q^\bullet$ of $X \in \mathcal{A}$, for each i there exists a *canonical* isomorphism

$$H^i(F(I^\bullet)) \cong H^i(F(Q^\bullet)), \quad \text{in } \mathcal{B}$$

Proof. Denote the two chain morphisms induced by $\mathbf{id}_X$ as:

$$f^\bullet \triangleq \mathbf{id}_X^\bullet : I^\bullet \to Q^\bullet \quad \text{and} \quad g^\bullet \triangleq \mathbf{id}_X^\bullet : Q^\bullet \to I^\bullet$$

We are required to check that $F(f^i)_* : H^i(F(I^\bullet)) \to H^i(F(Q^\bullet))$ and $F(g^i)_* : H^i(F(Q^\bullet)) \to H^i(F(I^\bullet))$ are inverse to each other. WLOG, we only show that

$$F(g^i)_* \circ F(f^i)_* = \mathbf{id}_{H^i(F(I^\bullet))}$$

By definition, we have

$$F(g^i)_* \circ F(f^i)_* = \left(F(g^i) \circ F(f^i)\right)_* = F(g^i \circ f^i)_*$$

Now, since, as one should check, both $g^i \circ f^i$ and $\mathbf{id}_{I^i}$ are induced by

$$
\begin{array}{ccccc}
X & \longrightarrow & I^0 & \longrightarrow & I^1 \\
\Big| & & & & \\
\mathbf{id}_X & & & & \\
\Big\downarrow & & & & \\
X & \longrightarrow & I^0 & \longrightarrow & I^1
\end{array}
$$

153

We know they are homotopic. Then because F is additive, as one should check, $F((g^i \circ f^i))$ and $F(\mathbf{id}_{I^i}) = \mathbf{id}_{F(I^i)}$ are homotopic. This then implies $F((g \circ f)^i)_* = \mathbf{id}_{H^i(F(I^\bullet))}$. ∎

In conclusion, we have a well-defined functor $R^i F : \mathcal{A} \to \mathcal{B}$ called the i**-th right derived functor** of the *covariant additive* functor $F : \mathcal{A} \to \mathcal{B}$ from an abelian category with enough injective, in which the morphisms $f : X \to Y$ in $\mathcal{A}$ are mapped to

$$R^i F(f) \triangleq F(f^i)_* : H^i(F(I^\bullet)) \to H^i(F(Q^\bullet))$$

where f_i is canonically induced by f.

Usually, we talk about right derived functor $R^i F$ when F is left-exact. This is because if F is left-exact, then the sequence

$$0 \longrightarrow F(X) \longrightarrow F(I^0) \longrightarrow F(I^1), \quad \text{in } \mathcal{B}$$

is exact, which implies

$$R^0 F(X) = F(X) \quad \text{and} \quad R^0 F = F$$

Moreover, given a short exact sequence $A \to B \to C$ in $\mathcal{A}$ with injective resolutions $A \to I_A^\bullet$ and $C \to I_C^\bullet$, by horseshoe lemma, we have a short exact sequence

$$0 \longrightarrow I_A^\bullet \longrightarrow I_A^\bullet \oplus I_C^\bullet \longrightarrow I_C^\bullet \longrightarrow 0, \quad \text{in } \mathbf{cCh}(\mathcal{A})$$

in which $I_B^\bullet \triangleq I_A^\bullet \oplus I_C^\bullet$ form an injective resolution of B. Then because additive functors preserve biproducts, we have a short exact sequence

$$0 \longrightarrow F(I_A^\bullet) \longrightarrow F(I_B^\bullet) \longrightarrow F(I_C^\bullet) \longrightarrow 0, \quad \text{in } \mathbf{cCh}(\mathcal{B})$$

Then because short exact sequence of cochains induces a *canonical* long exact sequence of cohomologies, we have a *canonical* long exact sequence:

$$0 \to F(A) \to F(B) \to F(C) \to R^1 F(A) \to R^1 F(B) \to R^1 F(C) \to \cdots$$

in $\mathcal{B}$.

Dually, given an *covariant additive* functor $F : \mathcal{A} \to \mathcal{B}$ from an abelian category *with enough projective*, we have a well-defined functor $L_i F : \mathcal{A} \to \mathcal{B}$ called the i**-th left derived functor** of $F : \mathcal{A} \to \mathcal{B}$

$$L_i F(X) \triangleq H_i(F(P_\bullet)) \quad \text{and} \quad L_i F(f) \triangleq F(f_i)_*$$

whilst, if $F : \mathcal{A} \to \mathcal{B}$ is right-exact, then we have

$$L_0 F(X) \cong F(X) \quad \text{and} \quad L_0 F = F$$

and a *canonical* long exact sequence:

$$\cdots \to L_1 F(A) \to L_1 F(B) \to L_1 F(C) \to F(A) \to F(B) \to F(C) \to 0$$

154

Theorem 4.8.2. (Derived functors on injective and projective objects) Let F : $\mathcal{A} \to \mathcal{B}$ be a covariant additive functor between two abelian categories. If $\mathcal{A}$ has enough injective and F is left-exact, then for all injective object $I \in \mathcal{A}$, we have

$$R^n F(I) = 0, \quad \text{for all } n \geq 1$$

Dually, if $\mathcal{A}$ has enough projective and F is right-exact, then for all projective object $P \in \mathcal{A}$, we have

$$L_n F(P) = 0, \quad \text{for all } n \geq 1$$

Proof. The statement for injective object follows from resoluting I by

$$I \longrightarrow I \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

where the first arrow is an isomorphism. The statement for projective objects can be proved similarly. ∎

Theorem 4.8.3. (Derived functors are δ-functors) Let $F : \mathcal{A} \to \mathcal{B}$ be a covariant additive functor. If $\mathcal{A}$ has enough injective, then $R^i F$ forms a homological covariant δ-functor. Dually, if $\mathcal{A}$ has enough projective, then $L_i F$ forms a cohomological covariant δ-functor.

Proof. The proofs are dual to each other. Note that even though we have already shown that right derived functors induces long exact sequences from short exact sequence, we haven't shown that such inducing is natural to conclude that $R^i F$ forms a δ-functor. The proof of naturalaity boils down to a long and routine computation, in which one, necessarily, use horseshoe lemma to construct a manageable injective resolution of B for us to conduct the computation. See Theorem 3.3.5 of this copy of the text *Homological algebra* by Romyar Sharifi. ∎

Theorem 4.8.4. (Characterization of universal δ-functor from abelian categories with enough injective or projective) Let $F^i : \mathcal{A} \to \mathcal{B}$ be a homological δ-functor from one abelian category to another. If $\mathcal{A}$ has enough injective and $F^n(I) = 0$ for all injective object $I \in \mathcal{A}$ and $n \geq 1$, then $F^i : \mathcal{A} \to \mathcal{B}$ is universal. The dual statement also holds.

Proof. See Theorem 3.3.9 of this copy of the text *Homological algebra* by Romyar Sharifi. ∎

Now, since derived functors satisfy $R^n F(I) = 0$ for all $n \geq 1$, we see that they are indeed universal δ-functors.

4.9   Tor Functor

Let A and B be two rings, and M be an (A, B)-bimodule. Then we have a right-exact functor $N \otimes_A -$ from $\mathbf{Mod}_A$ to $\mathbf{Mod}_{(A,B)}$. The n-**th Tor functor** $\mathrm{Tor}_n^A(N, -)$ is then its n-th left derived functor. In other words, we write

$$\mathrm{Tor}_n^A(N, M) \triangleq H_n(N \otimes P_\bullet)$$

where $P_\bullet$ is a projective resolution of M.

Theorem 4.9.1. (Balancing of Tor functor) Let A be a ring and M and N be two A-modules. Then we have an isomorphism

$$\mathrm{Tor}_n^A(M, N) \cong \mathrm{Tor}_n^A(N, M)$$

for all $n \geq 0$.

Proof. There are supposedly two methods to prove this. One, which seems more down to earth, is to consider the double complex of their projective resolutions. See the first proof of Proposition 3.5.9 of this copy of the text *Homological algebra* by Romyar Sharifi or Theorem 2.7.2 of Weibel.

The other supposed "solution" is to show that $\mathrm{Tor}_n(-, N)$ also forms a universal δ-functor, as suggested by the second proof of Proposition 3.5.9 of this copy of the text *Homological algebra* by Romyar Sharifi and the comment in this MO post. However, I will make the remark that the second proof by Romyar seems skeptical to me, in that he didn't prove the naturalaity of $\mathrm{Tor}_n(-, N)$, whilst the rest seems fine. ∎

Equivalent Definition 4.9.2. (Flat modules) Let N be an A-module. We say N is **flat** if any of the followings hold true

(i) $- \otimes N$ is exact.

(ii) Restriction of $- \otimes N$ onto the category of finitely generated A-modules is exact.

(iii) $\mathrm{Tor}_n^A(N, M) = 0$ for all $n \geq 1$ and $M \in \mathbf{Mod}_A$.

(iv) $\mathrm{Tor}_1^A(N, M) = 0$ for all $M \in \mathbf{Mod}_A$.

(v) $\mathrm{Tor}_n^A(N, M) = 0$ for all $n \geq 1$ and finitely generated $M \in \mathbf{Mod}_A$

(vi) $\mathrm{Tor}_1^A(N, M) = 0$ for all finitely generated $M \in \mathbf{Mod}_A$.

In particular, the definitions that use tor functor implies that projective modules are flat.

Proof. (i) $\implies$ (iii) $\implies$ (iv) $\implies$ (i) and (iii) $\implies$ (v) $\implies$ (vi) $\implies$ (ii) are routine, and (i) $\implies$ (ii) is clear, so it only remains to prove (ii) $\implies$ (i). In particular, since tensor product is right exact, we only have to prove that given injective homomorphism $f : M' \hookrightarrow M$, where M' and M need not be finitely generated, the homomorphism $f \otimes 1 : M' \otimes N \to M \otimes N$ remains injective.

Let $u \in \ker(f \otimes 1)$. We are required to show $u = 0$. Write $u \triangleq \sum x_i' \otimes y_i$. Consider the submodule $M_0' \triangleq (x_1', \dots, x_n') \leq M'$ and $u_0 \triangleq \sum x_i' \otimes y_i \in M_0' \otimes N$. Because the natural homomorphism from $M_0' \otimes N$ to $M' \otimes N$ maps u_0 to u, we only have to prove $u_0 = 0$.

Now, because $u \in \ker(f \otimes 1)$, we know $\sum f(x_i') \otimes y_i = 0$ in $M \otimes N$. This implies the existence of some finitely generated submodule $M_0 \leq M$ that makes $f(x_i') \in M_0$ for all i and $\sum f(x_i') \otimes y_i = 0 \in M_0 \otimes N$.

Clearly, f maps M_0' into M_0, so we have the restriction maps $f|_{M_0'} : M_0' \hookrightarrow M_0$ (Note that the codomain was shrunk). Because $f|_{M_0'} \otimes 1 : M_0' \otimes N \to M_0 \otimes N$ maps u_0 to 0 by the last paragraph, and because both M_0' and M_0 are finitely generated by construction, by premise $u_0 = 0$, as desired. ∎

Theorem 4.9.3. (Identities for flat modules) Let A be a ring. Then

(i) Let M_i be a *possibly infinite* collection of A-modules. Then

$$\bigoplus M_i \text{ is flat} \quad \Longleftrightarrow \quad \text{All } M_i \text{ are flat}$$

(ii) A is a flat A-module.

(iii) $A[x]$ is a flat A-module.

(iv) If M and N are both flat A-modules, then $M \otimes N$ is also flat.

(v) If B is a flat A-algebra and N is a flat B-module, then N is flat as an A-module.

Proof. Note that (iii) is a corollary of (i) and (ii), since $A[x] \cong \bigoplus M_i$, where M_i is the sub A-module generated x^i, which is isomorphic to A as A-modules. The rest are proved the same way: We wish to show flatness by showing that tensor preserve injectivity, so we factors the tensored morphism into a composition a isomorphisms and a tensored morphism that is guaranteed injectivity via flatness of the objects we are given.

We prove the ($\impliedby$) direction of (i) as an example. Note that the proof of the converse is a simple observation that if one of M_i isn't flat, then clearly $f \otimes \mathbf{id}_{\bigoplus M_i}$ isn't injective.

Let $f : P' \hookrightarrow P$ be an injective A-module homomorphism. Universal property of coproduct gives us an A-module homomorphisms $\bigoplus f \otimes \mathbf{id}_{M_i} : \bigoplus (P' \otimes M_i) \to \bigoplus (P \otimes M_i)$ that maps $p' \otimes m_i$ to $f(p') \otimes m_i$. Because M_i are flat, we know $f \otimes \mathbf{id}_{M_i}$ are injective. This clearly implies $\bigoplus f \otimes \mathbf{id}_{M_i}$ is flat. The proof then follows from noting that we have a commutative diagram:

$$
\begin{array}{ccc}
P' \otimes \bigoplus M_i & \xrightarrow{\ f \otimes \mathbf{id}_{\bigoplus M_i}\ } & P \otimes \bigoplus M_i \\[2mm]
\Big\downarrow & & \Big\uparrow \\[2mm]
\bigoplus P' \otimes M_i & \xrightarrow[\ \bigoplus (f \otimes \mathbf{id}_{M_i})\ ]{} & \bigoplus P \otimes M_i
\end{array}
$$

where the columns are the natural isomorphisms:

$$
P' \otimes \bigoplus M_i \cong \bigoplus P' \otimes M_i \quad \text{and} \quad P \otimes \bigoplus M_i \cong \bigoplus P \otimes M_i
$$

Now, (ii) use the isomorphism $P \otimes A \cong P$, (iv) use the isomorphism $P \otimes (M \otimes N) \cong (P \otimes M) \otimes N$, and (v) use the isomorphisms:

$$
P \otimes_A N \cong P \otimes_A (B \otimes_B N) \cong (P \otimes_A B) \otimes_B N
$$

∎

Theorem 4.9.4. (Homological identity of flat modules) Let A be a ring. Given an exact sequence

$$
0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0
$$

of A-modules with N'' flat, we have

$$
N' \text{ is flat} \iff N \text{ is flat}
$$

Proof. This follows from noting that since N'' is flat, we have a short exact sequence:

$$
0 = \mathrm{Tor}_2(M, N'') \longrightarrow \mathrm{Tor}_1(M, N') \longrightarrow \mathrm{Tor}_1(M, N) \longrightarrow \mathrm{Tor}_1(M, N'') = 0
$$

∎

Theorem 4.9.5. (Homological identity of flat modules) Let A be a ring and N an A-module. Then

$$
N \text{ is flat} \iff \mathrm{Tor}_1(A/\mathfrak{a}, N) = 0, \quad \text{for all finitely generated } \mathfrak{a} \leq A
$$

Proof. Left to right follows from definition of flatness. We prove from right to left. We first show that:

$$\text{Tor}_1(A/\mathfrak{b}, N) = 0, \quad \text{for all } \mathfrak{b} \trianglelefteq A$$

By premise, for each finitely generated submodule $\mathfrak{a}_i$, we have a short exact sequence

$$0 \longrightarrow \mathfrak{a}_i \otimes N \longrightarrow A \otimes N \longrightarrow A/\mathfrak{a}_i \otimes N \longrightarrow 0$$

Because $\text{Tor}(N, -)$ is a δ-functor, for each inclusion $\mathfrak{a}_i \hookrightarrow \mathfrak{a}_j$ of finitely generated submodules of $\mathfrak{b}$, we have a morphism of short exact sequence

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{a}_i \otimes N & \longrightarrow & A \otimes N & \longrightarrow & A/\mathfrak{a}_i \otimes N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{a}_j \otimes N & \longrightarrow & A \otimes N & \longrightarrow & A/\mathfrak{a}_j \otimes N & \longrightarrow & 0
\end{array}
$$

This implies that we have a short exact sequence of directed system

$$0 \to (\mathfrak{a}_i \otimes N) \to (A \otimes N) \to (A/\mathfrak{a}_i \times N) \to 0$$

consisting of finitely generated submodules of $\mathfrak{b}$. Then because direct limit is an exact functor, this induces a short exact sequence consisting of their direct limit

$$0 \longrightarrow \varinjlim(\mathfrak{a}_i \otimes N) \longrightarrow \varinjlim(A \otimes N) \longrightarrow \varinjlim(A/\mathfrak{a}_i \otimes N) \longrightarrow 0$$

Then because direct limit commute with tensor product, we have a short exact sequence

$$0 \to \mathfrak{b} \otimes N \longrightarrow A \otimes N \longrightarrow A/\mathfrak{b} \otimes N \longrightarrow 0$$

The injectivity of $\mathfrak{b} \otimes N \to A \otimes N$ in this short exact sequence then implies $\text{Tor}_1(A/\mathfrak{b}, N) = 0$. (done)

We now prove that

$$\text{Tor}_1(M, N) = 0, \quad \text{for all finitely generated module } M$$

This is proved by induction on number of generators. Let $M \triangleq (x_1, \ldots, x_n)$ and denote $M_i \triangleq (x_1, \ldots, x_i)$ for all $0 \le i \le n$. The base case $i = 0$ is clear. Consider the function defined by

$$A \to M_n/M_{n-1}, \quad a \mapsto \overline{ax_n}$$

This gives us a short exact sequence

$$0 \longrightarrow M_{n-1} \longrightarrow M_n \longrightarrow A/\ker(f) \longrightarrow 0$$

Then by inductive hypothesis and the earlier result, we have an exact sequence

$$0 = \text{Tor}_1(M_{n-1}, N) \longrightarrow \text{Tor}_1(M_n, N) \longrightarrow \text{Tor}(A/\ker(f), N) = 0$$
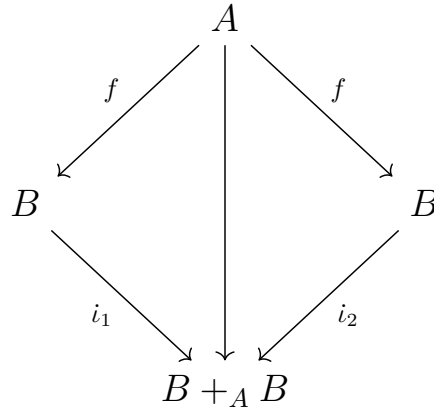
which implies $\text{Tor}_1(M_n, N) = 0$.

$\blacksquare$

4.10   more constructions in general categories

the **kernel** and **cokernel** of a morphism $f : A \to B$ is then defined by

$$\ker(f) \triangleq \mathrm{eq}(f, 0) \quad \text{and} \quad \mathrm{coker}(f) \triangleq \mathrm{coeq}(f, 0)$$

Let $f : A \to B$ be a morphism. Suppose the fiber coproduct $B +_A B$ exists:

Then the **image** of $f : A \to B$ is then defined to be, if exists, the equalizer $\mathrm{eq}(i_1, i_2)$ of the two canonical morphism of the fiber coproduct

$$\mathrm{eq}(i_1, i_2) \overset{j}{\longhookrightarrow} B \underset{i_1}{\overset{i_2}{\rightrightarrows}} B +_A B$$

which comes with a canonical monomorphism $j : \mathrm{eq}(i_1, i_2) \hookrightarrow B$ and induce by universal property of equalizer a unique morphism $\lambda : A \to \mathrm{eq}(i_1, i_2)$ that makes the diagram
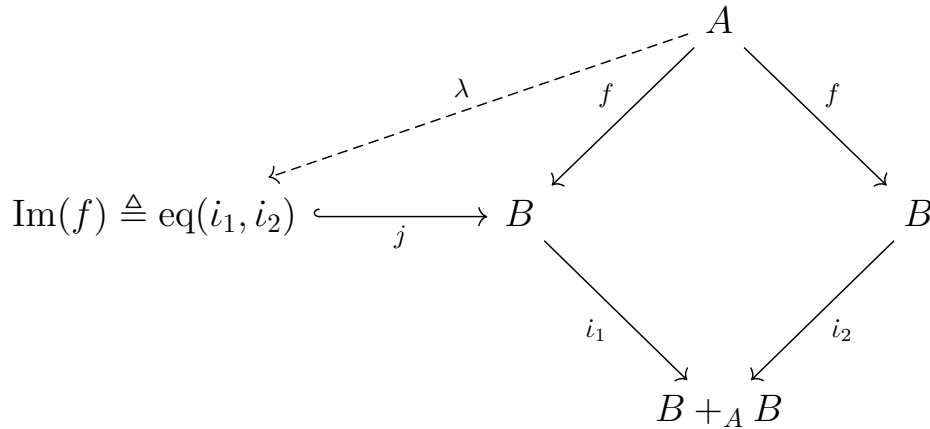
Theorem 4.10.1. (Images in familiar categories) Let R be a ring. Image exists in $\mathbf{Gp}, \mathbf{Ab}, \mathbf{Ring}$, and $\mathbf{Mod}_R$ in the usual form. In other word, given a homomorphism $f : A \to B$ in any of these categories, the usual image $f(A)$ together with the obvious map $f(A) \to B$ indeed satisfies the universal property of equalizer $\mathrm{eq}(i_1, i_2) \hookrightarrow B$ in which i_1, i_2

are the canonical morphisms of the fiber coproduct $B +_A B$, which we have proved indeed exists.

Proof. Routine. ∎

The **coimage** of a morphism $f : A \to B$ is then defined to be the coequalizer of the two canonical morphism in the fiber product $A \times_B A$.

$$A \underset{p_1}{\overset{p_2}{\rightrightarrows}} A +_B A \xrightarrow{\;s\;} \mathrm{coeq}(p_1, p_2)$$

which comes with a canonical epimorphism $s : A \to \mathrm{coeq}(p_1, p_2)$ for coequalizer:

$$
\begin{array}{ccc}
 & A \times_B A & \\
 \overset{p_1}{\swarrow} & & \overset{p_2}{\searrow} \\
A & & A \xrightarrow{\;s\;} \mathrm{coeq}(p_1, p_2) \triangleq \mathrm{coim}(f) \\
 \underset{f}{\searrow} & & \underset{f}{\swarrow} \\
 & B &
\end{array}
$$

Let morphism $f : A \to B$ admits both image and coimage, therefore both $A \times_B A$ and $B +_A B$ exists. Because $i_1 \circ f = i_2 \circ f$ by definition of fiber coproduct, there exists a unique morphism $\lambda : A \to \mathrm{Im}(f)$ such that $f = \lambda \circ j$ by universal property of image

$$
A \times_B A \underset{p_2}{\overset{p_1}{\rightrightarrows}} A \xrightarrow{\;f\;} B \underset{i_2}{\overset{i_1}{\rightrightarrows}} B +_A B
$$

with vertical maps s down from A to $\mathrm{coeq}(p_1, p_2) = \mathrm{coim}(f)$, the dashed map λ, and j up to B from $\mathrm{eq}(i_1, i_2) = \mathrm{Im}(f)$:

$$\mathrm{coeq}(p_1, p_2) = \mathrm{coim}(f) \qquad \mathrm{eq}(i_1, i_2) = \mathrm{Im}(f)$$

Now, because by definition of fiber product we have $f \circ p_1 = f \circ p_2$, we know $j \circ \lambda \circ p_1 = j \circ \lambda \circ p_2$ which by monicity of j implies $\lambda \circ p_1 = \lambda \circ p_2$, which by universal property of fiber product implies the existence and uniqueness of some morphism $u : \mathrm{coim}(f) \to \mathrm{Im}(f)$ that makes the diagram above commutes.

4.11 Every Mod$_A$ has enough injective and projective

A **divisible abelian group** G is an abelian group in which for all $g \in G$ and $n \in \mathbb{N}$, there exists some $y \in G$ that makes $ny = g$.

Theorem 4.11.1. (Divisible abelian groups are exactly injective objects) We have

$$J \in \mathbf{Ab} \text{ is injective} \iff J \text{ is divisible}$$

Proof. Left to right follows from a routine proof of contradiction.

∎

Therefore, $\mathbb{Q}/\mathbb{Z} \in \mathbf{Ab}$ is injective.
We say an A-module M is a **direct summand** of M'' if there exists some module M' that makes $M'' \cong M \oplus M'$.

Theorem 4.11.2. (Every module is a quotient of some free module) Let A be a ring and M be an A-module. Then we have a surjective module homomorphism from the free module

$$A^{(M)} \triangleq \bigoplus_{m \neq 0 \in M} A^m, \quad \text{where } A^m \cong A$$

to M by sending

$$a \in A^m \mapsto am$$

Proof. Routine. ∎

Equivalent Definition 4.11.3. (Projective Modules) Let A be a ring. We say an A-module P is **projective** if any of the followings hold true

(i) $P \in \mathbf{Mod}_A$ is a projective object.

(ii) P is a direct summand of some free module.

Proof. (i) $\implies$ (ii): Because $\mathbf{id}_P : P \to P$ is surjective, by universal property, the sequence right split.

(ii) $\implies$ (iii): This follows from the fact that P is a quotient of the free module $A^{(P)}$ and split lemma.

(iii) $\implies$ (i): Let $F \triangleq P \oplus N$ be free with basis $\{x_i\}$ and surjective homomorphism $\pi : F \to P$. Because $g : M \to M'$ is surjective, for all x_i there exists some $z_i \in M$ such that $g(z_i) = f \circ \pi(z_i)$. Therefore, ∎

Let A be a ring and M an A-module. We say a set $E \subseteq M$ is **linearly independent** if for all finite subset $\{e_1, \ldots, e_n\} \subseteq E$, we have

$$a_1 e_1 + \cdots + a_n e_n = 0 \implies a_1 = \cdots = a_n = 0$$

A **basis** for M is then a linearly independent generating set.

Equivalent Definition 4.11.4. (Free modules) Let A be a ring. We say an A-module M is **free** if any of the followings hold true:

(i) M admits a basis.

(ii) For some set S, we have an A-module isomorphism $M \cong \bigoplus_{i \in S} A$.

Proof. Routine. ∎