Algebra : Chapter 0

Leven Huang

July 8, 2024

Abstract

This is my notes on the book *Algebra : chapter 0* by Aluffi. The book is a modern introduction to abstract algebra, and it is suitable for self-study.

Contents

Chapter 1

Preliminaries: Set theory and categories

1.1 Naive Set Theory

1.1.1 Sets

一个 set 由它所包含无序的、无重复的 *elements* 决定。set 的一个变种是 'multiset'，它的 elements 允许重复，正确定义一个 multiset 的方式是使用 *functions*。

一些有名的 sets：

- $\emptyset$：空集；
- $\mathbb{N}$：自然数集；
- $\mathbb{Z}$：整数集；
- $\mathbb{Q}$：有理数集；
- $\mathbb{R}$：实数集；
- $\mathbb{C}$：复数集。

另外，用 *singleton* 表示只有一个元素的 set。

下面是一些有用的符号（称为 *quantifiers*）：

- $\exists$: 存在；
- $\forall$: 对所有；
- $\exists!$: 存在唯一。

1.1.2 Inclusion of sets

我们用 $S \subseteq T$ 来表示 S 是 T 的子集。

1.1.3 Operations between sets

- $\cup$: 并集；
- $\cap$: 交集；
- $\setminus$: 差集；
- $\coprod$: 对称差；
- $\times$: 笛卡尔积;
- 'quotient by an equivalence relation'.

1.1.4 Equivalence relations, partitions, quotients

Definition 1.1.1 (Equivalence relation). An *equivalence relation* on a set S is a relation $\sim$ satisfying the following properties:

- *Reflexivity*: $a \sim a$ for all $a \in S$;
- *Symmetry*: if $a \sim b$, then $b \sim a$;
- *Transitivity*: if $a \sim b$ and $b \sim c$, then $a \sim c$.

Definition 1.1.2 (Quotient). The *quotient* of a set S with respect to an equivalence relation $\sim$ is the set

$$S/\sim := \mathscr{P}_{\sim}$$

of equivalence classes of elements of S with respect to $\sim$.

Example. 令 $S = \mathbb{Z}$，并定义关系 $\sim$ 为

$$a \sim b \Leftrightarrow a - b \text{ is even.}$$

于是 $\mathbb{Z}/\sim$ 由两个等价类组成：

$$\mathbb{Z}/\sim = \{[0]_{\sim}, [1]_{\sim}\}$$

1.2 Functions between sets

1.2.1 Definition

sets 之间使用 functions 进行交互，function $f : A \to B$ 的所有信息就是 *which element b of B is the image of any given element of a of A*，这些信息相当于一些二元组的集合，即：

$$\Gamma_f := \{(a, b) \in A \times B \mid b = f(a)\} \subseteq A \times B$$

而集合 Γ_f 通常被称为 f 的 *graph*。

为了满足函数的定义，集合 Γ_f 需要满足下列约束：

$$(\forall a \in A)\,(\exists! b \in B) \quad (a, b) \in \Gamma_f$$

我们声明 f 是从 A 到 B 的函数，通常记作 $f : A \to B$，也可以画成下图（‘diagram’）的形式：

$$A \xrightarrow{f} B$$

对于任意 $a \in A$，我们记作：

$$a \mapsto f(a).$$

如果 S 是 A 的子集，我们可以定义 $f(S)$ 为：

$$f(S) := \{b \in B \mid (\exists a \in A)\, b = f(a)\}.$$

也就是说，$f(S)$ 是包含所有 S 中的 elements 的像的集合。最大的这样的集合是 $f(A)$，也记为 $\operatorname{Im} f$。

另外，我们用 $f|_S$ 表示将 f 限制在 S 上的函数：即 function $S \to B$ defined by

$$(\forall s \in S) : f|_S(s) = f(s).$$

Note. $f(S) = \operatorname{Im}(f|_S)$.

1.2.2 Examples: Multisetsm, indexed sets

Example (Multiset). 我们用一个 function 来定义 multiset，一种可能的方法是使用一个 function $f : A \to \mathbb{N}^*$，其中 A 是一个集合。这样，$f(a)$ 就是 a 在 multiset 中的重复次数。

Example (Indexed set). 同样使用 function 来得到一个 indexed set。将集合 I 看作下标，我们可以用一个 function $f : I \to A$ 来给 $\mathrm{Im}(I) \subseteq A$ 中的每个元素一个序号，从而得到一个 indexed set.

1.2.3 Composition of functions

functions 可以被组合，即给定两个 functions $f : A \to B$ 和 $g : B \to C$，我们可以定义它们的 *composition* $gf : A \to C$ 为：

$$(\forall a \in A) \quad (g \circ f)(a) := g(f(a))$$

用 diagram 的形式表示为：

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

我们称上图 *commutes* 或是 *commutative* 的，表示无论 A 从那条路径到 C，得到的结果都是一样的。

Note (Associativity). composition 是 *associative* 的，即对于任意三个 functions $f : A \to B, g : B \to C, h : C \to D$，有 $h \circ (g \circ f) = (h \circ g) \circ f$. 在 diagram 中表示为：

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & B \arrow[r, "g"] \arrow[rr, bend left, "h\circ g"] & C \arrow[r, "h"] & D \end{tikzcd}$$

1.2.4 Injections, surjections, bijections

- *Injection*: $f : A \to B$ is an *injection* if for all $a, a' \in A$, $f(a) = f(a')$ implies $a = a'$.
- *Surjection*: $f : A \to B$ is a *surjection* if for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.
- *Bijection*: $f : A \to B$ is a *bijection* if it is both an injection and a surjection.

injections 通常画作 $\hookrightarrow$，surjections 通常画作 $\twoheadrightarrow$.

如果 f 既是 injection 又是 surjection，我们称 f 是 *bijective* 的（或称之为一个 *bijection* 或 *one to one correspondence* 或 *isomorphism of sets*），写作 $f : A \xrightarrow{\sim} B$ 或

$$A \cong B,$$

此时我们称 A 和 B 是 '*isomorphic*' sets.

1.2.5 Injections, surjections, bijections: Second viewpoint

回顾前面对 Γ_f 的约束，我们希望定义一个函数 $g : B \to A$，使得 $\forall a \in A, \exists b \in B, s.t. f(a) = b \Rightarrow g(b) = a$，当 f 是 surjection 时，Γ_g 满足约束中的 $\forall b \in B$；当 f 是 injection 时，Γ_g 满足约束中的 $\exists! a \in A$。也就是说，当 f 是 bijection 时，存在唯一的函数 g 是 f 的逆函数。

从图形上看，g 有一个有趣的性质，即下面的图形是 commutative 的：

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "\mathrm{id}_A"'] & B \arrow[r, "g"] & A \end{tikzcd} \qquad \begin{tikzcd} B \arrow[r, "g"] \arrow[rr, bend right, "\mathrm{id}_B"'] & A \arrow[r, "f"] & B \end{tikzcd}$$

Proposition 1.2.1. Assume $A \neq \emptyset$, and let $f : A \to B$ be a function. Then

1. f has a left-inverse if and only if f is injective.

2. f has a right-inverse if and only if f is surjective.

Corollary 1.2.1. A function $f : A \to B$ is a bijection if and only if it has a (two-sided) inverse.

1.2.6 Monomorphisms and epimorphisms

monomorphisms 和 epimorphisms 是 category theory 中的概念，可以用更图形化的视角来看待 injectivity 和 surjectivity.

A function $f : A \to B$ is called a *monomorphism(monic)* if for any sets Z and functions $\alpha', \alpha'' : Z \to A$, $f \circ \alpha' = f\alpha''$ implies $\alpha' = \alpha''$.

Proposition 1.2.2. A function is injective if and only if it is a monomorphism.

类似的，epimorphisms 则对应 surjectivity.

1.2.7 Basic examples

Example (Natural projections). 令 A, B 为非空集合，则 *natural projections* π_A, π_B:

$$\begin{tikzcd} & A \times B \arrow[dl, two heads, "\pi_A"'] \arrow[dr, two heads, "\pi_B"] & \\ A & & B \end{tikzcd}$$

被定义为 $\pi_A(a, b) := a, \pi_B(a, b) := b, \forall (a, b) \in A \times B$。这两个映射都是 surjections.

Example (Natural injections). 类似的，有 natural injections from A and B to the disjoint union $A \coprod B$:

$$\begin{tikzcd} A \arrow[dr, hook] & & B \arrow[dl, hook'] \\ & A \coprod B & \end{tikzcd}$$

即将 $a \in A$ 映射到 $(a, 0) \in A \coprod B$，将 $b \in B$ 映射到 $(b, 1) \in A \coprod B$.

Example (Canonical projection). 假设 $\sim$ 是集合 A 上的等价关系，于是有（surjective）canonical projection:

$$A \twoheadrightarrow A/\sim$$

即将 $a \in A$ 映射到它的等价类 $[a]_\sim$.

1.2.8 Canonical decomposition

We define an equivalence relation $\sim$ on set A as follows: for all $a', a'' \in A, a' \sim a'' \Leftrightarrow f(a') = f(a'')$.

Theorem 1.2.1 (Canonical decomposition). Let $f : A \to B$ be any function, and define $\sim$ as above. Then f decomposes as follows:

$$\begin{tikzcd} A \arrow[r, two heads] \arrow[rrr, bend left, "f"] & (A/\sim) \arrow[r, "\sim", "\tilde{f}"'] & \operatorname{Im} f \arrow[r, hook] & B \end{tikzcd}$$

where the first function is the canonical projection $A \to A/\sim$, the third function is the inclusion induced $\operatorname{im} f \subseteq B$, and the bijection $\tilde{f}$ in the middle is defined by

$$\tilde{f}([a]_\sim) := f(a)$$

for all $a \in A$.

Remark. 可以看出，任何一个函数都可以分解为一个 surjection，一个 bijection 和一个 injection 的组合，这个定理的 key insight 在于按照 $\operatorname{Im} f$ 将 A 拆分为等价类。

如果对 $\tilde{f}$ 的定义合法，那么显然上述分解是 commutative 的。因此证明这个定理的关键在于：

- $\tilde{f}$ 确实是一个 function;
- $\tilde{f}$ 确实是一个 bijection.

在上述定理中对 $\tilde{f}$ 的定义中存在一个问题，那就是对于同一等价类中的 a' 和 a''，是否有 $f(a') = f(a'')$，如果是否定的话，那么 $[a]_\sim$ 会对应多个 image，从而 $\tilde{f}$ 不是一个 function. 从前面对 $\sim$ 的定义中，显然 $f(a') = f(a'')$，因此 $\tilde{f}$ 是 *well-defined* 的。

而对于 bijection，我们只需证明 $\tilde{f}$ 既是 injection 又是 surjection 即可，这里不再赘述。

1.2.9 Clarification

通过 disjoint unions, products 或 quotients 得到的集合，它们的主要性质并不是指它们包含了什么 elements，而是它们与其他集合之间的关系。这在之后的 Universal properties section 中会有所体现。

1.3 Categories

categories 的语言被 Norman Steenrod 称为 *abstract nonsense*，因为 categories 的主要研究重点是 'structure' 而非 'meaning'，这强调了你应该把注意力放在 how that set may sit in relationship with all other sets 而不是 how you run into a specific set.

1.3.1 Definition

一个 category 由一些满足特定条件的 'objects' 和 'morphisms' 组成（collection）。注意这里使用的是 'collection' 而不是 'set'，这是因为根据 Russell's paradox，我们应该避免讨论 'set of all sets'，而 category 的 objects 是一个比 set 更广泛的概念，它允许 'collection of all sets'.

用 technical name 来描述上述 collection 则是 *class*，即 'class of sets'，这是一个比 set 更大的概念。另一种描述是用 *universe* 来定义一个足够大的 set，然后默认所有的 categories 的所有 objects 都取自这个 universe.

在后面的一些 examples 中，我们会看到一些 category 的 objects 是 sets，这种 category 我们称它是 *small* 的。

Definition 1.3.1 (Category)**.** A *category* C consists of

- a class $\operatorname{Obj}(\mathsf{C})$ of *objects* of the category; and
- for every two objects A, B of C, a set $\operatorname{Hom}_{\mathsf{C}}(A, B)$ of *morphisms* with the properties listed below.
  - For every object of A of C, there exists (at least) one morphism $1_A \in \operatorname{Hom}_{\mathsf{C}}(A, A)$, the 'identity' on A.
  - One can compose morphisms: two morphisms $f \in \operatorname{Hom}_{\mathsf{C}}(A, B)$ and $g \in \operatorname{Hom}_{\mathsf{C}}(B, C)$ determine a morphism $gf \in \operatorname{Hom}_{\mathsf{C}}(A, C)$.
  - This 'composition law' is associative: if $f \in \operatorname{Hom}_{\mathsf{C}}(A, B), g \in \operatorname{Hom}_{\mathsf{C}}(B, C)$, and $h \in \operatorname{Hom}_{\mathsf{C}}(C, D)$, then
  $$h(gf) = (hg)f.$$
  - The identity morphisms are identities with respect to composition: that is, for all $f \in$

$\mathrm{Hom}_{\mathsf{C}}(A, B)$ we have

$$f 1_A = f, \quad 1_B f = f.$$

One further requirment is that the sets

$$\mathrm{Hom}_{\mathsf{C}}(A, B), \quad \mathrm{Hom}_{\mathsf{C}}(C, D)$$

be *disjoint* unless $A = C, B = D$.

Note. 值得注意的是，上述定义中 90% 描述的是 morphisms 的性质，这与上面提到的 “categories 的研究重点是 ‘structure’ ” 的观点不谋而合，因为 morphisms 才是描述 ‘structure’ 的关键。

但是，我们也会不可避免地从 objects 的角度来看待 categories，因为 morphisms 最终还是由 objects 决定的。

Definition 1.3.2 (Endomorphism). A morphism of an object A of a category C to itself is called an *endomorphism*; $\mathrm{Hom}_{\mathsf{C}}(A, A)$ is denoted $\mathrm{End}_{\mathsf{C}}(A)$.

Note. The composition defines an ‘operation’ on $\mathrm{End}_{\mathsf{C}}(A)$: if f, g are elements of $\mathrm{End}_{\mathsf{C}}(A)$, so is their composition gf.

1.3.2 Examples

Example (Set). We will use Set to denote the category of sets. Thus

- $\mathrm{Obj}(\mathsf{Set})$ = the class of all sets;
- for A, B in $\mathrm{Obj}(\mathsf{Set})$, $\mathrm{Hom}_{\mathsf{Set}}(A, B) = B^A$

Note. 尽管 sections 1.1.3 and 1.1.4 中提到了 sets 的 operations 体现了其他 categories 不一定有的 Set 的一些有意思的 features，但是它们与 Set 的定义无关。

Example (Relation). Suppose S is a set and $\sim$ is a relation on S satisfying the reflexive and transitive properties.

- *objects*: the elements of S;
- *morphisms*: $\mathrm{Hom}(A, b) = \begin{cases} \text{the set consisting of } (a, b) \in S, & \text{if } a \sim b \\ \emptyset, & \text{otherwise.} \end{cases}$

Example (Discrete). 最简单的一个特例是由等价关系（‘=’）形成的 category，此时唯一的 morphisms 是 identity morphisms. 这些 categories 被称为是 *discrete* 的。

Example. 假设 S 是一个集合。定义一个 category $\hat{S}$，其中：

- $\mathrm{Obj}(\hat{S}) = \mathscr{P}(S)$
- 对 $\hat{S}$ 中的 objects A, B（即 $A \subseteq S, B \subseteq S$），有

$$\mathrm{Hom}_{\hat{S}}(A, B) = \begin{cases} (A, B), & \text{if } A \subseteq b \\ \emptyset, & \text{otherwise.} \end{cases}$$

Remark. 用这种方式构成的样例在类似 algebraic geometry 这样的成熟的领域中十分重要。

1.4 Morphisms

1.4.1 Isomorphism

Definition 1.4.1 (Isomorphism). A morphism $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ is an *isomorphism* if it has a (two-sided) inverse under composition: if $\exists g \in \mathrm{Hom}_{\mathsf{C}}(B, A)$ such that

$$gf = 1_A, \quad fg = 1_B.$$

Appendix

Appendix A

Additional Proofs

A.1 Proof of ??

We can now prove **??**.

Proof of ??. See here. ■

Bibliography

[Alu09] Paolo Aluffi. *Algebra : chapter 0*. American Mathematical Society, 2009.