AJ-Note1

Written by An

Compile date: August 31, 2024

Repository address: https://github.com/PupilEarthquake/Aj_Note1
Home page: https://www.xiaorp.xyz/

The era of humanity has arrived.

Contents

Chapter 1

Set Theory

1.1 ZFC System

We ackonwledge the ZFC axiomatic system, and consider that the elements of a set are still sets.

Proposition 1.1.1 *If the axiom of regularity is accepted, namely:*

$$\forall A \neq \varnothing \ \exists a \in A \ (\forall a' \in A \Rightarrow a' \notin a)$$

which is equivalent to:

$$\forall A \neq \varnothing \ \exists a \in A \ (a \cap A = \varnothing)$$

The following propositions are true:

1. $\forall A \ (A \notin A)$.
2. $x_1 \in x_2 \Rightarrow x_1 \neq x_2$.
3. $\nexists \{x_i\}_{i \geq 0}$ *such that* $x_1 \ni x_2 \ni \cdots$

Corollary 1.1.2 *A_0 is a transitive set, then*

$$A_n \in A_{n-1} \in \cdots \in A_0 \Rightarrow (\forall 1 \leq k \leq n) \ A_k \in A_0$$

1.2 Mapping

Proposition 1.2.1 *The following propositions are equivalent:*

1 *1.1 $f : X \to Y$ is injection.*
1.2 f has the left inverse g that satisfies $gf = \mathrm{id}_X$.
1.3 f has the left cancellation law, namely $g_1 f = g_2 f \Rightarrow g_1 = g_2$ for $g_i : Y \to Z$.

2 *2.1 $f : X \to Y$ is surjection.*
2.2 f has the right inverse g that satisfies $fg = \mathrm{id}_Y$.

2.3 f *has the right cancellation law, namely* $fg_1 = fg_2 \Rightarrow g_1 = g_2$ *for* $g_i : Z \to X$.

Proof. see 李文威 2024 proposition 2.2.6. □

Proposition 1.2.2 *For mapping* $f : X \to Y$*, it holds that:*

Gnr *G.1.* $f(\bigcup_{i\in I} U_i) = \bigcup_{i\in I} f(U_i)$.
G.2. $f(\bigcap_{i\in I} U_i) \subset \bigcap_{i\in I} f(U_i)$.
G.3. $f(X \setminus U) \supset f(X) \setminus f(U)$.

Inj *I.1.* $f(\bigsqcup_{i\in I} U_i) = \bigsqcup_{i\in I} f(U_i)$.
I.2. $f(\bigcap_{i\in I} U_i) = \bigcap_{i\in I} f(U_i)$.
I.3. $f(X \setminus U) = f(X) \setminus f(U)$

Ivs *R.1.* $f^{-1}(\bigcup_{i\in I} V_i) = \bigcup_{i\in I} f^{-1}(V_i)$.
R.2. $f^{-1}(\bigcap_{i\in I} V_i) = \bigcap_{i\in I} f^{-1}(V_i)$.
R.3. $\forall V_1, V_2 \subset Y,\ f^{-1}(V_1 \setminus V_2) = f^{-1}(V_1) \setminus f^{-1}(V_2)$.

Proof. Gnr G.1. Trivial.

G.2. Trivial.

G.3. Trivial.

Inj I.1. We now prove that $\bigcap_{i\in I} f(U_i) \subset f(\bigcap_{i\in I} U_i)$. Suppose $y \in \bigcap_{i\in I} f(U_i)$, there exists $x \in X$ so that $y = f(x)$. If $x \notin \bigcap_{i\in I} U_i$, there must exists U_k that makes $x \notin U_k$. By properties of injection, we have $y = f(x) \notin f(U_k)$, it follows that $f(x) \notin \bigcap_{i\in I} f(U_i)$.

I.2. When $U_1 \cap U_2 = \varnothing$, $f(U_1 \cap U_2) = \varnothing$.

I.3. Assume $y \in f(X \setminus U)$, then there exists $x \in X \setminus U$ such that $y = f(x)$. Oberve that if $y \in f(U)$, then $\exists u \in U\ (f(u) = f(x))$, which contradicts the propertie of injection.

Ivs R.1. Trivial.

R.2. Trivial.

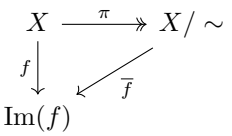
R.3. $x \in f^{-1}(V_1 \setminus V_2) \Leftrightarrow f(x) \in V_1 \setminus V_2 \Leftrightarrow f(x) \in V_1 \wedge f(x) \notin V_2 \Leftrightarrow x \in f^{-1}(V_1) \wedge x \notin f^{-1}(V_2)$. □

Corollary 1.2.3 $y_1 \neq y_2 \Rightarrow f^{-1}(y_1) \cap f^{-1}(y_2) = \varnothing$.

Theorem 1.2.4 $(X, \sim)$ *is a set* X *endowed with an equivalence relation* $\sim$*.* $f : X \to Y$ *is a mapping satisfies* $x_1 \sim x_2 \Rightarrow f(x_1) = f(x_2)$*. There exists unique mapping* $\overline{f} : X/\sim \to Y$ *that makes the following diagram commute:*

$$\begin{array}{ccc} X & \xrightarrow{\pi} & X/\sim \\ {\scriptstyle f}\downarrow & \swarrow_{\overline{f}} & \\ Y & & \end{array}$$

Theorem 1.2.5 *Conctinuing with the conditions of previous theorem, if $x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$, there exists unique bijection $\overline{f}$ such that:*



1.3 Ordinal

Since $A \notin A$, the following corollary is true:

Corollary 1.3.1 *If α is an ordinal, $\alpha + 1 := \alpha \cup \{\alpha\}$ is actually $\alpha \sqcup \{\alpha\}$.*

Lemma 1.3.2 *(This lemma suggests that* **On** *possesses a total-ordering.)*

1. *α is ordinal and $\beta \in \alpha$, then β is an ordinal.*
2. *For any ordinals α, β, if $\alpha \subsetneq \beta$, $\alpha \in \beta$.*
3. *For any ordinals α, β, $\beta \subset \alpha \vee \alpha \subset \beta$.*

Proof. (2): Let γ be the minimal element of $(\beta \setminus \alpha, \leq)$. By properties of well-ordered set, there holds that $\gamma \in \beta \setminus \alpha$. We assert $\alpha = \{x \in \beta : x < \gamma\}$, where the latter is nothing more than γ. The proof is as follows:

1. $\forall x \in \gamma \Rightarrow x \in \alpha$, otherwise $x \in \beta \setminus \alpha$ is smaller than γ.
2. $\forall x \in \alpha$, we first eliminate $x = \gamma$. Subsequently we have $x \subset \alpha$, which implies that $\gamma \notin x$.

(3): Let $\gamma = \alpha \cap \beta$, we assert that either $\gamma = \alpha$ or $\gamma = \beta$ must be true. □

Corollary 1.3.3 *Suppose C is a class of ordinals, then $\bigcap C$ is an ordinal, and $\bigcap C \in C$. (This corollary implies that every class of ordinals has a minimal element.)*

Proof. Firstly, we demonstrate that $\bigcap C \in C$ is an ordinal. Let γ be $\bigcap C$. Invoking the Axiom schema of separation, $\bigcap C = \{x \in c_0 : c_0 \in C \wedge \forall c \in C\ (x \in c)\}$ forms a set. It follows that $\gamma \subset c_0$. Then we have:

$$\forall x, y \in \gamma \Leftrightarrow x, y \in c_0$$

This implies every element in γ is comparable. Furthermore, we observe that every non-empty subset of γ possesses a minimal element, since:

$$\forall u \subset \gamma \Rightarrow u \subset c_0$$

and c_0 beging an ordianl guarentees the existance of a minimal element in u. Regarding the transitivity, we note that:

$$\forall x \in \gamma \Leftrightarrow \forall c \in C\ (x \in c) \Leftrightarrow \forall c \in C\ (x \subset c)$$

Therefore:

$$t \in x \Rightarrow \forall c \in C\ (t \in c) \Leftrightarrow t \in \gamma$$

Finally, to prove $\bigcap C \in C$, we assume for contradict that $\gamma \notin C$. Then for any $c \in C$, we have $\gamma \in c$. However, this leads to the contradiction that $\gamma \in \gamma$. □

Corollary 1.3.4 $\alpha \sqcup \{\alpha\} = \inf\{\beta : \beta > \alpha\} := \bigcap\{\beta : \beta > \alpha\}$.

Proof. Firstly, we observe that:

$$x \in \alpha \sqcup \{\alpha\} \Rightarrow x \in \alpha \vee x = \alpha \Rightarrow x \in \bigcap\{\beta : \beta > \alpha\}$$ □

To establish the reverse containment, let $\gamma = \bigcap\{\beta : \beta > \alpha\}$, it follows that $\gamma > \alpha$ and $\forall \beta > \alpha \Rightarrow \gamma \subset \beta$. Consequently, we have $\alpha < \gamma \leq \alpha \sqcup \{\alpha\}$, which is equivalent to stating that $\alpha \subsetneq \gamma \subset \alpha \sqcup \{\alpha\}$. The only posibility that satisfies this condition is $\gamma = \alpha \sqcup \{\alpha\}$.

Corollary 1.3.5 *S is a set of ordinals, then* $\sup S := \bigcup S$ *is also an ordinal.*

Proof. In accordance with the Axiom schema of repalcement, $\bigcup S$ is indeed a set.

We now prove that $\bigcup S$ is well-ordered. For any arbitrary $x_1,\ x_2 \in \bigcup S$, there exists $\alpha_1,\ \alpha_2 \in S$, so that $x_1 \in \alpha_1,\ x_2 \in \alpha_2$. $\alpha_1,\ \alpha_2$ are two ordinals that satisfy the ordering of **On**, so $x_1,\ x_2$ must belong to at least one of these two ordinals. Therefore $x_1,\ x_2$ are comparable under the ordering of ordinals. Thus, $\bigcup S$ is tot-ordered. Suppose $P \subset \bigcup S \wedge P \neq \varnothing$, then $P = \bigcup_{\alpha \in S}(\alpha \cap P)$. There must exists an α such that $\alpha \cap P \neq \varnothing$. Let m be the minimal element of it. We assert that m is the minimal element of P, if not, suppose $\min(P) = m_0$, then $m_0 < m < \alpha \cap P$, which implies m_0 is a smaller element than m in $\alpha \cap P$.

Next we prove that $\bigcup S$ is transitive. For any $x \in \bigcup S$, there exists $\alpha \in S$ such that $x \in \alpha$, thus $x \subset \alpha$. Moreover, it's easy to verify that $x \subset \bigcup S$. □

Corollary 1.3.6 *Suppose α is an limit ordinal, the following are equivalent:*

1. $\forall \beta < \alpha \Rightarrow \beta + 1 < \alpha$.
2. $\alpha = \bigcup\{\beta : \beta < \alpha\}$.

Proof. (1) ⇒ (2): A useful conclusion for any kind of ordinal is as follows:

$$\alpha \supset \bigcup\{\beta : \beta < \alpha\}$$

Regarding limit ordinals, we proceed to prove the reverse containment:

$$x \in \alpha \Rightarrow x + 1 \in \alpha \Rightarrow x \in x + 1 \subset \bigcup\{\beta : \beta < \alpha\}$$ □

We utilize Transfinite Recursion to define the various operations on ordinals, such as addition, multiplication and exponentiation (see 李文威 2019 p.18). For instance, addition is defined recursively as follows:

Define G as:

$$G(X) = \begin{cases} \alpha & (X = 0) \\ a(\gamma) \sqcup \{a(\gamma)\} & (X = \{(x, a(x)) : x < \beta \wedge \beta = \gamma + 1\}) \\ \bigcup\limits_{\gamma<\beta} a(\gamma) & (X = \{(x, a(x)) : x < \beta \wedge \beta \text{ is limit ordinal}\}) \\ \Omega & (\text{else}) \end{cases}$$

Then let $a + (\cdot)$ be a θ-sequence defined as:

$$\alpha + \beta := G(\{(x, \alpha + x)\}_{x<\beta})$$

By Transfinite Recursion, we can conclude that $a + (\cdot)$ is well-defined on **On**.

1.4 Transfinite Recursion

In terms of what I've been learned, Transfinite Induction is a well-established principle utilized to address problems of this nature, provided the following conditions are met:

- the ordinal 0 satisfies property P;
- if $\alpha < \theta$ (or **On**) satisfies P, then $\alpha + 1$ alse satisfies P;
- if α is a limit ordinal, and for all $\beta < \alpha$, β satisfies P, then α satisfies P;

Under the conditions, it can be concluded that the property P holds for all ordinals that belong to θ (or **On**).

This closely resembles the usual Induction, with the latter being a specific instance within the broder framework of Transfinite Induction. Specificly, when θ is set to be the smallest limit ordinal ω, the third condition mentioned earlier becomes redundant, and Transfinite Induction reduces to standerd Induction. However, Transfinite Induction offers a more comprehensive perspective, enableing us to extend our reasoning to broder contexts. For instance, it will be used to demonstrate that two funtions agree on **On**, assuming they satisfy certain prescribed properties, where standerd Induction is inadequate. Furthermore, Transfinite Induction finds its application in the proof of Transfinite Recursion.

Theorem 1.4.1 (Transfinite Induction) *Suppose C is a class of ordinals, and the following conditions are true.*

1. $0 \in C$.
2. $\alpha \in C \Rightarrow \alpha + 1 \in C$.
3. *Suppose α is a limit ordinal, and* $(\forall \beta < \alpha \Rightarrow \beta \in C) \Rightarrow \alpha \in C$.

*Then $C =$ **On**. This assertion remains valid when considering only ordinals less than a given ordinal θ*

Proof. We only consider the case on a given ordinal θ. Suppose $C \neq \theta$, and let $\gamma = \min(\theta \setminus C)$. We have $\gamma \notin C$ and $\gamma \neq 0$, and the remainder of proof can be devided into several cases.

case 1. γ is a successor, so $\exists\beta \in \theta(\gamma = \beta + 1)$.

case 1a. $\beta \in C$, by definition we have $\gamma = \beta + 1 \in C$.

case 1b. $\beta \notin C$, then $\gamma < \beta < \gamma$.

case 2. γ is a limit ordinal.

case 2a. $\forall\beta < \gamma\ (\beta \in C)$, by definition we have $\gamma \in C$.

case 2b. $\exists\beta < \gamma \wedge \beta \notin C$, then $\gamma < \beta < \gamma$. □

To define a funtion whose domain is the ordinal θ, a formal approach can be outline as follows. Initially, we assign $a(0)$ to be an element a_0 in $\mathbf{V}$. Subsequently, for any ordinal α satisfying $0 < \alpha < \theta$, we determine $a(\alpha)$ by rely on the previously established vlues $\{a(x)\}_{x<\alpha}$, which can be expressed as $a(\alpha) = G(\{a(x)\}_{x<\alpha})$, where G is a funtion mapping from $\mathbf{V}$ to $\mathbf{V}$.

For example, there exists a funtion from **On** to a nonempty set that is constructed in the proof of Zermelo's Theorem. Given an non-empty set S, it follows that $P(S) \setminus \{\varnothing\}$ is also non-empty. According to the Axiom of Choise, we have

$$\prod_{A \in P(S)\setminus\{\varnothing\}} A \neq \varnothing$$

which implies the existance of funtion

$$\begin{aligned} g : P(S) \setminus \{\varnothing\} &\to S \\ A &\mapsto x \text{ (an element belongs to } A) \end{aligned}$$

Next, we specify an arbitrary $a_0 \in S$, and choose distinct elements $\Omega_0,\ \Omega_1 \notin S$ with $\Omega_0 \neq \Omega_1$. We define G as follows

$$G(X) = \begin{cases} a_0 & X = \varnothing \\ g(S \setminus X) & X = \{a_x\}_{x<\alpha} \subsetneq S\ (\alpha \in \mathbf{On}) \\ \Omega_0 & X = S \vee X = S \sqcup \{\Omega_0\} \\ \Omega_1 & \text{else} \end{cases}$$

Finally, we recursively define the funtion a by

$$a(\alpha) = G(\{a(x)\}_{x<\alpha})$$

Seems like we've defined a funtion from $\mathbf{On} \to S \sqcup \{\Omega_0\}$. However, in my opinion, our endeavors so far has not been adequate, because we have merely assigned an initial value to a and provided a procedure for updating it's subsequent values.

Now back to the start. Does the funtion a exists (and even unique) given sole konwledge of it's initial value $a(0)$ an the funtion G that prescribe its updates? This inquiry directs us toward the principle of Transfinite Recursion, which addresses precisely usch questions regarding the construcion of funtions over the ordinals.

Theorem 1.4.2 (Transfinite Recursion) *For any ordinal θ, there exists a unique θ-sequence a such that for all ordinals $\alpha < \theta$, we have $a(\alpha) = G(a|_\alpha)$. In particular, there exists a unique function $a : \mathbf{On} \to \mathbf{V}$ so that for any ordinal α, $a(\alpha) = G(a|_\alpha)$.*

Proof. We consider the case involving a given ordinal θ, and initially demonstrate the uniqueness of the *θ-sequence*. Suppose both *θ-sequence* a and a' satisfy the recursive definitions

$$a(\alpha) = G(\{a(x)\}_{x<\alpha}),\ a'(\alpha) = G(\{a'(x)\}_{x<\alpha})$$

To prove uniqueness, we invoke the Transfinite Induction. We define a class C of ordinals as $C = \{\alpha < \theta : a(\alpha) = a'(\alpha)\}$. We then verify that C satisfies the three condition of Transfinite Induction. Firstly, notice that $a(0) = G(0) = a'(0)$ since any function constrained on an emptyset is $\varnothing$. This implies that $0 \in C$. Secondly, suppose that for all $x < \alpha$, we have $x \in C$, i.e., $a(x) = a'(x)$ for all $x < \alpha$. Whether α is a successor or a limit ordinal, the equality $\{a(x)\}_{x<\alpha} = \{a'(x)\}_{x<\alpha}$ holds. Consequently

$$a(\alpha) = G(\{a(x)\}_{x<\alpha}) = G(\{a'(x)\}_{x<\alpha}) = a'(\alpha)$$

Thus the Inductive step is satisfied for both successor and limit ordinals. Finally, by the Transfinite Induction, we conclude that $C = \theta$.

Next, we establish the existance of a by adopting a methodlogy analogous to the proof of uniqueness. We define C as the class of ordinals satisfing the condition:

$$C = \{\xi < \theta : \text{the } \xi\text{-sequence } a[\xi] \text{ exists}\}$$

Evidently, $a[0]$ exists and is trivilly set to be 0, thus $0 \in C$. Assume that $0 < \beta < \theta$ and that for all $\xi < \beta$, the function $a[\xi]$ exists. We process to demonstrate the existance of $a[\beta]$.

We assert that if $\zeta < \eta$, and $a[\zeta],\ a[\eta]$ exists, then $a[\eta]|_\zeta = a[\zeta]$. The basis for this assertion is

$$a[\zeta]|_\eta(x) = G(\{a[\zeta]|_\eta(t)\}_{t<x})$$
$$a[\eta](x) = G(\{a[\eta](t)\}_{t<x})$$

By the uniqueness mentioned above, we conclude that this assertion is true.

Subsequently, we let $a[\beta](\xi) := G(a[\xi])$ $(\forall \xi < \beta)$, and it gives that $\forall x < \beta$:

1. $a[\beta]|_x = \{G(a[t])\}_{t<x} = \{G(a[x]|_t)\}_{t<x} = \{a[x](t)\}_{t<x}$.
2. $a[\beta](x) = G(a[x]) := G(\{a[x](t)\}_{t<x})$.
3. $a[\beta](x) = G(a[\beta]|_x)$. □

Hence we conclude that $\beta \in C$. By the Transfinite Induction, it follows that $C = \theta$.

1.5 Cardinal

Definition 1.5.1 *X is a set, $|X|$ is defined as its equipotence class.*

Theorem 1.5.2 (Schröder–Bernstein) $|X| \leq |Y| \wedge |Y| \leq |X| \Rightarrow |X| = |Y|$.

Proof. Suppose there holds that $X \overset{f}{\hookrightarrow} Y \overset{g}{\hookrightarrow} X$. And notice the following diagram commutes:

$$\begin{array}{ccc} X & \overset{f}{\hookrightarrow} & Y \\ {\scriptstyle \mathrm{id}_X}\downarrow & & \downarrow{\scriptstyle g} \\ X_0 & \underset{f'}{\hookrightarrow} & Y_0 \end{array}$$

where $Y_0 = \mathrm{Im}(g)$. Our purpose is to build a bijction on $X_0 \to Y_0$. To archieve this, define X_n, Y_n recursively: $X_{n+1} = f'(X_n), Y_{n+1} = f'(Y_n)$. Then we obtain a chain like:

$$X_0 \supset Y_0 \supset X_1 \supset Y_1 \supset \cdots$$

It can be verified that:

$$X_0 = \left(\bigsqcup_{n\geq 0} (X_n \setminus Y_n) \right) \sqcup \left(\bigsqcup_{n\geq 0} (Y_n \setminus X_{n+1}) \sqcup \left(\bigcap_{n\geq 0} X_n \right) \right) =: U \sqcup V$$

By the propertie of injection, we also have:

$$X_n \setminus Y_n \overset{1:1}{\underset{f'}{\to}} X_{n+1} \setminus Y_{n+1}$$

Define $\phi : X_0 \to Y_0$ as:

$$\phi(x) = \begin{cases} f'(x) & (x \in U) \\ x & (x \in V) \end{cases}$$

It trival to show that ϕ is well defined. We proceed to prove it's injection: The only case need to specify is that $x \in U \wedge y \in V$. To show this, notice that $\phi(x) \in U$ and $\phi(x) \in V$. Moreover, ϕ is surjection since:

- ϕ is injection $\Rightarrow \phi(X \sqcup Y) = \phi(X) \sqcup \phi(Y)$.
- $\phi(V) = \mathrm{id}(V) = V$.
- $\phi(U) = f'(U) = \bigsqcup_{n\geq 0}(X_{n+1} \setminus Y_{n+1})$.
- $\phi(U \sqcup V) = Y_0$. □

Definition 1.5.3 $\kappa \in \mathbf{On}$ *is a cardinal iff* $\forall \lambda < \kappa \Rightarrow |\lambda| < |\kappa|$.

By Well-ordering Theorem, every set X has a equipotent ordinal α. Define $C = \{\alpha \in \mathbf{On} : |\alpha| = |X|\}$, and let $\alpha_X = \inf C$, it can be verified that α_X is a cardinal.

Proposition 1.5.4 *The following propositions are true:*

1. $|X| = |Y| \Leftrightarrow \alpha_X = \alpha_Y$.
2. $|X| < |Y| \Leftrightarrow \alpha_X < \alpha_Y$.

3. $|X| \leq |Y| \Leftrightarrow \alpha_X \leq \alpha_Y$

Proposition 1.5.5 *For any non-zero cardinals $0 < \kappa \leq \lambda$, in which λ is infinite cardinal. Then:*

1. $\kappa + \lambda = \kappa \cdot \lambda = \max\{\lambda, \kappa\}$.
2. *If $2 \leq \kappa < \lambda$, then $\kappa^\lambda = 2^\lambda$.*

Proof. See 李文威 2019 Corollary 1.4.9. □

Proposition 1.5.6 *If $|A| \geq \aleph_0$, then $\aleph_0|A| = |A|$.*

Proof. Let set $\mathcal{F}$ be

$$\mathcal{F} = \{f \in S^{\mathbb{Z}_{\geq 0} \times S} : S \subset A \wedge f \text{ is bijction}\}$$

Notice that when $S = \mathbb{Z}_{\geq 0}$, there exists a bijction $\mathbb{Z}_{\geq 0}^2 \to \mathbb{Z}_{\geq 0}$, thus $\mathcal{F} \neq \varnothing$. Define a relation on $\mathcal{F}$ such that $f \preccurlyeq g \Leftrightarrow \Gamma_f \subset \Gamma_g$, which can be easily verified to be a partial ordering on $\mathcal{F}$.

We claim that every chain in $\mathcal{F}$ has an upper bound. The proof proceeds as follows. Let $\{f_t\}_{t \in T}$ be a chain contained in $\mathcal{F}$. Define $U = \bigcup_{t \in T} \Gamma_{f_t}$. It can be verified that U is a graph and corresponds to a bijction in $\mathcal{F}$, which we denote as f_0.

By Zorn's Lemma, $\mathcal{F}$ has a maximal element, denoted as $h : \mathbb{Z}_{\geq 0} \times \tilde{S} \to \tilde{S}$. If $\tilde{S} \subsetneq A$, then we choose an element $\gamma \in A \setminus \tilde{S}$, and $s \in \tilde{S}$. We define a bijction $h' : \mathbb{Z}_{\geq 0} \times \tilde{S} \sqcup \{\gamma\} \to \tilde{S} \sqcup \{\gamma\}$ as follows:

$$h'(n, a) = \begin{cases} \gamma & (n = 0 \wedge a = \gamma) \\ h(s, 2n+1) & (n > 0 \wedge a = \gamma) \\ h(s, 2n+2) & (a = s) \\ h(a, n) & \text{else} \end{cases}$$

Since $\Gamma_{h'}$ is larger than Γ_h, which contradicts the assumption that h is maximal element in $\mathcal{F}$, we conclude that $\tilde{S} = A$. □

1.6 Grothendieck Universe

Definition 1.6.1 *A universe is a set $\mathcal{U}$ that satisfies the following properties:*

U.1. $\mathcal{U}$ is a transitive set, namely $\forall u \in \mathcal{U} \Rightarrow u \subset \mathcal{U}$.

U.2. $u, v \in \mathcal{U} \Rightarrow \{u, v\} \in \mathcal{U}$. (Quite alike paring axiom)

U.3. $u \in \mathcal{U} \Rightarrow P(u) \in \mathcal{U}$.

U.4. $I \in \mathcal{U}$, $\forall i \in I$ $u_i \in \mathcal{U}$, then $\bigcup_{i \in I} u_i \in \mathcal{U}$.

U.5. $\mathbb{Z}_{\geq 0} \in \mathcal{U}$. (This implies that $\varnothing \in \mathcal{U}$).

Corollary 1.6.2 *Suppose $\mathcal{U}$ is a universe:*

1. $u \subset v \in \mathcal{U} \Rightarrow u \in \mathcal{U}$.
2. $u \in \mathcal{U} \Rightarrow \bigcup u \in \mathcal{U}$.
3. $u, v \in \mathcal{U} \Rightarrow u \times v \in \mathcal{U}$.
4. $I \in \mathcal{U},\ \forall i \in I\ u_i \in \mathcal{U}$, *then* $\prod_{i\in I} u_i \in \mathcal{U}$.

Proof. (1) $v \in \mathcal{U} \Rightarrow P(v) \in \mathcal{U}$. Using axiom U.3., we have $u \in P(v) \in \mathcal{U}$. Using axiom U.1., $u \in \mathcal{U}$.

(2) By axiom U.1., $\forall x \in u \Rightarrow x \in \mathcal{U}$. Then applying axiom U.4., we obtain $\bigcup u = \bigcup_{x\in u} x \in \mathcal{U}$.

(3) Recall the definition of set product, it follows that:

$$u \times v := \{\{\mu, \{\mu, \xi\}\} \in P(P(u \cup v)) : \mu \in u \wedge \xi \in v\}$$

Thus $u \times v \subset P(P(u \cup v))$. Invoking the 2nd proof, the rest steps are as follows:

$$u \cup v \in \mathcal{U} \Rightarrow P(u \cup v) \in \mathcal{U} \Rightarrow P(P(u \times v)) \in \mathcal{U} \Rightarrow u \times v \in \mathcal{U}$$

(4) Observe that $\bigcup_{i\in I} u_i \in \mathcal{U} \Rightarrow \bigcup_{i\in I} u_i \times I \in \mathcal{U}$, and that

$$\prod_{i\in I} u_i \subset (\bigcup_{i\in I} u_i)^I \subset P(\bigcup_{i\in I} u_i \times I)$$

The remains of the proof are trivial. □

Definition 1.6.3 *The cumulative hierachy of set is recursively constructed in the following way:*

$$V_0 := \varnothing$$
$$V_{\alpha+1} = P(V_\alpha)$$
$$V_\alpha := \bigcup_{\beta<\alpha} V_\beta \ (\alpha \textit{ is a limit ordinal})$$

Corollary 1.6.4

1. *Each V_α is transitive set.*
2. $\alpha \subset V_\alpha$.
3. $\alpha < \beta \Rightarrow V_\alpha \subset V_\beta$.

Proof. (1) Define C be the class of ordinals that makes V_α a transitive set. An initial result is $0 \in C$. Furthermore, assume that V_α is transitive. For any $x \in V_{\alpha+1} = P(V_\alpha)$, we have $x \subset V_\alpha$. $\forall t \in x \Rightarrow t \in V_\alpha \Rightarrow t \subset V_\alpha \Rightarrow t \in P(V_\alpha)$, thus $x \subset V_{\alpha+1}$. Therefore we obtain that $\alpha \in C \Rightarrow \alpha + 1 \in C$. When α is a limit ordinal, it is easy to verify $\forall \beta < \alpha, \beta \in C \Rightarrow \alpha \in C$. Consequently, applying Transfinite Induction, we have $C = \mathbf{On}$.

(2) Define $C = \{\alpha : \alpha \subset\in V_\alpha\}$, and it follows that $0 \in C$. If $\alpha \in C$, then $\alpha \sqcup \{\alpha\} \subset P(\alpha) \subset P(V_\alpha)$. When α is a limit ordinal, $\alpha = \bigcup_{\beta<\alpha} \beta \subset \bigcup_{\beta<\alpha} V_\beta$.

(3) Define $C = \{\beta : V_\alpha \subset V_{\alpha+\beta}\}$. The result is that $C = \mathbf{On}$. □

Theorem 1.6.5 *Every set is contained within a V_α, where α is an ordianl.*

Definition 1.6.6 *α is a regular cardinal iff:*

RC.1. $\alpha \geq \aleph_0$.

RC.2. There does not exsits a limit ordinal β such that $\beta < \alpha$ and a strictly increasing sequence of ordinals $\{a_\xi : \xi < \beta\}$ such that $\sup\{a_\xi : \xi < \beta\} = \alpha$.

Definition 1.6.7 *A cardinal κ is a strongly inaccessible cardinal iff:*

SI.1. $\kappa > \omega$.

SI.2. κ is a regular cardinal.

SI.3. $\forall \lambda \in \mathbf{On},\ \lambda < \kappa \Rightarrow 2^\lambda < \kappa$.

Grothendieck Universe are equivalent to strongly inaccessible cardinals (WikiPedia 2024),

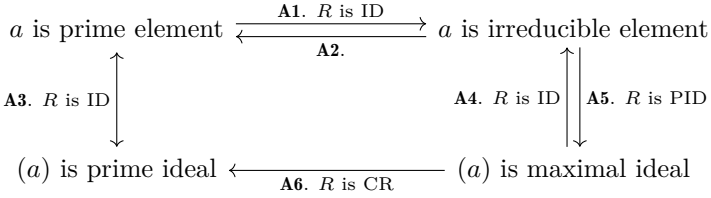
Chapter 2

Ring and Field

2.1 Zoom Table

Abbreviated specification:

- **ID**: Integral domain.
- **CR**: Commutative ring.
- **PID**: Principle ideal domain.
- **UFD**: Unique factorization domain.
- **EID**: Euclidean integral domain.



Other conclusions:

B1. R is EID $\Rightarrow$ R is PID.

B2. R is PID $\Rightarrow$ R is UFD.

B3. (i) R is ID, (ii) every proper factor chain in R is finite, (iii) every irreducible element is prime element $\Rightarrow$ R is UFD.

B4. (i) R is ID, (ii) every $r \in R$ can be denoted as a multiplication of irreducible elements, (iii) every irreducible element is prime element $\Leftrightarrow$ R is UFD.

B5. R is UFD $\Rightarrow$ $\exists \gcd(a, b)$.

Proof

A1. Let p be a prime element, suppose $a|p$, then $p|ab$. If $p|a$, we have $p \sim a$. On the other hand, if $p|b$, then $p = hpa$. Due to there is no zero divisor in ID, we conclude that $ha = 1$, which implies $a \sim 1$.

A2. **case1**. R is ID, and every two elements in R have the greatest common divisor. The proof proceeds as follows: Let p be the irreducible element in R, and $p|bc$. Then $\gcd(p, b)$ is either the invertible element of R or the equivalent element of b. If $\gcd(p, b) \sim 1$, then $\gcd(cp, cb) \sim c$ (丘维声 2015 p.146.). We have $p|\gcd(cp, cb) \wedge \gcd(cp, cb)|c$, thus $p|c$. If $\gcd(p, b) \sim p$, we immediatly get $p|b$.

case2. R is PID. (The proof can be performed as the process that R is PID $\Rightarrow$ R is UFD $\Rightarrow$ $\exists \gcd(a, b)$. The following we provid another way of solution, see 李文威 2024 Lemma 6.2.9). Suppose p is a prime element and $p|ab$, there exists f such that $\langle p, a\rangle = (f)$. Therefore $(a) \subset (f)$ and $(p) \subset (f)$ hold, which is equivalent to $f|a$ and $f|p$. If $f \sim 1$, then $\langle a, p\rangle = R$, which implies there exists u, v such that $ua + vp = 1$. Thus we have $uab + vpb = b$, hence $p|uab + vpb = b$. If $f \sim p$, we immediatly get $p|a$.

A3. a is a prime $\Leftrightarrow a \neq 0 \wedge a \notin R^\times \wedge (a|bc \Rightarrow a|b \vee a|c) \Leftrightarrow (a) \neq (0) \wedge (a) \neq R \wedge (bc \in (a) \rightarrow b \in (a) \vee c \in (a))$.

A4. By **A6**. **A3**. and **A1**.

A5. Suppose $(a) \subset I \subset R$. By prescribed condition that R is PID, so we have $I = (b)$. Thus either $b \sim 1$ or $b \sim a$ holds.

A6. (a) is maximal ideal $\Leftrightarrow$ $R/(a)$ is a filed $\Rightarrow$ $R/(a)$ is an ID $\Leftrightarrow$ (a) is a prime element.

B1. EZ.

B2. **step1**. R is PID, then every ascending chain of ideals in R stops. To be specific, suppose $(I_n)_{n\geq 0}$ is a series of ideals, which satisfies $I_1 \subset I_2 \subset \cdots$. There must exists $n \in \mathbb{Z}_{\geq 0}$ such that $I_n = I_{n+1} = \cdots$. The proof is as follows: Let $I = \bigcup_{n\geq 0} I_n$, it follows that I is an ideal, thus $I = (h)$. It can be verified that $\exists n \in \mathbb{Z}_{\geq 0}$ that $h \in I_n$, and therefore $I \subset I_n$.

step2. If R satisfies the ascending chain condition that every ascending chain of ideals in R stops, then $\forall r \in R^*$ can be denoted as a multiplication of irreducible elements. If $r \in R^\times$, we agree that r is a multiplication of 0 irreducible element. If $r \notin R^\times$, we let $r_0 = r$ and assume that r has no irreducible factorization. It follows that r is not irreducible, or $r = r$ is a irreducible factorization. Thus we have $r_0 = r_1 s_1$ where $r_1, s_1 \nsim r_0$, which implies that $(r_0) \subsetneq (r_1)$ and $(r_0) \subsetneq (s_1)$. By the assumption that r has no irreducible factorization, we conclude that r_1 or s_1 remains the same property. Suppose r_1 has no irreducible factorization, and continue the process. Finally we end up with a strictly ascending chain of ideals $(r_0) \subsetneq (r_1) \subsetneq \cdots$, which contradicts the discussion in step1.

step3. By **A2**. we conclude that in PID every irreducible element is prime element. The uniqueness of decomposition can be easily verified by using Induction.

B3. Similar to **B2**.

B4. ($\Rightarrow$) is similar to **B2**. Next we prove the ($\Leftarrow$) direction (李文威 2024 Proposition 6.3.2). Suppose R is UFD , $p \in R$ is irreducible, and $p|ab$ where $a = q_1 \cdots q_m$, $b = r_1 \cdots r_n$. Therefore $\frac{ab}{p}$ can be decomposited as $s_1 \cdots s_t$. Thus $q_1 \cdots q_m r_1 \cdots r_n = ab = s_1 \cdots s_t p$. By the uniqueness of decomposition, it follows that $p \sim q_i \vee p \sim r_i$.

B5. Suppose $a = \prod_{i\geq 1} p_i^{n_i}$, $b = \prod_{i\geq 1} p_i^{m_i}$. Let $g_0 = \prod_{i\geq 1} p_i^{\min\{n_i,m_i\}}$. Recall the definition of gcd in PID that $\langle a_1, \cdots, a_n\rangle = \gcd(a_1, \cdots, a_n)R = gR$. It directs us toward the proof of $g_0 \sim g$. Pursuant to 李文威 2024 Proposition 2.7.3, we have $g_0|a \wedge g_0|b \Leftrightarrow (\forall x \in \langle a, b\rangle \Rightarrow g_0|a) \Leftrightarrow g_0|g$. To prove the reverse direction, notice that $g|a \wedge g|b$, which implies that $g = \prod_{i\geq 1} p_i^{t_i}$ and $t_i \leq \min\{n_i, m_i\}$. We conclude that $g|g_0$.

2.2 Some properties of ring

Several isomophism theorems can copy the results of linear space, see Section 3.4.

Proposition 2.2.1 *For any ring R, there exists unique homomorphism $\sigma : \mathbb{Z} \to R$ that maps 1 into 1_R.*

Definition 2.2.2 *Continuing with the conditions above, $\operatorname{Ker}\sigma \subset \mathbb{Z}$ is an ideal. By the propertie of PID, there exists unique number $\operatorname{char} R \in \mathbb{Z} \wedge \operatorname{char} R \geq 0$ such that:*

$$\operatorname{Ker}\sigma = (\operatorname{char} R)\mathbb{Z}$$

Proposition 2.2.3 *R_0 is a subring of R, then $\operatorname{char}(R_0) = \operatorname{char}(R)$.*

Proposition 2.2.4 *R is an ID, then:*

1. $\operatorname{char}(R) = 0 \Rightarrow \mathbb{Q} \hookrightarrow R$.
2. $\operatorname{char}(R) = p > 0 \Rightarrow \mathbb{F}_p \hookrightarrow R$.

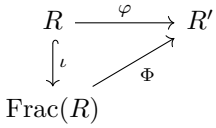
Proof. (1): By Proposition 2.2.1, observe that $\mathbb{Z} \overset{\sigma}{\hookrightarrow} R$, and then apply Proposition 2.2.6.

(2): It holds that $\mathbb{Z}/\operatorname{Ker}\sigma = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \simeq \operatorname{Im}\sigma = R$. □

Proposition 2.2.5

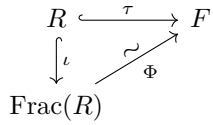
1. *R is a filed iff R has only ordinary ideals.*
2. *Any ring homomorphism defined on F, a field, is injective.*

Proposition 2.2.6 *Suppose R is ID, R' is CR. $\varphi : R \to R'$ is a ring homomorphism, which satisfies $\varphi(R^*) \subset (R')^\times$. Then there exists unique $\Phi : \mathrm{Frac}(R) \to R'$ that maps $[f, g]$ to $\varphi(f)\varphi(g)^{-1}$, in other words, the following diagram commutes:*



Proof. Define mapping $\psi : \mathrm{Ratio}(R) \to R'$ as follows: $(a, b) \mapsto \varphi(a)\varphi(b)^{-1}$. It can be verified that (i) ψ is well defined; (ii) ψ is ring homomorphism; (iii) $(a, b) \sim (c, d) \Leftrightarrow ad = bc \Rightarrow \psi(a, b) = \psi(c, d)$. Applying Theorem **??**, there exists unique mapping $\Phi : \mathrm{Ratio}(R)/\sim \to R'$ that maps $[a, b]$ to $\varphi(a)\varphi(b)^{-1}$. It straitfoward to verify it is a ring homomorphism. □

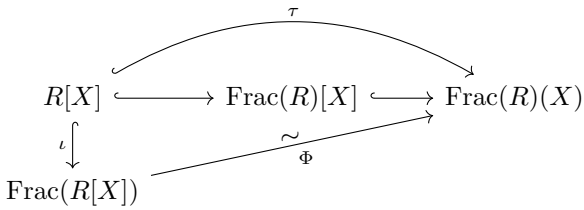
Corollary 2.2.7 *The ID R embeded into field F, where each element can be represented as $\tau(a)\tau(b)^{-1}$. There exists unique ring isomorphism $\Phi : \mathrm{Frac}(R) \to F$ that maps $[a, b]$ to $\tau(a)\tau(b)^{-1}$, which is equivalent to the diagram:*



Proposition 2.2.8 *R is ID, then*

$$\mathrm{Frac}(R)(X) \simeq \mathrm{Frac}(R[X])$$

Proof.



The noly thing that need to clarify is that every element in $\mathrm{Frac}(R)(X)$ can be denoted as $\tau(a)\tau(b)^{-1}$ where $a, b \in R[X]$, and it is straitforward:

$$\frac{\sum_{i=0}^{n} \frac{a_i}{b_i} X^i}{\sum_{j=0}^{m} \frac{c_j}{d_j} X^j} = \frac{\prod_{j=0}^{m} d_j \sum_{i=0}^{n} a'_i X^i}{\prod_{i=0}^{n} b_i \sum_{j=0}^{m} c'_i X^i}$$

□

Proposition 2.2.9 *For any ring L, given homomorphism $F \overset{\xi}{\hookrightarrow} L$, we can endow L a F-vector space structure. This is done by defining addition as the addition in L, and scalar multiplication as $k \cdot x := \xi(k)x$.*

Suppose F is a filed, $f \in F[X]$. define ι as follows:

$$\iota : F \longrightarrow F[X]/(f)$$

$$a \longmapsto a + (f)$$

Clearly ι is injective.

Corollary 2.2.10 *Endowed with ι, $F[X]/(f)$ becomes a F-vector space.*

Theorem 2.2.11 *Suupose $\xi : F \to L$ is a ring homomorphism, and Ψ is a substitution mapping:*

$$\Psi : F[X] \longrightarrow L$$

$$\sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} \xi(a_i)\beta^i$$

Then there exists a unique $\psi \in \mathrm{Hom}_{\mathsf{Vect}(F)}(F[X]/(f), L)$

2.3 Unique factorization domain

Definition 2.3.1 *R is UFD iff (i) each non-zero element in R can be decomposited into the multiplication of finite many irreducible elements; (ii) this decomposition is Unique in the sense of equivalence that $a \sim b \Leftrightarrow a \in bR^\times$.*

Corollary 2.3.2 *p is an irreducible element, then every element in $pR^\times$ is irreducible.*

Define $P = \{p \in R : \text{irreducible element}\}$. The equivalence relationship was defined as $a \sim b \Leftrightarrow a \in bR^\times$. We hope to decompose P into the disjoint union of equivalence classes, and select a subset consisting of representative elements. To archieve this, the first step is choose an function $g \in \prod(P/\sim)$. Then $\mathrm{Im}\, g$ is what we want.

Proposition 2.3.3 *Suppose $\mathrm{Im}\, g = \{p_a\}_{a\in A}$. R is UFD. Then $\forall a \in R^*$ can be decomposited as:*

$$\underbrace{e}_{\in R^\times} \prod_{a\in A} \underbrace{p_a^{n_a}}_{fm\ n_a \neq 0}$$

Proof. By definition of UFD, we obtain that $a = q_1^{n_1} \cdots q_s^{n_s}$, where $q_i \in [p_i]_\sim$. Thus $a = e_1^{n_1} \cdots e_s^{n_s} p_1^{n_1} \cdots p_s^{n_s}$. □

Suppose R is a ring, and $a_1, \cdots, a_s \in R$. In principle, the greatest common divisor of $a_1, \cdots, a_s$ are define as an element d which satisfies the following properties: (i) d is a common factor; (ii) for any common factor l it holds that $l|d$. For other spacial rings, the gcd has different definitions. Below is an example in UFD:

Definition 2.3.4 *$a_1, \cdots, a_s \in R^*$, each of them can be decomposited to $e_i \prod_{a\in A} p_a^{n_{ai}}$. Then*

$$\gcd(a_1, \cdots, a_s) := \prod_{a\in A} p_a^{\min\{n_{a1}, \cdots, n_{as}\}}$$

(This definition ensures it's output is 1 when the inputs are mutual prime.)

Using the newly definition of gcd, it can be verified that:

Proposition 2.3.5 *If $a_1, \cdots, a_s \in R^*$, then:*

1. $\forall i,\ \gcd(a_1, \cdots, a_s) | a_i$.
2. $\forall i\ (d|a_i) \Rightarrow d|\gcd(a_1, \cdots, a_s)$.

Additionally, if $r \in R$ satisfies the following properties:

1. $\forall i,\ r|a_i$.
2. $\forall i\ (d|a_i) \Rightarrow d|r$.

then $r \in \gcd(a_1, \cdots, a_s)R^\times$. In other words, the set that consisting of all gcd of $a_1, \cdots, a_s$ is $\gcd(a_1, \cdots, a_s)R^\times$.

Corollary 2.3.6 *Suppose $a = u\prod_{i=1}^s p_i^{n_i}, b = v\prod_{i=1}^s p_i^{m_i}$, then*

$$a|b \Leftrightarrow \forall i\ (n_i \leq m_i)$$

Proof. Without losing generality, suppose for the contradiction that $n_1 > m_1$, and it leads to a contradiction:

$$\begin{aligned} a|b &\Leftrightarrow \exists h \in R\ (ah = b) \\ &\Rightarrow p_i^{m_1}\left(uhp_1^{n_1-m_1}p_2^{n_2}\cdots p_s^{n_s} - vp_2^{m_2}\cdots p_s^{m_s}\right) = 0 \\ &\Rightarrow uhp_1^{n_1-m_1}p_2^{n_2}\cdots p_s^{n_s} = vp_2^{m_2}\cdots p_s^{m_s} \\ &\text{(By the definition of UFD)} \Rightarrow n_1 = m_1 \end{aligned}$$

For the reverse direction, suppose $\forall i\ (n_i \leq m_i)$. It follows that:

$$u\prod_{i=1}^s p_i^{n_i} \cdot u^{-1}v\prod_{i=1}^s p_i^{m_1-n_i} = v\prod_{i=1}^s p_i^{m_i}$$

□

Proposition 2.3.7 *R is UFD, then each irreducible element is prime element.*

All subsequent R , if not otherwise specified, is UFD.

Definition 2.3.8 *$R[X]^* \ni f = a_nX^n + \cdots + a_0$, and d is one of the gcds of $a_n, \cdots, a_0$, then:*

$$f \text{ is primitive polynomial} \Leftrightarrow d \sim 1$$

Definition 2.3.9 *$R[X]^* \ni f = a_nX^n + \cdots + a_0$, then:*

$$c(f) := \gcd(a_n, \cdots, a_0)$$

Proposition 2.3.10 *For any $f \in R[X]^*$:*

1. *$f = df_0$, where $d \in R^*$ and f_0 is primitive polynomial.*
2. *If $f = d_1f_1 = d_2f_2$, then $d_1 \sim d_2$ in R and $f_1 \sim f_2$ in $R[X]$.*

Proof. (1)

$$f = c(f)\sum_{i=0}^{n}\frac{a_i}{c(f)}X^i \wedge \gcd\left(\frac{a_0}{c(f)},\cdots,\frac{a_n}{c(f)}\right) = 1$$

(2) Suppose

$$a_1\left(\sum_{i=0}^{n}c_iX^i\right) = a_2\left(\sum_{i=0}^{n}d_iX^i\right)$$

where $\frac{a_2}{a_1} = \frac{p}{q} \wedge \gcd(p,q) = 1$, and both polynomials are primitive. It is equivalent to:

$$\begin{aligned}
&q\left(\sum_{i=0}^{n}c_iX^i\right) = p\left(\sum_{i=0}^{n}d_iX^i\right)\\
&\Rightarrow \forall i,\ qc_i = pd_i\\
&\Rightarrow \forall i,\ q|d_i \wedge p|c_i\\
&\Rightarrow p \sim 1 \wedge q \sim 1
\end{aligned}$$

□

Proposition 2.3.11 *R is UFD, and F is its fraction filed, then for $f_1, f_2 \in R[X]^*$, its holds that:*

$$f_1 \sim f_2 \text{ on } R[X] \Leftrightarrow f_1 \sim f_2 \text{ on } F[X]$$

Proof. See 丘维声 2015 p.156. ($\Rightarrow$): Obvious. ($\Leftarrow$): similar to Proposition 2.3.10. □

Lemma 2.3.12 *$f_1, f_2 \in R[X]$ are primitive polynomials, then f_1f_2 is primitive polynomial.*

Proof. See 李文威 2024 Lemma 6.9.4. □

Proposition 2.3.13 *Suppose $f \in R[X]$ where $\deg f > 0$ and is primitive polynomial. The following propositions are equivalent:*

1. *f is reducible in $F[X]$.*
2. *$f = f_1f_2$ in $R[X]$ where $\deg f_i > 0$ and each f_i is primitive polynomial.*

subsequently, the following propositionsa are equivalent:

i. f is irreducible in $F[X]$.

ii. There does not exists $f_1, f_2 \in R[X]$ where $\deg f_i > 0$ and is primitive polynomial, such that $f = f_1f_2$.

Proof. (1) $\Rightarrow$ (2): $f = g_1g_2 \in F[X]$ where $g_i \in F[X]^\times$. Notice that $F[X]^\times = F^\times = F^*$ and $g_i \notin fF^*$, which implies that $0 < \deg g_i < \deg f$. Apply Proposition 2.3.10, we have $f = k_1k_2 \underbrace{g_1'g_2'}_{\text{pp in } R[X]}$. Then by Proposition 2.3.11, $f = eg_1'g_2' = g_1g_2$.

(2) $\Rightarrow$ (1): Trival.

(i) $\Leftrightarrow$ (ii): Inverse negative proposition of (1) $\Leftrightarrow$ (2). □

Corollary 2.3.14 *primitive polynomial $f \in R[X]$ and $\deg f > 0$, the following propositions are equivalent:*

1. *f is irreducible in $R[X]$.*
2. *f is irreducible in $F[X]$.*

Proof. (2) $\Rightarrow$ (1): Suppose $f \in R[X]$ is reducible, so $f = f_1 f_2$ where $f_i \notin R[X]^\times \cup fR^\times \cup \{0_R\}$. Notice that if $f_1 \in R^* \setminus R^\times$ then f is not primitive polynomial. If $\deg f_1 = \deg f$. this implies that $\deg f_2 = 0$, which leads to a contradiction. In conclusion, $0 < \deg f_i < \deg f$. It follows that f is reducible in $F[X]$.

(1) $\Rightarrow$ (2): Assuming that f is reducible in $F[X]$. Applying Proposition 2.3.13, it immediatly follows that f is reducible in $R[X]$. □

Corollary 2.3.15 *Irreducible element in $R[X]$ can be devided into two classes:*

- *$\deg f = 0$: f is irreducible element in R.*
- *$\deg f > 0$: element that satisfies with the condition of Proposition 2.3.13 (ii).*

$f \in R[X]$ can be denoted as:

$$f = p_1^{e_1} \cdots p_s^{e_s}$$

where each p_i is irreducible element of $R[X]$. It follows that:

$$f' = \sum_{i=1}^{s} e_i p_i^{e_i - 1} p_i' \prod_{j \neq i} p_j^{e_j}$$

Further more:

$$\begin{aligned} p_i | f' &\Leftrightarrow p_i | e_i p_i^{e_i - 1} p_i' \prod_{j \neq i} p_j^{e_j} \\ &\Leftrightarrow p_i | e_i p_i^{e_i - 1} p_i' \text{ (This holds true when } e_i 1_R = 0 \vee p_i' = 0) \\ &\Leftrightarrow (p_i' = 0) \vee (p_i' \neq 0 \wedge e_i \geq 2) \end{aligned}$$

Thus we obtain that $p_i \nmid f' \Leftrightarrow p_i' \neq 0 \wedge e_i = 1$. Notice that

$$\gcd(f, f') = 1 \Leftrightarrow \begin{cases} f' \neq 0 \\ p_i' \nmid f' \end{cases}$$

Consequently, we have:

$$\gcd(f, f') = 1 \Leftrightarrow \begin{cases} f' \neq 0 \\ p_i' \neq 0 \wedge e_i = 1 \end{cases}$$

This indicates that when $p_i' \neq 0$, f has no repeated roots iff $\gcd(f, f') = 1$. In particular, if f split over R, $p_i' \neq 0$ natually holds, then f has no repeated roots iff $\gcd(f, f') = 1$.

2.4 Principle ideal domain

Theorem 2.4.1 (Chinese Remainder Theorem) *Suppose R is an ID, $a_1, \cdots, a_n \in R^*$ are pairwise coprime, $a = a_1 \cdots a_n$. There exists a ring isomorphism:*

$$\varphi : R/(a) \longrightarrow \prod_{i=1}^{n} R/(a_i)$$

$$r + (a) \longmapsto (r + (a_i))_{i=1}^{n}$$

Proof. The well-definedness and injectivity is easy to prove. Below is the proof of surjectivity. First, consider the case of $n = 2$. Since $\gcd(a_1, a_2) = 1$, there exists $x_1 \in (a_1), x_2 \in (a_2)$ such that $x_1 + x_2 = 1$. For any $r_1, r_2 \in R$, $r_1x_1 + r_1x_2 = r_1$ and $r_2x_1 + r_2x_2 + r_2$ hold. It can be verified that $\varphi(r_1x_2 + r_2x_1 + (a)) = (r_1 + (a_1), r_2 + (a_2))$.

For the case that $n \geq 3$, note that:

$$R/(a) \xrightarrow{\sim} R/(a_1 \cdots a_{n-1}) \times R/(a_n) \xrightarrow{\sim} \cdots$$

□

Proposition 2.4.2 *In PID, for any $r_1, \cdots, r_n \in R$:*

$$\langle r_1, \cdots, r_n \rangle = \gcd(r_1, \cdots, r_n)R$$

Proof.

$$\forall i \ d|r_i \Leftrightarrow \forall x \in \langle r_1, \cdots, r_n \rangle \ (d|x) \Leftrightarrow \forall x \in gR \ (d|x)$$

□

Proposition 2.4.3

$$\bigcap_{i=1}^{n}(r_i) = (\mathrm{lcm}(r_1, \cdots, r_n))$$

Proof.

$$\forall i \ (r_i|d) \Leftrightarrow d \in \bigcap_{i=1}^{n}(r_i) \Leftrightarrow d \in (m)$$

□

Chapter 3

Vector Space

3.1 Basis

V is F-vector space, $S \subset V$:

1. The linear combination of S is $\langle S\rangle := \{\sum_{\alpha\in S} k_\alpha \alpha\}$.
2. The linear relationship can be viewed as a function $k \in F^S$. All linear relationships on set S can be denoted as $\{k \in F^S : \sum_{\alpha\in S} k_\alpha \alpha = 0\}$.

   2.1 We say S is linearly independent iff $\{k \in F^S : \sum_{\alpha\in S} k_\alpha \alpha = 0\} = \{\mathcal{O}\}$.
3. S is the base of V iff (i) S is linearly independent; (ii) $\langle S\rangle = V$.

   3.1 $\forall v \in V$ can be uniquely denoted as $\sum_{\alpha\in S} k_\alpha \alpha$.

Proposition 3.1.1 *The following propositions are equivalent:*

1. *S is basis.*
2. *S is maximal linearly independent set.*
3. *S is minimal generating set.*

Proposition 3.1.2 *The following propositions are equivalent:*

1. *$\{w_1, \cdots, w_m\} \subset \langle v_1, \cdots, v_n\rangle \wedge m > n \Rightarrow \{w_i\}_{i=1}^m$ is linearly dependent set.*
2. *$\{w_1, \cdots, w_m\} \subset \langle v_1, \cdots, v_n\rangle \wedge \{w_1, \cdots, w_m\}$ is linearly independent $\Rightarrow m \leq n$.*

Theorem 3.1.3 *The following propositions are true:*

1. *Any F-vector space has basis.*
2. *Any basis of V has the same cardinality.*
3. *$T : V \overset{\sim}{\longmapsto} W$ is an isomophism, then B is the basis of V iff $T(B)$ is the basis of W.*

Proof. Zorn's Lemma and Axiom of Choise are equivalent propositions. We use Zorn's Lemma in this proof directly.

(1) Let S be a linearly independent set (it is permissible for$S = \varnothing$). Define set P as

$$P = \{T \subset V : S \subset T \wedge T \text{ is linearly independent set}\}$$

P, together with the subset relation $\subset$, forms a partially ordered set. Suppose T' is a chain contained in P, let $T_0 = \bigcup_{t \in T'} t$, it can be verified that T_0 is linearly independent set. Thus we have established that every chain in P has an upper bound. Applying Zonr's Lemma we get P contains an maximal element, which is precisely the basis of V.

(2) Suppose B, B' are two sets of basis for V. We first consider the case where $|B| < \aleph_0$ and denote $B = \{\beta_1, \cdots, \beta_n\}$. Since $B' \subset \langle \beta_1, \cdots, \beta_n \rangle$ and B' is linearly independent, $|B'|$ must smaller than n. To see this, suppose for contradiction that $|B'| > n$. Then there would exists $n+1$ elements in B' that also belong to $\langle \beta_1, \cdots, \beta_n \rangle$, implying that these elements are linearly dependent. By a similar argument, we obtain $|B| \leq |B'|$.

Now let $|B| \geq \aleph_0$, by the discussion above, we immediatly get $|B'| \geq \aleph_0$ as well. For any $\alpha \in B$, there exists a finite set B'_α that $\alpha \in \langle B'_\alpha \rangle$. Define $A = \bigcup_{\alpha \in B} B'_\alpha$. It can be verified that $V = \langle A \rangle$. We asser that $A = B'$. If not, there exists $\alpha' \in B' \setminus A$. Notice that $\alpha' \in \langle A \rangle$, so we have $\alpha' = \sum_{x \in A} k_x x$, where the equition $\alpha' - \sum_{x \in A} k_x x = 0$ is a non-trival linear relationship among the elements of B', which contradicts the property of the independence of B'. According to proposition 1.5.6, we get:

$$|B'| = \left| \bigcup_{\alpha \in B} B'_\alpha \right| \leq \left| \bigsqcup_{\alpha \in B} B'_\alpha \right| \leq |B \times \mathbb{Z}_{\geq 0}| = |B|$$

(3) ($\Rightarrow$): It is straitforward to verify that $T(S) \subset W$ is linearly independent and spans W. Furthermore, T^{-1} is also a isomophism, then proof of the reverse direction follows immediatly. □

Proposition 3.1.4 *B_i is set of basis of V_i. Let ι_i be the embedding mapping from V_i to $\bigoplus_{i \in I}^{\text{Ext}} V_i$. Then $\bigsqcup_{i \in I} \iota_i(B_i)$ is the basis of $\bigoplus_{i \in I}^{\text{Ext}}$.*

Proposition 3.1.5 *$V = \langle v_1, \cdots, v_m \rangle$, the following propositions are true.*

1. *V has basis.*
2. *$\exists n \in Z_{\geq 0}$ such that $\dim V = n \leq m$.*
3. *Any linearly independent set can be extended to basis.*
4. *Any spaning set can be reduced to basis.*

3.2 Direct Sum

Definition 3.2.1 *Let $(V_i)_{i \in I}$ be a series of F-vector space:*

1. $\prod_{i \in I} V_i := \left\{ \left[f : I \to \bigcup_{i \in I} V_i \right] : f(i) \in V_i \right\}$.

2. $\bigoplus_{i\in I}^{\text{Ext}} V_i := \left\{(v_i)_{i\in I} \in \prod_{i\in I} V_i : \textit{finite many } v_i \neq 0\right\}$

If V_i is the subspace of V:

1. $\sum_{i\in I} V_i := \left\{\sum_{i\in I} v_i \in V : v_i \in V_i \wedge \textit{finite many } v_i \neq 0\right\}$

We define σ as follows:

$$\begin{aligned}\sigma : \bigoplus_{i\in I}^{\text{Ext}} V_i &\to \sum_{i\in I} V_i \\ (v_i)_{i\in I} &\mapsto \sum_{i\in I} v_i\end{aligned}$$

It can be verified that σ is a well defined linear mapping, and is surjective. When σ is injective, the vector space in both sides are isomophic, in which case we use $\bigoplus_{i\in I} V_i$ to represent $\sum_{i\in I} V_i$. Additionally, the definition of external direct sum can be approached from two perspectives, as showed in the following formula:

$$\bigoplus_{i\in I}^{\text{Ext}} V_i = \bigoplus_{i\in I} \iota_i(V_i)$$

Proposition 3.2.2 *The following propositions are equivalent:*

1. *σ is injection.*
2. *$V_i \cap \sum_{j\in I\setminus\{i\}} V_j = \{0\}$.*
3. *Every $v \in \sum_{i\in I} V_i$ can be uniquely decomposited into the form $\sum_{i\in I} v_i$.*
4. *$0 \in \sum_{i\in I} V_i$ can be only decomposited into the form $0 + \cdots$*
5. *(V_i is finite dimentional sapce and I is finite set) $\dim(\sum_{i\in I} V_i) = \sum_{i\in I} \dim V_i$.*

Proof.

$$\begin{aligned}\sigma \text{ is injection} &\Leftrightarrow \left(\sum_{i\in I} v_i = \sum_{i\in I} w_i \Rightarrow (v_i)_{i\in I} = (w_i)_{i\in I}\right) \\ &\Leftrightarrow \left(\sum_{i\in I} (v_i - w_i) = 0 \Rightarrow (v_i - w_i)_{i\in I} = 0\right) \\ &\Leftrightarrow \left(\sum_{i\in I} a_i = 0 \Rightarrow (a_i)_{i\in I} = 0\right)\end{aligned}$$

We can extract the equivalence of the 1st, 3rd and 4th propositions from the above formula. Subsequently, we proceed to prove the equivalence between the 1st and 2nd propositions. Assuming that σ is injective, and that $\gamma \in V_i \cap \sum_{j\in I\setminus\{i\}} V_j$. It follows that $\gamma - \sum_{j\in I\setminus\{i\}} v_j = 0$, thereby concluding that $\gamma = 0$. For the converse, suppose that $\sum_{i\in I} v_i = 0$. Our goal is to show that $v_i = 0$. For any i, observe that $v_i + \sum_{j\in I\setminus\{i\}} v_j \in V_i \cap \sum_{j\in I\setminus\{i\}} V_j$, which implies that $v_i = 0$.

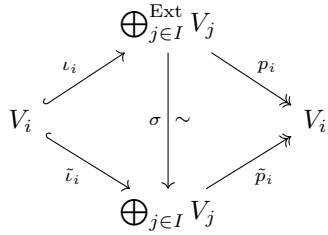
In the case of V_i is finite dimentional and I is finite. We have

$$\begin{aligned}\sigma \text{ is injection} &\Leftrightarrow \overset{\text{Ext}}{\bigoplus_{i\in I}} V_i \simeq \sum_{i\in I} V_i \\ &\Leftrightarrow \dim\left(\overset{\text{Ext}}{\bigoplus_{i\in I}} V_i\right) = \dim\left(\sum_{i\in I} V_i\right) \\ &\Leftrightarrow \sum_{i\in I}\dim V_i = \dim\left(\sum_{i\in I} V_i\right)\end{aligned}$$ □

When σ is isomophism, we define the series of functions as follows:

- $\iota_i : V_i \hookrightarrow \bigoplus_{j\in I}^{\text{Ext}} V_j : v \mapsto (v_j)_{j\in I}$ where $(v_i = v,\ v_j = 0)$.
- $\tilde{\iota}_i : V_i \hookrightarrow \bigoplus_{j\in I} V_j : v \mapsto v$.
- $p_i : \bigoplus_{j\in I}^{\text{Ext}} V_j \to V_i : (v_j)_{j\in I} \mapsto v_i$.
- $\tilde{p}_i = p_i\sigma^{-1} : \bigoplus_{j\in I} V_j \to V_i$

The diagram commutes:



Henceforth, we'll uniformly use use ι_i (or p_i) to represent either ι_i or $\tilde{\iota}_i$ (p_i or $\tilde{p}_i$) in the commutative diagram above. Therefore, the function ι_i (or p_i) will possesses two perspectives, and under the two perspectives, it will satisfies the following properties:

Corollary 3.2.3

1. $p_i\iota_i = \mathrm{id}_{V_i}$.
2. $p_j\iota_i = \mathcal{O}$ $(i \neq j)$.
3. *If I is finite, then* $\sum_{i\in I}\iota_i p_i = \mathrm{id}_{\bigoplus V_i}$

Corollary 3.2.4 *V is F-vector scpace. $P_1, \cdots, P_s \in \mathrm{End}(V)$ which satisfies that*

$$P_1 + \cdots + P_s = \mathrm{id},\ P_iP_j = \begin{cases} P_i & i = j \\ \mathcal{O} & i \neq j \end{cases}$$

then the following propositions are ture:

1. $V = \bigoplus_{1\le i\le s} \operatorname{Im} P_i$.
2. *P_i is the projection form V to* $\operatorname{Im} P_i$.

In particular, if $P \in \operatorname{End}(V)$ that satisfies $P^2 = P$, V has direct sum decomposition as:

$$V = \operatorname{Im} P_i \oplus \operatorname{Im}(\mathrm{id} - P_i)$$

When σ is isomophism and the objects in both ends of the linear mapping have direct sum decompositions, the diagram under 'inner perspective' can be copied into 'external perspective'. For instance, the following diagram demonstrates the copy of linear mapping T:

$$\begin{array}{ccc} \bigoplus_{j\in J} V_j & \xrightarrow{T} & \bigoplus_{i\in I} W_i \\ {\scriptstyle \sigma_1^{-1}}\downarrow\sim & & \sim\downarrow{\scriptstyle \sigma_2^{-1}} \\ \bigoplus^{\mathrm{Ext}}_{j\in J} V_j & \xrightarrow[T']{} & \bigoplus^{\mathrm{Ext}}_{i\in I} W_i \end{array}$$

where

$$T' : (v_j)_{j\in J} \mapsto \left(\sum_{j\in J} p_i^W T \iota_j^V v_j \right)_{i\in I} .$$

Under the 'external perspective' that ι_i is the embedding $V_i \hookrightarrow \bigoplus^{\mathrm{Ext}}_{j\in J} V_j$ and p_i is the corresponding projection, the following proposition is true:

Proposition 3.2.5 *There exists isomophism:*

$$\begin{array}{ccc} \operatorname{Hom}(\bigoplus^{\mathrm{Ext}}_{j\in J} V_j, \prod_{i\in I} W_i) & \xleftrightarrow{\sim} & \bigoplus^{\mathrm{Ext}}_{(i,j)\in I\times J} \operatorname{Hom}(V_j, W_i) \\ T & \longmapsto & (T_{i,j})_{(i,j)} := (p_i^W T \iota_j^V)_{(i,j)} \\ \left[f : (v_j)_{j\in J} \mapsto \left(\sum_{j\in J} T_{i,j} v_j \right)_{i\in I} \right] & \longmapsto & (T_{i,j})_{(i,j)} \end{array}$$

In particular, let V_j and W_i be subspaces of V, W respectively, and let I, J be finite sets. We obtain that

$$\operatorname{Hom}(\bigoplus^{\mathrm{Ext}}_{j\in J} V_j, \bigoplus^{\mathrm{Ext}}_{i\in I} W_i) \xleftrightarrow{\sim} \bigoplus^{\mathrm{Ext}}_{(i,j)\in I\times J} \operatorname{Hom}(V_j, W_i)$$

As depicted in the previous commutative diagram, this isomophism can be copied to 'inner perspective', namely:

$$\begin{array}{ccccc} T & \in & \operatorname{Hom}(\bigoplus^{\mathrm{Ext}}_{j\in J} V_j, \bigoplus^{\mathrm{Ext}}_{i\in I} W_i) & \xrightarrow[M]{\sim} & \bigoplus^{\mathrm{Ext}}_{(i,j)\in I\times J} \operatorname{Hom}(V_j, W_i) \\ \downarrow & & \downarrow\wr & \nearrow_{\sim} & \\ \sigma_2 T \sigma_1^{-1} & \in & \operatorname{Hom}(\bigoplus_{j\in J} V_j, \bigoplus_{i\in I} W_i) & & \end{array}$$

Furthermore, under the condition of compatible index set size, we can also define the "marix multiplication" of $(S_{i,j})_{(i,j)\in I\times J}$ and $(T_{j,k})_{(j,k)\in J\times K}$, that is:

$$\odot : \bigoplus\nolimits^{\text{Ext}}_{(i,j)\in I\times J} \operatorname{Hom}(V_j, W_i) \times \bigoplus\nolimits^{\text{Ext}}_{(j,k)\in J\times K} \operatorname{Hom}(U_k, V_j) \to \bigoplus_{(i,K)\in I\times K}^{\text{Ext}} \operatorname{Hom}(U_k, W_i)$$

$$((S_{i,j})_{(i,j)\in I\times J}, (T_{j,k})_{(j,k)\in J\times K}) \mapsto \left(\sum_{j\in J} S_{i,j}T_{j,k}\right)_{(i,k)\in I\times K}$$

Proposition 3.2.6 *The isomophism M preserves multiplication:*

$$M(\circ(S,T)) = \odot(M(S), M(T))$$

Proof.

$$\begin{aligned}(S\circ T)_{i,k} &= p^W_i\, ST\, \iota^U_k \\ &= p^W_i\, S\left(\sum_{j\in J} \iota^V_j\, p^V_j\right) T\, \iota^U_k \\ &= \sum_{j\in J} S_{i,j}T_{j,k}\end{aligned}$$

Finlly, we use the above isomophism to derive the definition of block matrixs and their multiplication. Let the index sets, I, J be finite. The conditions are listed as follows:

- $V = \bigoplus_{1\le j\le s} V_j,\ W = \bigoplus_{1\le i\le r} W_i$.
- $V_j = \langle \underline{\mathbf{v}}_j \rangle$ and $\underline{\mathbf{v}}_j = \{v_{j,1}, \cdots, v_{j,n_j}\}$.
- $W_i = \langle \underline{\mathbf{w}}_i \rangle$ and $\underline{\mathbf{w}}_i = \{w_{i,1}, \cdots, w_{i,m_i}\}$.
- $n_1 + \cdots + n_s = n$ and $m_1 + \cdots + m_r = m$.
- $\underline{\mathbf{v}}_1, \cdots, \underline{\mathbf{v}}_s$ arranged in order form a basis $\underline{\mathbf{v}}$ for V, and similarly for W, yielding a basis $\underline{\mathbf{w}}$.

Define mapping φ as:

$$\bigoplus_{\substack{1\le i\le r\\ 1\le j\le s}} \mathrm{M}_{m_i\times n_j}(F) \xrightarrow{\quad\varphi\quad} \mathrm{M}_{m\times n}(F)$$

$$(A_{i,j})_{\substack{1\le i\le r\\ 1\le j\le s}} \longmapsto \begin{bmatrix} A_{1,1} & \cdots & A_{1,s} \\ \vdots & & \vdots \\ A_{r,1} & \cdots & A_{r,s} \end{bmatrix}$$

Theorem 3.2.7 *The following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Hom}(\bigoplus_{j\in J} V_j, \bigoplus_{i\in I} W_i) & \xrightarrow{\sim} & \bigoplus_{(i,j)\in I\times J}^{\mathrm{Ext}} \mathrm{Hom}(V_j, W_i) \\ \mathcal{M}_{\underline{\mathbf{V}}}^{\underline{\mathbf{W}}} \downarrow \sim & & \sim \downarrow \mathcal{M}_{\underline{\mathbf{V}}_j}^{\underline{\mathbf{W}}_i} \\ \mathrm{M}_{m\times n}(F) & \xleftarrow[\sim]{\varphi} & \bigoplus_{(i,j)\in I\times J}^{\mathrm{Ext}} \mathrm{M}_{m_i\times n_j}(F) \end{array}$$

Proof.

$$\begin{aligned} Tv_{j,\mu} &= \sum_{i=1}^{r} p_i^W \iota_i^W T \iota_j^V (v_{j,\mu}) \\ &= \sum_{i=1}^{r} T_{i,j} v_{j,\mu} \\ &= \left[\sum_{\rho=1}^{m_1} (\mathcal{M}_{\underline{\mathbf{V}}_j}^{\underline{\mathbf{W}}_1}(T_{1,j}))_{\rho,\mu} w_{1,\rho}\right] + \cdots + \left[\sum_{\rho=1}^{m_r} (\mathcal{M}_{\underline{\mathbf{V}}_j}^{\underline{\mathbf{W}}_r}(T_{r,j}))_{\rho,\mu} w_{r,\rho}\right] \end{aligned}$$

Notice that the following array is exactly the corresponding row of $\mathcal{M}_{\underline{\mathbf{V}}}^{\underline{\mathbf{W}}}(T)$:

$$\left[(\mathcal{M}_{\underline{\mathbf{V}}_j}^{\underline{\mathbf{W}}_1}(T_{1,j}))_{1,\mu}, (\mathcal{M}_{\underline{\mathbf{V}}_j}^{\underline{\mathbf{W}}_1}(T_{1,j}))_{2,\mu}, \cdots, (\mathcal{M}_{\underline{\mathbf{V}}_j}^{\underline{\mathbf{W}}_r}(T_{r,j}))_{m_r,\mu}\right]$$

Arranging them will form a matrix as:

$$\begin{bmatrix} \mathcal{M}_{\underline{\mathbf{V}}_1}^{\underline{\mathbf{W}}_1}(T_{1,1}) & \cdots & \mathcal{M}_{\underline{\mathbf{V}}_s}^{\underline{\mathbf{W}}_1}(T_{1,s}) \\ \vdots & & \vdots \\ \mathcal{M}_{\underline{\mathbf{V}}_1}^{\underline{\mathbf{W}}_r}(T_{r,1}) & \cdots & \mathcal{M}_{\underline{\mathbf{V}}_s}^{\underline{\mathbf{W}}_r}(T_{r,s}) \end{bmatrix}$$

□

When the index set sizes of I, J, K are compatible, we can easily obtain the multiplication of blcok marixs, that is:

$$\mathcal{M}((ST)_{i,k}) = \mathcal{M}\left(\sum_{j\in J} S_{i,j}T_{j,k}\right) = \sum_{j\in J} \mathcal{M}(S_{i,j})\mathcal{M}(T_{j,k})$$

3.3 Linear Mapping

The mapping $\mathcal{M}$ preserves multiplication, which is represented as:

$$\mathcal{M}(\circ(S,T)) = \cdot(\mathcal{M}(S), \mathcal{M}(T))$$

The isomophism of the vector sapce at both ends of a linear mapping makes a copy of the mapping, represented as the diagram:

$$\begin{array}{ccc} V_1 & \xrightarrow{T} & W_1 \\ \wr \downarrow & & \downarrow \wr \\ V_2 & \xrightarrow[T']{} & W_2 \end{array}$$

Here are some common cases:

1. V, W are two vector spaces, $T \in \mathrm{Hom}(V, W)$. Under the isomophism that $V \simeq \mathrm{Hom}(F, V) : v \mapsto [k \mapsto k \cdot v]$ the following diagram commutes, where $T\circ$ maps f_v to $T \circ f_v$:

$$\begin{array}{ccc} V & \xrightarrow{\quad T \quad} & W \\ \wr\downarrow & & \downarrow\wr \\ \mathrm{Hom}(F, V) & \xrightarrow{T\circ} & \mathrm{Hom}(F, W) \end{array}$$

2. Conctinuing the above definitions, under the isomophism between $\mathrm{Hom}(F, V)$ and $\mathrm{M}_{n\times 1}(F)$, the diagram commutes, where $A\cdot$ maps x to $A \cdot x$:

$$\begin{array}{ccc} V & \xrightarrow{\quad T \quad} & W \\ \wr\downarrow & & \downarrow\wr \\ \mathrm{M}_{n\times 1}(F) & \xrightarrow{A\cdot} & \mathrm{M}_{m\times 1}(F) \end{array}$$

3. Given basis $\underline{\mathbf{v}}$ and $\underline{\mathbf{w}}$ of V, W, let $\varphi_{\underline{\mathbf{v}}}$ be the isomophism of V and F^n. The diagram commutes, where A maps $(x_i)_{i=1}^n$ to $(\sum_{j=1}^n a_{i,j}x_j)_{i=1}^m$:

$$\begin{array}{ccc} V & \xrightarrow{\quad T \quad} & W \\ \wr\downarrow & & \downarrow\wr \\ F^n & \xrightarrow{\quad A \quad} & F^m \end{array}$$

Definition 3.3.1 *$T \in \mathrm{Hom}(V, W)$, then T is invertible iff $\exists S \in \mathrm{Hom}(W, V)$, such that $ST = \mathrm{id}_V \wedge TS = \mathrm{id}_W$.*

Proposition 3.3.2 *T is invertible as a linear mapping iff T is linear and bijective.*

Proposition 3.3.3 *There exists bijection that:*

$$\{(v_i)_{i=1}^n : \textit{ordered basis}\} \xleftrightarrow{1:1} \{\varphi \in \mathrm{Hom}(F^n, V) : \textit{isomophic}\}$$

$$(v_i)_{i=1}^n \longmapsto [\varphi : (x_i)_{i=1}^n \mapsto \textstyle\sum_{i=1}^n x_i v_i]$$

$$(\varphi(e_i))_{i=1}^n \longmapsfrom \varphi$$

As the isomophism of finite dimentional space and its coordinate space, φ very commonly used.

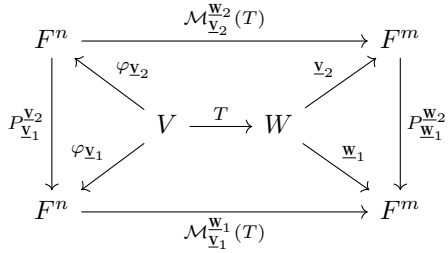
Proposition 3.3.4 *Given finite dimentional F-vector scpace V, W and their basis $\underline{\mathbf{v}}, \underline{\mathbf{w}}$. $T \in \mathrm{Hom}(V, W)$. Define $\varphi_{\underline{\mathbf{v}}}$ as the isomophism discussed above. Then the diagram commutes:*

$$\begin{array}{ccc} V & \xrightarrow{\quad T \quad} & W \\ \varphi_{\underline{\mathbf{v}}}\uparrow & & \uparrow\varphi_{\underline{\mathbf{w}}} \\ F^n & \xrightarrow[\mathcal{M}_{\underline{\mathbf{v}}}^{\underline{\mathbf{w}}}(T)]{} & F^m \end{array}$$

If $T = \mathrm{id}_V$ and $W = V$, we also use $P_{\underline{\mathbf{v}}_2}^{\underline{\mathbf{v}}_1}$ to represent $\mathcal{M}_{\underline{\mathbf{v}}_2}^{\underline{\mathbf{v}}_1}(T)$. It can be verified that

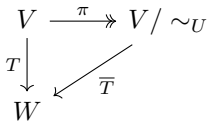
$$P_{\underline{\mathbf{v}}_2}^{\underline{\mathbf{v}}_1} P_{\underline{\mathbf{v}}_1}^{\underline{\mathbf{v}}_2} = P_{\underline{\mathbf{v}}_1}^{\underline{\mathbf{v}}_2} P_{\underline{\mathbf{v}}_2}^{\underline{\mathbf{v}}_1} = I_n$$
$$P_{\underline{\mathbf{v}}_2}^{\underline{\mathbf{v}}_3} P_{\underline{\mathbf{v}}_1}^{\underline{\mathbf{v}}_2} = P_{\underline{\mathbf{v}}_1}^{\underline{\mathbf{v}}_3}$$

Theorem 3.3.5 *Given V, W and thier ordered basis $\underline{\mathbf{v}}_1, \underline{\mathbf{v}}_2, \underline{\mathbf{w}}_1, \underline{\mathbf{w}}_2$, the following diagram commutes:*

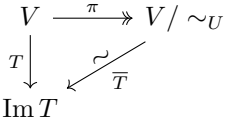


3.4 Quotient Space

Theorem 3.4.1 *Suppose $U \subset V$ is a subspace, $T \in \mathrm{Hom}(V, W)$. If $U \subset \operatorname{Ker} T$, there exists unique $\overline{T} \in \mathrm{Hom}(V/U, W)$ which makes the diagram commute:*

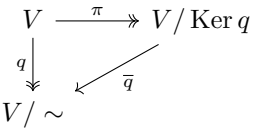


Conctinuing with the above conditions. If $\operatorname{Ker} T = U$, then $\overline{T}$ is isomophism that makes the diagram commute:



Proof. using Theorem **??** and Theorem **??**, and prove that $\overline{T}$ is linear. □

Theorem 3.4.2 *Given a vector space V endowed with a equivalence relation $\sim$, where $V/\sim$ forms a F-vector space, and $q : V \to V/\sim$ is its quotient mapping. Then $v_1 \sim v_2 \Leftarrow v_1 - v_2 \in \operatorname{Ker} q \Leftarrow v_1 \sim_{\operatorname{Ker} q} v_2$. The mapping $\overline{q}$ derived form theorem3.4.1 is actually identity, thereby ensuring the commutativity of the diagram below:*



Theorem 3.4.3 *Suppose U_1, U_2 are subspaces of V_1, V_2 respectively. $T \in \mathrm{Hom}(V_1, V_2)$ satisfies $T(U_1) \subset U_2$. Then there exists $\overline{T} \in \mathrm{Hom}(V_1/U_1, V_2/U_2)$, makes the diagram commute:*

$$\begin{array}{ccc} V_1 & \xrightarrow{T} & V_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ V_1/U_1 & \xrightarrow[\overline{T}]{} & V_2/U_2 \end{array}$$

Furthermore, the following diagram commutes if $T_1(U_1) \subset U_2 \wedge T_2(U_2) \subset U_3$:

$$\begin{array}{ccccc} V_1 & \xrightarrow{T_1} & V_2 & \xrightarrow{T_2} & V_3 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_3} \\ V_1/U_1 & \xrightarrow[\overline{T}_1]{} & V_2/U_2 & \xrightarrow[\overline{T}_2]{} & V_3/U_3 \end{array}$$

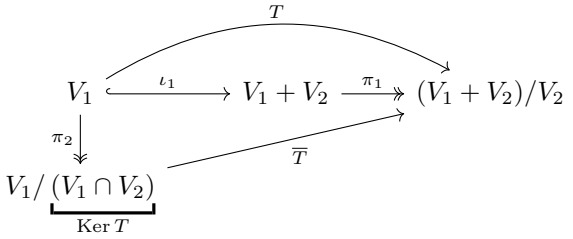
Proof. For the first case, $\pi_2 T$ is a linear mapping. Notice that $v \in \operatorname{Ker} \pi_2 T \Leftrightarrow Tv \in U_2$, thus $v \in U_1 \wedge T(U_1) \subset U_2 \Rightarrow v \in \operatorname{Ker} \pi_2 T$. Therefore $U_1 \subset \operatorname{Ker} \pi_2 T$, so we could apply theorem 3.4.1. □

Theorem 3.4.4 (1st Isomophism Theorem) *Suppose V_1, V_2 are subspace of V, there exists isomophism:*

$$V_1/(V_1 \cap V_2) \xrightarrow{\sim} (V_1 + V_2)/V_2$$

$$v_1 + (V_1 \cap V_2) \longmapsto v_1 + V_2$$

Proof.



Theorem 3.4.5 (2nd Isomophism Theorem) *Suppose $U \subset V$ is a subspace, then*

1 *There exists bijection:*

$$\{W \subset V : \text{ subspace containing } U\} \overset{1:1}{\longleftrightarrow} \left\{\overline{W} \subset \overline{V} : \text{ subspace}\right\}$$

$$W \longmapsto \pi(W)$$

$$\pi^{-1}(\overline{W}) \longmapsto \overline{W}$$

2 $W_1 \subset W_2 \Leftrightarrow \overline{W}_1 \subset \overline{W}_2$.

3 There exists isomophism:

$$V/W \xrightarrow{\sim} \overline{V}/\overline{W}$$

$$v + W \longmapsto (v + U) + (V/W)$$

Proof.

1 1.1 $\pi(W)$ is an element in prescribed set, and the mapping $W \mapsto \pi(W)$ is well defined.

1.2 $\pi^{-1}(\overline{W})$ is an element in prescribed set, and mapping $\overline{W} \mapsto \pi^{-1}(\overline{W})$ is well defined.

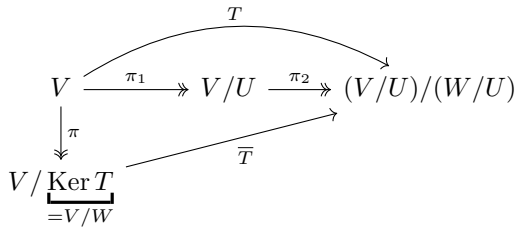
1.3 $W \mapsto \pi(W) \mapsto \pi^{-1}(\pi(W))$ is identity: Obviously $W \subset \pi^{-1}(\pi(W))$. For any $x \in \pi^{-1}(\pi(W))$, we have $\pi(x) \in \pi(W)$. Thus there exists $w \in W$ such that $x + U = w + U$. Hence $x - w \in U \subset W$.

1.4 $\overline{W} \mapsto \pi^{-1}(\overline{W}) \mapsto \pi(\pi^{-1}(\overline{W}))$ is identity: Obviously $\pi(\pi^{-1}(\overline{W})) \subset \overline{W}$. Assume $\overline{x} \in \overline{W}$, by the surjection of π, there exists $x \in V$ such that $\pi(x) = \overline{x}$, because of that $\overline{W} \subset \overline{V}$. It implies $x \in \pi^{-1}(\overline{W})$, thus $\overline{x} = \pi(x) \in \pi(\pi^{-1}(\overline{W}))$.

2 2.1 $W_1 \subset W_2 \Rightarrow \pi(W_1) \subset \pi(W_2)$.

2.2 $\overline{W}_1 \subset \overline{W}_2 \Rightarrow \pi^{-1}(\overline{W}_1) \subset \pi^{-1}(\overline{W}_2)$.

3



□

Theorem 3.4.6 *Suppose $U \subset V$ is a subspace. S_0 is a set of basis of U, and $\overline{S}_1$ is a set of basis of V/U. Let $g \in \prod_{\overline{a} \in \overline{S}_1} \pi^{-1}(\overline{a})$, and $S_1 = g(\overline{S}_1)$. The following propositions are ture:*

1. *S_1 is linearly independent set.*
2. *$\langle S_0 \rangle \cap \langle S_1 \rangle = \{0\}$.*
3. *$\langle S_0 \sqcup S_1 \rangle = \langle S_0 \rangle \oplus \langle S_1 \rangle = V$.*
4. *$\dim V = \dim U + \dim V/U$.*

Corollary 3.4.7 *If $V = U \oplus W$, then $W \simeq V/U$.*

Proof. Verify that $\pi|_W : w \mapsto w + U$ is bijection directly. □

Corollary 3.4.8 *For any subspace $U \subset V$, there exists W such that $V = U \oplus W$.*

Consider the diagram under the condition that $T(U_1) \subset U_2$:

$$\begin{array}{ccc} V_1 & \xrightarrow{T} & V_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ V_1/U_1 & \xrightarrow[\overline{T}]{} & V_2/U_2 \end{array}$$

The other assumtions are listed as follows:

1. $U_1 = \langle \underline{\mathbf{A}}_1 \rangle = \langle \alpha_1, \cdots, \alpha_r \rangle$.
2. $V_1/U_1 = \langle \underline{\mathbf{A}'}_2 \rangle = \langle \alpha'_{r+1}, \cdots, \alpha'_{r+n} \rangle$.
3. $U_2 = \langle \underline{\mathbf{B}}_1 \rangle = \langle \beta_1, \cdots, \beta_s \rangle$.
4. $V_2/U_2 = \langle \underline{\mathbf{B}'}_2 \rangle = \langle \beta'_{s+1}, \cdots, \beta'_{s+m} \rangle$.
5. Applying Theorem 3.4.6, we obtain the conplement space of U_i and thier basis, namely $W_1 = \langle \underline{\mathbf{A}}_2 \rangle = \langle \alpha_{r+1}, \cdots, \alpha_{r+n} \rangle$, $W_2 = \langle \underline{\mathbf{B}}_2 \rangle = \langle \beta_{s+1}, \cdots, \beta_{s+m} \rangle$.

Under the decomposition of $V_1 = U_1 \oplus W_1$ and $V_2 = U_2 \oplus W_2$, $\mathrm{Hom}(V_1, V_2)$ undergoes a decomposition, where each of its element T admits an equivalent form:

$$\begin{bmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{bmatrix}$$

Subsequently, we proceed to prove the following propositions:

1. $T_{21} = \mathcal{O}$.
2. $T_{11} = T|_{U_1}$.
3. $\mathcal{M}(T_{22}) = \mathcal{M}(\overline{T})$.

The 1st and 2nd proposition are easy to verify. Regarding the 3rd one, our inital conclusion is that the subsequent diagram commutes:

$$\begin{array}{ccc} V_1/U_1 & \xrightarrow{\overline{T}} & V_2/U_2 \\ {\scriptstyle \sigma_1 = \pi_1|_{W_1}}\uparrow & & \uparrow{\scriptstyle \sigma_2 = \pi_2|_{W_2}} \\ W_1 & \xrightarrow[\sigma_2^{-1}\overline{T}\sigma_1]{} & W_2 \end{array}$$

Suppose $w_1 \in W_1$, then we have

$$w_1 \overset{\sigma_1}{\longmapsto} w_1 + U_1 \overset{\overline{T}}{\longmapsto} Tw_1 + U_2 \overset{\sigma_2^{-1}}{\longmapsto} p_2^{V_2} T w_1 = p_2^{V_2} T \iota_2^{V_1} w_1 = T_{22} w_1$$

Thus $\sigma_2^{-1}\overline{T}\sigma_1 = T_{22}$. The rest work we need to do is to demonstrate that $\mathcal{M}(\sigma_2^{-1}) = I_m, \mathcal{M}(\sigma_1) = I_n$ and $\mathcal{M}(T_{22}) = \mathcal{M}(\sigma_2^{-1})\mathcal{M}(\overline{T})\mathcal{M}(\sigma_1) = \mathcal{M}(\overline{T})$, which is straitforward to prove.

Consequently, the matix of T under the prescribed basis has the form

$$\begin{bmatrix} \mathcal{M}(T|_{U_1}) & * \\ 0 & \mathcal{M}(\overline{T}) \end{bmatrix}$$

Bibliography

[Wik24] WikiPedia. Grothendieck universe. Website. 2024.

[丘 15] 丘维声. 近世代数. 北京大学出版社, 2015.

[李 19] 李文威. 代数学方法. 北京大学出版社, 2019.

[李 24] 李文威. 代数学讲义. 北京大学出版社, 2024.