Thinking and Method of FAA

Jiete XUE

Otctober 7, 2025 - October 31, 2025

Contents

1 Basic Logic

Iff. $P = Q = \neg R$ =True, $P \Rightarrow (Q \Rightarrow R)$ is False. This is equivalent to $(P \wedge Q) \Rightarrow R$. So in `LEAN 4`, you can see a goal in the form

$$a \to b \to c \to \dots,$$

then you can use *intro* to get props. They have the relation *and* logically.

2 Set Theory

Definition 2.4.1 defines quantifiers, by 2.6.3 and 2.7.4 , we can use set to understand quantifiers. Let us first consider

$$\forall x \in X, \forall y \in Y, P(x, y). \tag{2.1}$$

That is

$$X = \{x \in X \mid \forall y \in Y, P(x, y)\} = \bigcap_{y \in Y} \{x \in X \mid P(x, y)\}. \tag{2.2}$$

That means

$$\forall y \in Y, \ X \subseteq \{x \in X \mid P(x, y)\}. \tag{2.3}$$

Thus,

$$\forall y \in Y, X = \{x \in X \mid P(x, y)\}, \tag{2.4}$$

equivalent to

$$\forall y \in Y, \forall x \in X, P(x, y). \tag{2.5}$$

But if we consider

$$\forall x \in X, \exists y \in Y, P(x, y), \tag{2.6}$$

the situation becomes

$$X = \bigcup_{y \in Y} \{x \in X \mid P(x, y)\} \tag{2.7}$$

The union equals to X does not give enough information. Similarly, $\exists, \forall, \dots$ can't go farther, too[1]. But

$$\exists x \in X, \exists y \in Y, P(x, y) \tag{2.8}$$

is equivalent to

$$\bigcup_{y \in Y} \{x \in X \mid P(x, y)\} \neq \varnothing. \tag{2.9}$$

That means

$$\exists y \in Y, \{x \in X \mid P(x, y)\} \neq \varnothing. \tag{2.10}$$

Thus,

$$\exists y \in Y, \exists x \in X, P(x, y). \tag{2.11}$$

[1] The intersection is not empty leads to any sets is not empty, but it is not equivalent, $\exists x \in X, \forall y \in Y, P(x, y) \Rightarrow \forall y \in Y, x \in X, P(x, y)$.

3 Correspondence

For the similar reason, if f is a correspondence, then

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f\left(A_i\right), \tag{3.1}$$

$$f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f\left(A_i\right). \tag{3.2}$$

If in addition, f is injective, then

$$f\left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} f\left(A_i\right). \tag{3.3}$$

A conclusion: Let f, g be correspondences, if $f \circ g = \mathrm{Id},\ g \circ f = \mathrm{Id}$, then f is a bijection and $f^{-1} = g$.

4 Ordering

Forgettable concepts: Well-ordered set 4.7.1, Order-complete 4.8.1

Problem 4.1 (Eg.)

$$m := \inf(A^{\mathrm{u}}) \in A^{\mathrm{u}}.$$

Proof. By definition, we only need to prove $\forall x \in A,\ x \leq m$. m is the max element in $(A^{\mathrm{u}})^{l}$, then we only need to prove $\forall x \in A,\ x \in (A^{\mathrm{u}})^{\mathrm{l}}$. It is easy to check.

□

The power set with $\subseteq$ forms a order-complete partially ordered set. If we want to construct a order-complete partially ordered set, we may consider build a relation between them. Knaster-Tarski fixed point theorem tell us a property of monotonic functions, and Dedekind-MacNeille theorem tell us how to do in detail.

5 Rings and Modules

Definition 5.1 (Unitary Ring)
A set A with "+"[1] (communicative group), "$*$" (monoid[2]), and distributivity forms a unitary ring.

The homomorphism of unitary rings is the combination of groups and monoids.

Definition 5.2 (Division Ring & Field)
Let K be a unitary ring. We denote by $K^\times$ the invertible elements of $(K, \cdot)$. If $K^\times = K \backslash \{0\}$ then we say that K is a division ring. If in addition, K is commutative, then we say that K is a **field**.

Definition 5.3 (Actions)
Set X, monoid G, We call **left action** of G on X any mapping

$$\phi : G \times X \to X,$$

such that
(1) $\phi(e, x) = x$, for any $x \in X$.
(2) $\forall (a, b) \in G \times G, \forall x \in X$,

$$\phi(a * b, x) = \phi(a, \phi(b, x)).$$

If we let G be a group, then we get a equivalent relation like orbit[3].

Definition 5.4 (Modules)
K: unitary ring. $(V, +)$: abelian group. We call a **left K-module structure** any left action of $(K, \cdot)$ on V.

$$\phi : K \times V \longrightarrow V$$

(1) $\forall (a, b) \in K \times K, \forall x \in V$,

$$\phi(a + b, x) = \phi(a, x) + \phi(b, x).$$

(2) $\forall a \in K$, $\forall (x, y) \in V \times V$,

$$\phi(a, x + y) = \phi(a, x) + \phi(a, y).$$

$(V, +)$ equipped with a left K-module structure is called a **left K-module**. If K is communitative, left and right K-modules structures have the same axioms: K-module structures. Left and right K-modules structures: K-modules. If K is a field, a K-module is called a **vector space** over K.

[1] "+" usually equipped with communicative law. So we say a communicative unitary ring means the "$*$" is communicative, in addition.
[2] "Unitary" refer to the unitary element.
[3] Denote as $\mathrm{orb}_\phi(x)$.

Definition 5.5 (Sub-K-modules)
V: left K-module, we call **left sub-K-module** of V any subgroup W of $(V,+)$ if $\forall(a,x) \in K \times W, ax \in W$. (resp. right.)

Definition 5.6 (Homomorphism)
E, F be left-K-modules. We call **homomorphism of left K-modules from** E **to** F any mapping $f : E \to F$, such that
(1) f is a homomorphism of groups from $(E,+)$ to $(F,+)$.
(2) For any $(a,x) \in K \times E, f(ax) = af(x)$.
If K is communitative, also called a K**-linear mapping**.

Definition 5.7 (Ideal)
Let A be a unitary ring. If a subset I of A is a left sub-A-module of A and a right sub-A-module of A, then we call I a **ideal** of A. If I is an ideal of A, then the composition laws of A define by passing to quotient a structure of unitary ring on the quotient mapping A/I. So that A/I becomes a quotient ring of A.

Definition 5.8 (Principal Ideal)
Let A be a communitative unitary ring. If an ideal of A is of the form

$$Ax : \{ax \mid a \in A\} \text{ with } x \in A.$$

We say that it is a **principal ideal**. If all ideals of A are principal, we say that A is a **principal ideal ring**.

Definition 5.9
Let V be a left K-module. For any family $\underline{x} := (x_i)_{i \in I} \in V^I$, we denote by

$$\varphi_{\underline{x}} : K^{\oplus I} \longrightarrow V$$

the homomorphism sending $(a_i)_{i\in I}$ to $\sum_{i \in I} a_i x_i$.
(1) $\mathrm{Im}\left(\varphi_{\underline{x}}\right)$ is a left K-submodule of V, called the **left sub-K-module generated by** $\underline{x}$, denote as $\mathrm{Span}_K\left((x_i)_{i\in I}\right)$. If φ_x is surjective, we say that $(x_i)_{i\in I}$ is a **system of generators** of V. $(\forall y \in V, \exists (a_i)_{i\in I} \in K^{\oplus I}, y = \sum_{i\in I} a_i x_i)$
Elements of $\mathrm{Span}_K\left((x_i)_{i\in I}\right)$ are called **K-linear combinations** of $(x_i)_{i\in I}$.
(2) If $\varphi_{\underline{x}}$ is injective, we say that $(x_i)_{i\in I}$ is **K-linearly independent**. $(\forall (a_i)_{i\in I} \in K^{\oplus I}, \sum_{i\in I} a_i x_i = 0 \to a_i = 0, \forall i \in I)$
(3) If $\varphi_{\underline{x}}$ is an isomorphism, we say $(x_i)_{i\in I}$ is a **basis** of V. If V has at least a basis, we say that V is a **free left K-module**. If V has a system of generators $(x_i)_{i\in I}$ such that I is finite, we say that V is **finitely generated**, or is **finite types**.

Definition 5.10 (Rank)
Let K be a division ring and V is a left K-module of finite type. We denote by $\mathrm{rk}(V)$ the least cardinality of the bases V, called the **rank** of V. If K is a field, then $\mathrm{rk}(V)$ is also denoted as $\dim(V)$, called the **dimension** of V. If $f : W \longrightarrow V$ is a homomorphism of left K-modules, the rank of f is defined as the rank of $\mathrm{Im}(f)$, denoted as $\mathrm{rk}(f)$.

Definition 5.11 (Algebra)
Let K be a communicative unitary ring. If A is a K-module equipped with a composition law

$$A \times A \longrightarrow A,$$

$$(a, b) \longmapsto ab.$$

such that $(A, +, \cdot)$ forms a unitary ring, such that

$$\forall \lambda \in K, \forall (a, b) \in A \times A,\ \lambda (ab) = (\lambda a) b = a (\lambda b).$$

Then we say that A is a **K-Algebra**.

Definition 5.12 (Sub-algebra)
Let A be a K-algebra. If B is a subset of A which is a sub-K-module and a unitary subring of A, we say that B is a **sub-K-algebra** of A.

Theorem 5.1 (Rank–Nullity Theorem)
$A : V \longrightarrow W$, $\dim(V) = n,\ \dim(W) = m,\ A \in M_{m,n}$,

$$n = \dim(\ker(A)) + \dim(\mathrm{Im}(A)).$$

6 Filters

Definition 6.1
Let X be a set. We call **filter** on X any non-empty subset $\mathcal{F}$ of $\wp(X)$ this satisfies:
(1) $\forall (V_1, V_2) \in \mathcal{F}^2, V_1 \cap V_2 \in \mathcal{F}$.
(2) $\forall V \in \mathcal{F}, \forall W \in \wp(X)$, if $V \subseteq W$, then $W \in \mathcal{F}$.

Definition 6.2
Let S be a subset of $\wp(X)$. We denote by $\mathcal{F}_S$ the intersection of all filters containing S. It is thus the least filter containing S. We call it the filter generated by S.

Definition 6.3
We say that a subset S of $\wp(X)$ is a **filter basis** if, for any $(A, B) \in S \times S$, there exists $C \in S$, such that $C \subseteq A \cap B$.[1]

If S is a filter basis, then

$$\mathcal{F}_S = \{U \in \wp(X) \mid \exists A \in S, A \subseteq U\}.$$

If S is a subset of $\wp(X)$, then

$$\mathcal{B}_S := \{A_1 \cap \cdots \cap A_n \mid n \in \mathbb{N},\ (A_1, \ldots, A_n) \in S^n\}$$

is a filter basis containing S. Moreover, $\mathcal{F}_S = \mathcal{F}_{\mathcal{B}_S}$.

[1] If $n \in \mathbb{N}_{\geq 1}$ and $(A_1, \ldots, A_n) \in S^n, \exists C \in S$ such that $C \subseteq A_1 \cap \cdots \cap A_n$.

Definition 6.4
Let X be a set and $f : X \longrightarrow G$ be a mapping. For any $U \in \wp(X)$, we define

$$f^s(U) := \sup_{x \in U} f(x) = \sup f(U).$$

$$f^i(U) := \inf_{x \in U} f(x) = \inf f(U).$$

If $U \neq \varnothing$, $f^s(U) \geq f^i(U)$. Let $\mathcal{F}$ be a filter on X. We define

$$\limsup_{\mathcal{F}} f := \inf_{U \in \mathcal{F}} f^s(U).$$

$$\liminf_{\mathcal{F}} f := \sup_{U \in \mathcal{F}} f^i(U).$$

They are called the **superior limit** and the **inferior limit** of f along $\mathcal{F}$. If

$$\liminf_{\mathcal{F}} f = \limsup_{\mathcal{F}} f,$$

we say that f has a limit along $\mathcal{F}$, and we denote $\lim_{\mathcal{F}} f$ this value.

Definition 6.5
Let $(G, *)$ be a group, and $\leq$ be a partial order on G. If

$$\forall (a, b, c) \in G^3, a < b \Rightarrow a * c < b * c \text{ and } c * a < c * b,$$

we say that $(G, *, \leq)$ is a **partially ordered group**. If in addition $\leq$ is a total order, we say that $(G, *, \leq)$ is a **totally ordered group**. (Resp. semigroup, monoid.)