Chapter 1

Set Theory

1.1 Ordinal

Proposition 1.1.1 *If α is an ordinal, then $\alpha \notin \alpha$.*

Proof. α is an ordinal if it is a transitive set and is well-ordered with respect to $\in$. Assume that $\alpha \in \alpha$ holds, then α is an element of itself. This lead to the contradiction $\alpha < \alpha$, which violate the property of tot-ordering that states $\alpha \leq \alpha \wedge \alpha \leq \alpha \Rightarrow \alpha = \alpha$.$\square$

Corollary 1.1.2 *If α is an ordinal, $\alpha + 1 := \alpha \cup \{\alpha\}$ is actually $\alpha \sqcup \{\alpha\}$.*

Lemma 1.1.3 *(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 $(\beta \setminus \alpha, \leq)$. It is clear that $\gamma \in \beta \setminus \alpha$. We assert that $\alpha = \{x \in \beta : x < \gamma\}$, where the latter is nothing more than γ. Here is the proof: Firstly, suppose $y \in \{x \in \beta : x < \gamma\} = \gamma$. If $y \notin \alpha$, then $y < \gamma \wedge y \in \beta \setminus \alpha$, thus making y the minimal element and contradicts our assumption. Therefore we established that $\gamma \subset \alpha$. Secondly, notice that $\gamma,\ \alpha$ are elements that comply with the well-ordering of β, and $\gamma \notin \alpha$, thus $\gamma \geq \alpha$. We only consider the case of $\alpha < \gamma$: due to the transitivity, $\forall x \in \alpha,\ x \in \alpha \wedge \alpha \in \gamma \Rightarrow x \in \alpha \subset \gamma \Rightarrow x \in \gamma$, therefore $\alpha \subset \gamma$.

(3): Let $\gamma = \alpha \cap \beta$, we assert that either $\gamma = \alpha$ or $\gamma = \beta$ must be true since $\gamma \in \alpha \wedge \gamma \in \beta \Rightarrow \gamma \in \gamma$. $\square$

Corollary 1.1.4 *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, and therefore* **On** *is well-ordered.)*

Proof. (step1) Firstly, we prove that $\bigcap C \in C$ is an ordinal. Let γ be $\bigcap C$. According to the Axiom schema of separation, $\bigcap C$ is a set. Choosing a $c_0 \in C$, then we have:

$$\begin{aligned} \text{for any arbitrary } x \in \gamma &\Leftrightarrow x \in c \ (\forall c \in C) \\ &\Rightarrow \gamma \subset c_0 \\ &\Rightarrow \gamma \text{ is well ordered} \end{aligned}$$

As for the transitivity, the proof is as follows:

$$\begin{aligned} \text{for any arbitrary } x \in \gamma &\Leftrightarrow x \in c \ (\forall c \in C) \\ &\Rightarrow x \subset c \ (\forall c \in C) \\ &\Rightarrow x \subset \gamma \end{aligned}$$

(step2) Next, we prove that $\bigcap C \in C$. Assume that $\gamma \notin C$, $\forall x \in \gamma \Rightarrow x \in c$ $(\forall x \in C)$, thus $\gamma \subset c \ \forall c \in C$, we also have $\gamma \neq c$ $(\forall c \in C)$ because $\gamma \notin C$. Combine these two conclusions clause (2) of 1.1.3, we get $\gamma \in c$ $(\forall c \in C)$. This implies $\gamma \in \bigcap C = \gamma$, which is impossible. □

Corollary 1.1.5 $\alpha \sqcup \{\alpha\} = \inf\{\beta : \beta > \alpha\} := \bigcap\{\beta : \beta > \alpha\}$.

Proof.

$$\begin{aligned} \forall x \in \alpha \sqcup \{\alpha\} &\Rightarrow x \in \alpha \vee x = \alpha \\ &\Rightarrow (\forall \beta > \alpha \Rightarrow \beta > x) \\ &\Rightarrow x \in \bigcap\{\beta : \beta > \alpha\} \end{aligned}$$ □

To prove the reverse containment, pursuant to lemma 1.1.3 we have $\forall x \in \mathbf{On} \wedge x \notin \alpha \sqcup \{\alpha\} \Rightarrow a \in x \Rightarrow x \in \{\beta : \beta > \alpha\}$. We now verify that $x \notin \bigcap\{\beta : \beta > \alpha\}$. Let γ be $\bigcap\{\beta : \beta > \alpha\}$, and assume that $x \in \gamma$. If $x = \gamma$, it makes $x = \gamma \in \gamma$. If $x \neq \gamma$, as discussed in 1.1.4, let γ be the minimal element of set $\{\beta : \beta > \alpha\}$.Suppose x is an element belongs to the same class but distinct from γ. The only posibility is that $\gamma \in x$, which leads to the contradiction.

Corollary 1.1.6 *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 $\mathbf{On}$, 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 $x \subset \bigcup S$. □

Proposition 1.1.7 *α is not a successor if and only if* $\forall x \in \alpha \Rightarrow x + 1 \in \alpha$.

1.2 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 1.2.1 (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 $\gamma < \beta < \gamma$. $\square$

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 $\mathbf{On}$ 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 1.2.2 (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:

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

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

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

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 $C = \theta$.

1.3 Cardinality

Proposition 1.3.1 *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 $\mathbb{Z}^2_{\geq 0} \to \mathbb{Z}_{\geq 0}$, 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 $\tilde{S} = A$. $\square$

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.

$$
\begin{tikzcd}
a \text{ is prime element} \arrow[r, shift left, "\textbf{A1}.\ R \text{ is ID}"] \arrow[d, leftrightarrow, "\textbf{A3}.\ R \text{ is ID}"'] & a \text{ is irreducible element} \arrow[l, shift left, "\textbf{A2}."] \arrow[d, shift left, "\textbf{A5}.\ R \text{ is PID}"] \\
(a) \text{ is prime ideal} & (a) \text{ is maximal ideal} \arrow[l, "\textbf{A6}.\ R \text{ is CR}"] \arrow[u, shift left, "\textbf{A4}.\ R \text{ is ID}"]
\end{tikzcd}
$$

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 $\Rightarrow \exists \gcd(a, b)$.

2.1.1 Proofs

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

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 $g|g_0$.

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. *$T : V \xrightarrow{\sim} W$ is an isomophism, then B is the basis of V iff $T(B)$ is the basis of W.*

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

(1) Let S be a linearly independent set ($S = \varnothing$ is allowed). We define set P as

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

P, together with the $\subset$, 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 has a maximal element, which is indeed the basis of V.

(2) Suppose B, B' are two sets of basis for V. We first consider the case of $|B| < \aleph_0$. We denote B as $\{\beta_1, \cdots, \beta_n\}$. Then $|B'|$ must smaller than n since $B' \subset \langle \beta_1, \cdots, \beta_n \rangle$ and B' is linearly independent. If not, asusming that $|B'| > n$. There exists $n + 1$ elements in B' that also belong to $\langle \beta_1, \cdots, \beta_n \rangle$, which implies these elements are dependent, contradicting the facts that B' is linearly independent set. Using the same method, we obtain that $|B| \le |B'|$.

Now let $|B| \ge \aleph_0$, by the discussion above, we immediatly get $|B'| \ge \aleph_0$ as well. For any $\alpha \in B$, there exists a finite set B'_α that $\alpha \in \langle B'_\alpha \rangle$. Let A be $\bigcup_{\alpha \in B} B'_\alpha$. It can be verified that $V = \langle A \rangle$. We asser that $A = B'$. If not, there exists $\alpha' \in B' \smallsetminus A$. Notice that $\alpha' \in \langle A \rangle$, thus we have $\alpha' = \sum_{x \in A} k_x x$, where the equition $\alpha' - \sum_{x \in A} k_x x = 0$ is a nontrival linear relationship on set B', contradicts the property of independence. According to proposition 1.3.1, we get:

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

(3) ($\Rightarrow$): It is easy to verify that $T(S) \subset W$ is linearly independent and spans W. On the other hand, T^{-1} is also a isomophism, then proof of the reverse direction is clear. $\square$

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. *$\exists n \in Z_{\ge 0}$ such that $\dim V = n \le m$.*
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. *$V_i \cap \sum_{j\in I\smallsetminus\{i\}} V_j = \{0\}$.*
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. Next, we prove the equivalence of the 1st and 2nd propositions. Assuming that σ is injective, and that $\gamma \in V_i \cap \sum_{j\in I\smallsetminus\{i\}} V_j$. It follows that $\gamma - \sum_{j\in I\smallsetminus\{i\}} v_j = 0$, thus $\gamma = 0$. For re the reverse direction, suppose that $\sum_{i\in I} v_i = 0$, we want to demonstrate that $v_i = 0$. For any i, we have $v_i + \sum_{j\in I\smallsetminus\{i\}} v_j \in V_i \cap \sum_{j\in I\smallsetminus\{i\}} V_j$, which implies that $v_i = 0$.

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

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

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

And the diagram commutes:

$$\begin{tikzcd}
& \bigoplus_{j\in I}^{\text{Ext}} V_j \arrow[dr, two heads, "p_i"] \arrow[dd, "\sigma"', "\sim"] & \\
V_i \arrow[ur, hook, "\iota_i"] \arrow[dr, hook, "\tilde{\iota}_i"'] & & V_i \\
& \bigoplus_{j\in I} V_j \arrow[ur, two heads, "\tilde{p}_i"'] &
\end{tikzcd}$$

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:

$$\begin{tikzcd}
\bigoplus_{j \in J} V_j \arrow[r, "T"] \arrow[d, "\sigma_1^{-1}"', "\sim"] & \bigoplus_{i \in I} W_i \arrow[d, "\sim"', "\sigma_2^{-1}"] \\
\bigoplus^{\mathrm{Ext}}_{j \in J} V_j \arrow[r, "T'"'] & \bigoplus^{\mathrm{Ext}}_{i \in I} W_i
\end{tikzcd}$$

where

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

Next, we get a closer look of the transformation of T.

We first prove the following proposition 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.

Proposition 3.2.5 *There exists isomophism:*

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

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

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

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

$$\begin{tikzcd}
T \arrow[d, mapsto] & \in & \operatorname{Hom}(\bigoplus^{\mathrm{Ext}}_{j \in J} V_j, \bigoplus^{\mathrm{Ext}}_{i \in I} W_i) \arrow[r, "\sim", "M"'] \arrow[d, "\wr"] & \bigoplus^{\mathrm{Ext}}_{(i,j) \in I \times J} \operatorname{Hom}(V_j, W_i) \\
\sigma_2 T \sigma_1^{-1} & \in & \operatorname{Hom}(\bigoplus_{j \in J} V_j, \bigoplus_{i \in I} W_i) \arrow[ur, "\sim"] &
\end{tikzcd}$$

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:

$$\begin{aligned}\odot : \bigoplus^{\text{Ext}}_{(i,j)\in I\times J} \operatorname{Hom}(V_j, W_i) \times \bigoplus^{\text{Ext}}_{(j,k)\in J\times K} \operatorname{Hom}(U_k, V_j) &\to \bigoplus^{\text{Ext}}_{(i,K)\in I\times K} \operatorname{Hom}(U_k, W_i)\\ ((S_{i,j})_{(i,j)\in I\times J}, (T_{j,k})_{(j,k)\in J\times K}) &\mapsto \left(\sum_{j\in J} S_{i,j}T_{j,k}\right)_{(i,k)\in I\times K}\end{aligned}$$

Proposition 3.2.6 *The isomophism M preserves multiplication:*

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

Proof.

$$\begin{aligned}(S\circ T)_{i,k} &= p_i^W ST\iota_k^U\\ &= p_i^W S\left(\sum_{j\in J}\iota_j^V p_j^V\right)T\iota_k^U\\ &= \sum_{j\in J} S_{i,j}T_{j,k}\end{aligned}$$

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 $\underline{\mathbf{w}}$.

We define mapping φ as:

$$\begin{aligned}\bigoplus_{\substack{1\le i\le r\\ 1\le j\le s}} \mathrm{M}_{m_i\times n_j}(F) &\xrightarrow{\quad\varphi\quad} \mathrm{M}_{m\times n}(F)\\ (A_{i,j})_{\substack{1\le i\le r\\ 1\le j\le s}} &\longmapsto \begin{bmatrix} A_{1,1} & \cdots & A_{1,s}\\ \vdots & & \vdots\\ A_{r,1} & \cdots & A_{r,s}\end{bmatrix}\end{aligned}$$