

CHAPTER

Contents

目录

Contents

Preliminaries: Set theory & categories

1.1

SECTION

Naive set theory

1.1.1 集合的运算

「DEF

集合的运算

- \cup : *union*;
- \cap : *intersection*;
- \setminus : *difference*;
- \amalg : *disjoint union*;
- \times : *set product*;

」

1.1.2 disjoint union

「DEF

Disjoint union

$S \amalg T$: 得到 S 与 T 的拷贝 S' 与 T' , 且 $S' \cap T' = \emptyset$, 则 $S' \cup T' = S \amalg T$. 其中一种依赖于 *set product*

的实现:

$$\begin{cases} S' := \{0\} \times S, \\ T' := \{1\} \times T. \end{cases}$$

」

1.1.3 set product

「**DEF**

Set product

$$S \times T := \{\{\{s\}, \{s, t\}\} : s \in S \wedge t \in T\}.$$

将 $\{\{s\}, \{s, t\}\}$ 写作 (s, t) , 称为 *pair*.

」

1.1.4 等价关系

「**DEF**

等价关系

若 \mathcal{R} 是二元关系, 则 a, b 满足关系 \mathcal{R} 写为:

$$a \mathcal{R} b.$$

若关系 \sim 定义在集合 S 上满足:

- reflexivity: $(\forall a \in S) a \sim a$.
- symmetry: $(\forall a \in S)(\forall b \in S) a \sim b \implies b \sim a$.
- transitivity: $(\forall a \in S)(\forall b \in S)(\forall c \in S) a \sim b \wedge b \sim c \implies a \sim c$.

则称 \sim 是在集合 S 上的等价关系.

」

1.1.5 分划与等价类 (partition & equivalence class)

「**DEF**

分划与等价类

- 分划是一个集合的集合, 满足:

$$\begin{cases} (\forall a \in P)(\forall b \in P) a \cap b = \emptyset, \\ \bigcup_{a \in P} a = S. \end{cases}$$

则称 P 是 S 的分划.

- 等价类:

$$[a]_{\sim} := \{x \in S : x \sim a\}.$$

称此为在 S 上 a 的等价类, 由于等价类两两不交, 且具有自反性, 则 S 上某等价关系得到的所有等价类组成的集合是 S 的分划 \mathcal{P}_{\sim} .

」

1.1.6 集合商 (set quotient)

「**DEF**

集合商

集合 S 与等价关系 \sim 的商定义为:

$$S/\sim := \mathcal{P}_{\sim}.$$

」

即 $a, b \in S$ 等价 \iff 商到同一个元素.

一个集合商的例子

定义 \mathbb{Z} 上的等价关系 $\sim : a \sim b \iff \frac{a-b}{2} \in \mathbb{Z}$, 则:

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

1.2

Functions between sets

SECTION

1.2.1 函数

「**DEF**

函数

- 函数的 Graph:

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

且满足 $(\forall a \in A)(\exists! b \in B)(a, b) \in \Gamma_f$, 即 $(\forall a \in A)(\exists! b \in B)f(a) = b$.

- 函数的图的表示:

$$\begin{cases} A \xrightarrow{f} B, \\ a \mapsto f(a). \end{cases}$$

」

1.2.2 Identity function(id)

在集合 A 上有:

$$\text{id}_A : A \rightarrow A, (\forall a \in A) \text{id}_A(a) = a.$$

1.2.3 函数的 image

若 $S \subset A, f : A \rightarrow B$, 则:

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

则 $f(A)$ 就是函数的 image, 记作 $\text{im } f$

1.2.4 函数的 restriction

记 $S \subset A$, 则:

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

1.2.5 函数的复合 (composition)

- 若 $f : A \rightarrow B, g : B \rightarrow C$, 则 $g \circ f : A \rightarrow C, (\forall a \in A) g \circ f(a) := g(f(a)).$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow g \circ f & \downarrow g \\ & & C \end{array}$$

此时称图是交换 (commutative) 的, 因为图描述的所有从 A 到 C 的通路都会送 A 中的任意一个元素到相同的结果.

函数的复合满足结合律:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \\ & & \searrow g \circ f & & \nearrow h \circ g & & \\ & & & & & & \end{array}$$

即 $h \circ (g \circ f) = (h \circ g) \circ f.$

1.2.6 单射、全射、双射 (injections, surjections, bijections)

「DEF

单射 (Injections, Inj)

 $f: A \rightarrow B$ 是单的若:

$$(\forall a' \in A)(\forall a'' \in A)a' \neq a'' \implies f(a') \neq f(a'').$$

实际上就是 $(\forall a' \in A)(\forall a'' \in A)f(a') = f(a'') \implies a' = a''$. 一般用箭头 $f: A \hookrightarrow B$ 表示.

」

「DEF

全射 (Surjections, Surj)

 $f: A \rightarrow B$ 是全的若:

$$(\forall b \in B)(\exists a \in A)f(a) = b.$$

此时 $\text{im } f = B$. 一般用箭头 $f: A \twoheadrightarrow B$ 表示.

」

「DEF

双射 (Bijections, Bij)

 f 是双的当且仅当 f 又单又全, 一般用箭头 $f: A \xrightarrow{\sim} B$ 表示.

- 若 $\exists f: A \xrightarrow{\sim} B$, 则记此时 $A \cong B$, 若其中一个集合元素数量有限, 则另一个也有限且两个集合元素数量相等.
- 集合 A 中的元素数量写作 $|A|$; 幂集写作 2^A .

」

1.2.7 单射、全射、双射的性质

- 双射有逆 (inverse):

THEOREM 1.2.1: 双射有逆

定义函数 $f: A \xrightarrow{\sim} B$, 定义 $g: B \rightarrow 2^A, (\forall b \in B)g(b) = \{a: f(a) = b\}$, 则由于 f 是单的, 则 $(\forall a', a'' \in A)f(a') = f(a'') \implies a' = a''$, 故 $(\forall b \in B)|g(b)| = 1$. 故可以定义 $g': B \rightarrow A, (\forall b \in B)g(b) = a, \text{ st } f(a) = b$, 且是良定义的.

此时 $g' \circ f = \text{id}_A, f \circ g' = \text{id}_B$, 此称 g' 为 f 的逆, 记为 f^{-1} .

双射的逆唯一:

PROOF 1.2.1: 双射的逆唯一

定义 $f: A \xrightarrow{\sim} B$ 的逆 g, g' , 由于 $f \circ \text{id}_A = f = \text{id}_B \circ f$, 因此:

$$g = g \circ \text{id}_B = g \circ (f \circ g') = (g \circ f) \circ g' = \text{id}_A \circ g' = g'.$$

故唯一. □

- 左逆与右逆 (Linv & Rinv) 若 $f : A \rightarrow B, g \circ f = \text{id}_A$, 则称 g 是 f 的左逆, 同理有右逆.
如果 $A \neq \emptyset, f : A \rightarrow B$:
◦ f 有 Linv $\iff f$ 是单的.

PROOF 1.2.2

1. (\implies) 若 f 有左逆, 设为 f^{-1} , 则:

$$(\forall a, b \in A \wedge a \neq b) f^{-1}(f(a)) = \text{id}_A(a) = a \neq b = f^{-1}(f(b)).$$

若 $(\exists a, b \in A) f(a) = f(b)$, 则与上式矛盾, 故 f 是单的.

2. (\impliedby) 若 f 是单的, 有双射有逆那部分的讨论知道 $(\forall b \in \text{im } f) \exists! a \in A \text{ st } f(a) = b$, 故定义:

$$g(b) := \begin{cases} a, & \text{if } (\exists a \in A) b = f(a) \\ S, & \text{if } b \notin \text{im } f. \end{cases}$$

则 g 满足 $g \circ f = \text{id}_A$.

□

- f 有 Rinv $\iff f$ 是单的.

PROOF 1.2.3

只证明 (\impliedby) 的部分, 由于 f 是单的, 定义:

$$g : B \rightarrow 2^A, b \mapsto \{a \in A : f(a) = b\}.$$

则 $(\forall b \in B) g(b) \neq \emptyset$, 定义:

$$h : B \rightarrow A, b \mapsto a \text{ st } a \in g(b).$$

这样定义的 h 可能有很多种, 但都满足其是 f 的右逆:

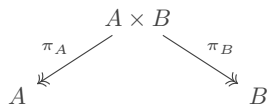
$$(\forall b \in B) h(b) \in g(b) \implies f \circ h(b) = \text{id}_B.$$

□

- 若 f 同时有左逆和右逆, 则两个逆相同.

一些单射、全射的例子

- 投影



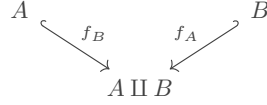
1.3. 范畴 (CATEGORIES)

其中 π 是投影 (projection) 映射:

$$\begin{aligned}\pi_A((a, b)) &:= a, \\ \pi_B((a, b)) &:= b.\end{aligned}$$

是全射.

- 与不交并的映射



若将 $A \amalg B$ 表示为 $A' \cup B'$, 其中 $A' \xrightarrow{F_A} A, B' \xrightarrow{F_B} B$, 则 $(\forall a \in A) f_A(a) := F_A(a) \in A \amalg B$.

- 商

$$A \xrightarrow{f} A/\sim$$

- 函数的标准分解 (Canonical decomposition) 对函数 $f: A \rightarrow B$, 在 A 上建立等价关系:

$$a \sim b \iff f(a) = f(b).$$

则函数可以分解为:

$$\begin{array}{ccccc} & & f & & \\ & \searrow & & \swarrow & \\ A & \xrightarrow{\quad} & A/\sim & \xrightarrow[\tilde{f}]{\sim} & \text{im } f \hookrightarrow B \end{array}$$

其中 $\tilde{f}: A/\sim \rightarrow \text{im } f, \tilde{f}([a]_{\sim}) := f(a)$, 不难验证这是良定义的, 现在证明 \tilde{f} 是双射:

PROOF 1.2.4

只需证明 f 既是单射也是全射就可以了:

1. inj:

$$\tilde{f}([a]_{\sim}) = \tilde{f}([b]_{\sim}) \implies f(a) = f(b) \implies a \sim b \implies [a]_{\sim} = [b]_{\sim}.$$

2. surj:

$$(\forall b \in \text{im } f) \exists a \in A \text{ st } f(a) = b \implies \tilde{f}([a]_{\sim}) = b.$$

□

1.3

SECTION

范畴 (Categories)

一个范畴 C 包括:

- 一个类 $\text{Obj}(C)$, 包括了对象 (object).

- 对任意两个对象 A, B 存在一个集合记为 $\text{Hom}_{\mathbf{C}}(A, B)$ 包含了从 A 到 B 的全部态射 (morphisms), 态射和 Hom 满足以下特点:

- 幺元的存在性

$\forall A \in \mathbf{C}, \exists 1_A \in \text{Hom}_{\mathbf{C}}(A, A) =: \text{End}_{\mathbf{C}}(A)$, 称为 A 的 identity.

- 态射复合的存在性

若 $\exists f \in \text{Hom}_{\mathbf{C}}(A, B), g \in \text{Hom}_{\mathbf{C}}(B, C)$, 则存在 f, g 决定的态射 $gf \in \text{Hom}_{\mathbf{C}}(A, C)$, 由于 Hom 是集合, 因此存在函数:

$$\text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) \rightarrow \text{Hom}_{\mathbf{C}}(A, C).$$

- 态射复合的结合性

若 $f \in \text{Hom}_{\mathbf{C}}(A, B), g \in \text{Hom}_{\mathbf{C}}(B, C), h \in \text{Hom}_{\mathbf{C}}(C, D)$, 则

$$(hg)f = h(gf).$$

这一性质导致态射图可交换.

- 幺元律

$$\forall f \in \text{Hom}_{\mathbf{C}}(A, B), f1_A = 1_B f = f.$$

一些范畴的小例子

1. 对象为集合、态射为集合函数的范畴, 记为 SET :

- $\text{Obj}(\text{SET}) :=$ 一个包含所有集合的类.
- $\text{Hom}_{\text{SET}}(A, B) := B^A$.

2. 一个关于二元运算的范畴: 若 S 上的二元运算 \sim 满足:

$$(\forall a, b, c \in S) \begin{cases} a \sim a, \\ a \sim b \wedge b \sim c \implies a \sim c. \end{cases}$$

则定义 \mathbf{C}_{\sim} :

- $\text{Obj}(\mathbf{C}_{\sim}) := S$.
- $\text{Hom}_{\mathbf{C}_{\sim}}(A, B) := \begin{cases} (A, B), & \text{if } A \sim B, \\ \emptyset, & \text{if } A \not\sim B. \end{cases}$

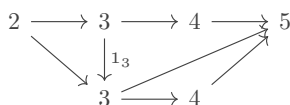
定义复合为:

$$\circ_{\mathbf{C}_{\sim}} : ((A, B), (B, C)) \mapsto (A, C).$$

则其为一个范畴.

1.3. 范畴 (CATEGORIES)

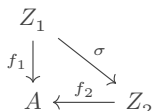
- 一个特例，如果认为 $S = \mathbb{Z}$ ， \sim 为 \leq ，则态射图如下：



3. 由范畴诱导范畴

Slice CAT 考虑范畴 C 中的对象 A ，接下来构建 C_A ：

- $\text{Obj}(C_A) := C$ 中所有到 A 的态射.
- $\text{Hom}_{C_A}(f_1, f_2) = \{\sigma : f_1 = f_2 \sigma\}$.



C_A 中态射的复合取自 C 中的态射复合.

CoSlice CAT 同理，只不过将从到 A 变成了 A 到其他对象的态射.

Opp CAT

$$\begin{cases} \text{Obj}(C^{\text{op}}) := \text{Obj}(C), \\ \text{Hom}_{C^{\text{op}}}(A, B) := \text{Hom}_C(B, A). \end{cases}$$

1.3.1 态射们

「**DEF**

同构 (Isomorphisms)

若一个态射 $f \in \text{Hom}_C(A, B)$ 满足：

$$\exists g \in \text{Hom}_C(B, A) \text{ st } gf = 1_A, fg = 1_B.$$

则 f 是一个同构，此时记 g 为 f^{-1} ，如果 f 有左逆、右逆，则它们必然相等（唯一）。

」

一些关于逆相关范畴的例子

- 一个同构都是 *identity* 的例子，用 (\mathbb{Z}, \leq) 定义的范畴.
- 一个每个态射都是同构的例子，用 $(\mathbb{Z}, =)$ 定义的范畴. 这种性质的范畴被称为广群 (Groupoids).

「**DEF**

自同构 (Automorphisms)

就是属于 End 的同构，所有 A 的自同构组成的集合称为 $\text{Aut}_C(A)$.

- $f, g \in \text{Aut}_C(A) \implies fg \in \text{Aut}_C(A)$.

- $f \in \text{Aut}_{\mathbf{C}}(A) \implies f^{-1} \in \text{Aut}_{\mathbf{C}}(A)$.

Aut 是一个群 (Group).

「DEF

单态射 (Monomorphisms, Monic)

即满足左消去律的态射:

$$\forall Z \in \text{Obj}(\mathbf{C}), \forall a, b \in \text{Hom}_{\mathbf{C}}(Z, A), f : A \rightarrow B$$

$$f \text{ is a monic} \iff (f \circ a = f \circ b \implies a = b)$$

「DEF

全态射 (Epimorphisms, Epic)

满足右消去律的态射:

$$\forall Z \in \text{Obj}(\mathbf{C}), \forall a, b \in \text{Hom}_{\mathbf{C}}(B, Z), f : A \rightarrow B$$

$$f \text{ is an epic} \iff (a \circ f = b \circ f \implies a = b)$$

在 SET 中, 单态射和全态射就是集合之间的单射和全射.

PROOF 1.3.1: SET 中的单/全态射是集合之间的单/全射

(\Leftarrow), 只需考虑单/全射的左/右逆即可:

$$f \circ a = f \circ b \implies f^{-1} \circ f \circ a = f^{-1} \circ f \circ b \implies a = b.$$

(\Rightarrow), 可以用反证法, 若 f 是非单射但是单态射, 则 $\exists a \neq b (f(a) = f(b))$, 考虑态射 $A : \{*\} \rightarrow a, B : \{*\} \rightarrow b$, 则 $A \neq B \wedge f \circ A = f \circ B$, 与单态射的定义矛盾.

类似的, 若 $f : A \rightarrow B$ 是非全射但是全态射, 则 $B \setminus \text{im } f \neq \emptyset$, 定义态射 $X : B \rightarrow \{1\}, Y : B \rightarrow \{0, 1\}$, 且:

$$Y(y) := \begin{cases} 1, & \text{if } y \in \text{im } f, \\ 0, & \text{if } y \notin \text{im } f. \end{cases}$$

则同样与全态射的定义矛盾. □

注意! Iso 并不等于 Monic \wedge Epic! 具体例子可以见 (\mathbb{Z}, \leq) 所定义的范畴: 每个 Hom 中只有一个态射, 则必然左/右可消去, 但只有 End 是同构. 同时, Monic 的复合是 Monic, Epic 同理.

1.4

SECTION

泛性质 (Universal properties)

泛性质与 I(nitial) / F(inal) 对象有关:



「DEF

I 对象与 F 对象

$A \in \text{Obj}(C)$, 则 A 是 I 的若:

$$(\forall Z \in \text{Obj}(C)) |\text{Hom}_C(A, Z)| = 1.$$

A 是 F 的若:

$$(\forall Z \in \text{Obj}(C)) |\text{Hom}_C(Z, A)| = 1.$$

若 I_1, I_2 是 C 上的 I/F 对象, 则 $I_1 \cong I_2$.

」

1.4.1 泛性质与一些例子

泛性质长得像一个范畴的 I/F 对象, 比如:

空集的泛性质是「集合之间的映射」

因为以集合为对象、集合映射为态射的范畴 SET 中, 空集是 I 对象.

一些其他例子

- 集合商 A/\sim 的泛性质是从集合 A 到其他映射集合的映射, 满足: “等价的 A 中元素有相同的像.” 即

$$A \xrightarrow{f} Z, f \text{ st } a \sim b \implies f(a) = f(b).$$

以此为范畴 $C_{A, \sim}$ 的 Obj , 则态射为 $\text{Hom}(f_1, f_2) = \{\sigma : \sigma f_1 = f_2\}$, 则考虑以下 cd :

$$\begin{array}{ccc} A/\sim & \xrightarrow{\exists! \sigma} & Z \\ \pi \uparrow & f_A \nearrow & \\ A & & \end{array}$$

其中 π 已给定 (为商投影映射), 则 A/\sim 是这个范畴的 I 对象.

PROOF 1.4.1

$\forall a \in A$ 都有 $\sigma\pi(a) = f_A(a)$, 即 $\sigma([a]_{\sim}) = f_A(a)$, 此就相当于定义了 σ (保证唯一), 易证 σ 是良定义的. \square

同时, $\text{im } f$ 也是其 I 对象:

$$\begin{array}{ccc} \text{im } f & \xrightarrow{\exists! \sigma'} & Z \\ f \uparrow & f_A \nearrow & \\ A & & \end{array}$$

故由 I 对象的特点有 $\text{im } f \cong A/\sim$.

- 集合的积集合 A, B 的积的泛性质是一个集合到 A 和 B 的两个映射.

给出三元组 (Z, f_A, f_B) , 此为 C 的 Obj . 则其态射为:

$$\text{Hom}((Z_1, f_A, f_B), (Z_2, g_A, g_B)) := \{\sigma : g_A\sigma = f_A \wedge g_B\sigma = f_B\}.$$

$A \times B$ 是其 F 对象:

$$\begin{array}{ccccc} & & A & & \\ f_A \nearrow & & \nwarrow \pi'_A & & \\ Z & \xrightarrow{\exists! \sigma} & A \times B & & \\ f_B \searrow & & \nwarrow \pi_B & & \\ & & B & & \end{array}$$

对 $\forall z \in Z$, 都有:

$$\begin{cases} \pi_A \sigma(z) = f_A(z), \\ \pi_B \sigma(z) = f_B(z). \end{cases}$$

故 $\sigma: z \mapsto (f_A(z), f_B(z))$, 唯一.

定义 $A \times B$ 中的积 (product) 为 $C_{A,B}$ 那个的 F 对象 (若存在).

- 另一个例子, 在 \mathbb{Z}, \leq 定义的范畴中, $A \times B := \min(A, B)$.
- 余积 (Coproduct) 定义 A, B 余积 $A \amalg B$ 为 $C^{A,B}$ 中的 I 对象, 则 SET 中的余积为两个集合的不交并.

PROOF 1.4.2

$$\begin{array}{ccccc} & & A \amalg B & & \\ I_A \nearrow & & \nwarrow I_B & & \\ A & \xrightarrow{\exists! \sigma} & A \amalg B & \xrightarrow{\exists! \sigma} & B \\ f_A \searrow & & \nwarrow f_B & & \\ & & Z & & \end{array}$$

如图所示, 考虑 $A \amalg B$ 的一种实现:

$$A \cong A', B \cong B', A' \cap B' = \emptyset, A' \cup B' \cong A \amalg B.$$

则, $\begin{cases} \forall a \in A, \sigma I_A(a) = f_A(a) \\ \forall b \in B, \sigma I_B(b) = f_B(b) \end{cases}$, 故:

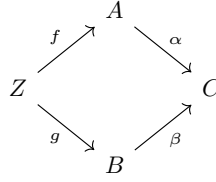
$$\sigma: a \mapsto \begin{cases} f_A(I_A^{-1}|_{A'}(a)), & \text{if } a \in A', \\ f_B(I_B^{-1}|_{B'}(b)), & \text{if } a \in B'. \end{cases}$$

□

- 纤维积 (Fiber product)

1.4. 泛性质 (UNIVERSAL PROPERTIES)

首先定义范畴 $\mathbf{C}_{\alpha, \beta}$:

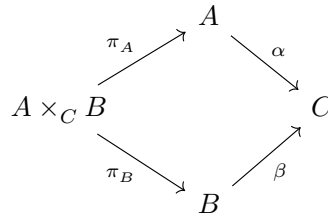


其 Obj 是如上三元组 (Z, f, g) 满足 $\alpha f = \beta g$. 其态射为

$$\text{Hom}((Z_1, f_1, g_1), (Z_2, f_2, g_2)) := \{\sigma : f_1 = f_2 \sigma \wedge g_1 = g_2 \sigma\}.$$

看起来和 $\mathbf{C}_{A, B}$ 很像, 只不过交换图要求更高了. 定义 A, B 的纤维余积 $A \times_C B$ 为此范畴的 F 对象. \square

SET 上的纤维积可以如下定义:



不妨设 $A \times_C B \subset A \times B$, 由于态射图要交换, 即 $\alpha \pi_A = \beta \pi_B$, 故 $A \times_C B := \{(x, y) : \alpha(x) = \beta(y)\}$. 现在来证明 $A \times_C B$ 是终对象:

PROOF 1.4.3

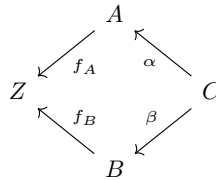
对于 $\forall Z$, 若存在 Z 到 A, B 的映射 f_A, f_B 满足 $\alpha f_A = \beta f_B$, 则 $\exists! \psi$ 满足 $f_A = \pi_A \psi \wedge f_B = \pi_B \psi$, 不妨设 ψ 将 z 映射到 $(\psi_A(z), \psi_B(z))$. 则易得 $\psi_A = f_A, \psi_B = f_B$, 因此 ψ 是存在且唯一的. \square

• 纤维余积 (Fiber coproduct)

\square DEF

纤维余积

定义范畴 $\mathbf{C}^{\alpha, \beta}$:



以上是 $\mathbf{C}^{\alpha, \beta}$ 的 Obj , 其态射为定义为:

$$\text{Hom}((Z_1, f_1, g_1), (Z_2, f_2, g_2)) := \{\sigma : \sigma f_1 = f_2 \wedge \sigma g_1 = g_2\}.$$

则纤维余积是这个态射的 I 对象.

」

以下是 SET 上的纤维余积:

重点是要解决态射图的“交换性质”, 即 $(\forall z \in C)(f_A \alpha(z) = f_B \beta(z))$, 同时, I_A 也会将同一个元素映射到同一个元素, 故设定价关系:

$$a \sim_A b \iff \alpha(a) = \alpha(b).$$

故 $[a]_{\sim_A} \subset C$ 中的所有元素都会被映射到 $A \amalg_C B$ 中的同一个元素, 若 $[a]_{\sim_A} \cap [b]_{\sim_B} \neq \emptyset$, 则这两个等价类中的元素也都会映射到 $A \amalg_C B$ 中的同一个元素, 故考虑等价关系:

$$[a]_{\sim_A} \sim_C [b]_{\sim_B} \iff [a]_{\sim_A} \cap [b]_{\sim_B} \neq \emptyset,$$

$$[a]_{\sim_A} \sim_C [b]_{\sim_A} \iff a = b.$$

故考虑商集:

$$(C/\sim_A \amalg C/\sim_B)/\sim_C.$$

则满足交换性质. 另若 $a \notin \text{im } \alpha$, 则可映射到自身 (的等价类), 因此可以认为:

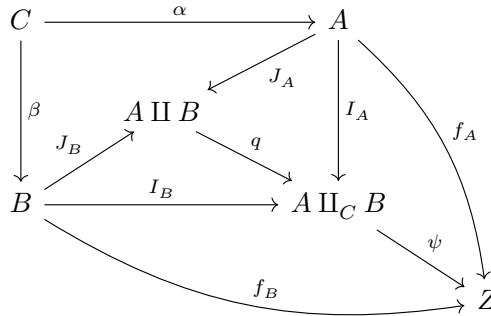
$$A \amalg_C B \cong (C/\sim_A \amalg C/\sim_B)/\sim_C \cup ((A \setminus \text{im } \alpha) \amalg (B \setminus \text{im } \beta)).$$

另外一个不太明显的想法是直接在 $A \amalg B$ 上直接商:

考虑等价关系 \sim , 满足 $A \amalg B$ 被其商掉后的商集满足态射图的交换. 也就是说若 $\alpha^{-1}(z_1) \cap \beta^{-1}(z_2) \neq \emptyset$, 则这样 $z_1 \sim z_2$, 在商后会将 C 中的一大把元素映射到 $A \amalg B$ 中的一个元素.

$$\sim := \begin{cases} (z_1, A) \sim (z_2, B) \iff \alpha^{-1}(z_1) \cap \beta^{-1}(z_2) \neq \emptyset, \\ (z_1, A) \sim (z_2, A) \iff z_1 = z_2. \end{cases}$$

则 $A \amalg_C B := A \amalg B / \sim$.



接下来我们知道对于 $\forall c \in C$, 都有 $\alpha^{-1}(\alpha(c)) \cap \beta^{-1}(\beta(c)) \neq \emptyset$, 也即 $J_A \alpha(c) \sim J_B \beta(c)$, 因此在集合商之后有:

$$q J_A \alpha(c) = q J_B \beta(c) \implies I_A \alpha = I_B \beta.$$

其中, J_A, J_B 是不满足态射图的交换的, 但最终 I_A 和 I_B 满足. 接下来证明这是个 I 对象:

PROOF 1.4.4

设 $\psi : A \amalg_C B \rightarrow (Z, f_A, f_B)$, 则有 $\psi I_A = f_A, \psi I_B = f_B$, 故 $(x, A) \mapsto [(x, A)]_{\sim} \mapsto \psi([(x, A)]_{\sim}) = f_A(x)$, 故:

$$\psi([x, ?]_{\sim}) = f_?(x), ? \in \{A, B\}.$$

由于如果 $[x, A] \sim [y, B] \implies \alpha^{-1}(x) \cap \beta^{-1}(y) \neq \emptyset \implies \forall m_1, m_2 \in \alpha^{-1}(x) \cup \beta^{-1}(y)$, 则 m_1, m_2 在 Z 中的像都相同 (由于态射图的交换性质), 因此 $A \amalg_C B$ 的确为 I 对象.

如果是 $(C/\sim_A \amalg C/\sim_B)/\sim_C \cup ((A \setminus \text{im } \alpha) \amalg (B \setminus \text{im } \beta))$ 形状的纤维余积, 则考虑

$$I_A : a \mapsto \begin{cases} [[\alpha^{-1}(a)]_{\sim_A}]_{\sim_C}, & \text{if } a \in \text{im } \alpha, \\ a, & \text{otherwise.} \end{cases}$$

I_B 同理. 则:

$$\psi : x \mapsto \begin{cases} [[x]_{\sim_?}]_{\sim_C}, & \text{if } x \in C/\sim_A \amalg C/\sim_B, \\ f_?(x), & \text{if } x \in (A \setminus \text{im } \alpha) \amalg (B \setminus \text{im } \beta). \end{cases}$$

□

Group, first encounter

乐子. 一个群 (group) 是一个单对象广群的同态集 Aut .

2.1

SECTION

群的定义

「DEF

群

- 群 G 是一个集合, 上面赋予了二元运算 $\circ_G : G \times G \rightarrow G$, 满足结合律:

$$(\forall a, b, c \in G) a \circ_G b \circ_G c = a \circ_G (b \circ_G c).$$

- 存在幺元

$$(\exists e_G \in G)(\forall g \in G) \underline{st} \ g \circ_G e_G = e_G \circ_G g = g.$$

- 存在逆元

$$(\forall g \in G)(\exists g^{-1} \in G) g \circ_G g^{-1} = g^{-1} \circ_G g = e_G.$$

」

一些例子

比如 $(\mathbb{Z}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}_{\neq 0}, \times)$ 都是群.

可逆 $n \times n$ 实矩阵组成的群表示为 $\text{GL}_n(\mathbb{R})$.

2.1.1 群的一些小性质

- 幺元唯一
- 逆元唯一

(由于结合律, 记 $g^n := \underbrace{g \circ \cdots \circ g}_{n \text{ times}}, g^{-n} := \underbrace{g^{-1} \circ \cdots \circ g^{-1}}_{n \text{ times}}$), 显然 $g^a g^b = g^{a+b}$.

如果是可交换群则用 $+$ 表示定义在其上的运算.

- 群的消去律

由于群元素有逆, 因此可以同时左/右消去.

2.1.2 阶

「DEF

群元素的阶

若 $g \in G, \exists n \in \mathbb{N}, g^n = e$, 则 $|g| := \inf_{g^n=e} n$, 称为该元素在群 G 中的阶.

- 如 $g^n = e$, 则 $|g| \mid n$.

PROOF 2.1.1

考虑 $g^{n-|g| \lfloor \frac{n}{|g|} \rfloor}$.

□

- 如果群是有限的, 那么 $|G|$ 记为该群的阶. 则 $|G| \geq |g|, \forall g \in G$.

群的阶在交换的前提下长得比较奇妙. 以下是另一个重要的推论:

- 若 $g \in G$ 的阶为 n , 则对任意 $m \in \mathbb{N}_{>0}$:

$$|g^m| = \frac{\text{lcm}(m, |g|)}{m} = \frac{|g|}{\text{gcd}(m, |g|)}.$$

PROOF 2.1.2

若 $(g^m)^n = g^{mn} = e$, 则:

$$|g| \mid mn \wedge m \mid mn \Rightarrow \inf mn = \text{lcm}(m, |g|) \Rightarrow \inf n = \frac{\text{lcm}(m, |g|)}{m} = \frac{|g|}{\text{gcd}(m, |g|)}.$$

□

- 如果 $gh = hg$, 则 $|gh| \mid \text{lcm}(|g|, |h|)$: 显然 $(gh)^N = g^N h^N \Rightarrow (gh)^{\text{lcm}(|g|, |h|)} = e$.

2.1.3 一些总结

- 乘法表可以用来表示一些群:

	e	g	h
e	e	g	h
g	g	h	e
h	h	e	g

	e	g
e	e	g
g	g	e

从乘法表看出, 单元素群 (平凡群)、二元素、三元素群都只有一种结构.

- $gG := \{gh : h \in G\} = G$, 实际上是群到群自身的映射 $I_g : G \rightarrow G$. 由群元素可逆易证.

以下是一些关于交换的例子:

- 若 $\gcd(|g|, |h|) = 1$, 则 $|gh| = |g||h|$, 以下是一个典型的证明:

PROOF 2.1.3

考虑 $(gh)^{|gh|} = e \implies (gh)^{|gh||h|} = e$, 即:

$$g^{|gh||h|} = e \implies |g| \mid |gh||h| \xrightarrow{\gcd(|h|, |g|)=1} |g| \mid |gh|.$$

同理 $|h| \mid |gh|$, 故 $\text{lcm}(|g|, |h|) \mid |gh|$, 又 $|gh| \mid \text{lcm}(|g|, |h|)$, 故 $|gh| = |g||h|$. □

- 若一个交换群 G 有有限的阶, 则设其元素阶的最大值为 $|g|$, 则 $\forall h \in G (|h| \mid |g|)$, 以下是另一个典型的证明:

PROOF 2.1.4

如果 $|h| \nmid |g|$, 则 $\exists p \in \mathbb{P}$ st $|g| = p^m r, |h| = p^n s, m < n$, 否则 $|h|$ 中所有质数的指数都不大于 $|g|$, 即 $|h| \mid |g|$.

接下来考虑 $|g^{p^m} h^s|$, 使用上一个推论:

$$|g^{p^m}| = r, |h^s| = p^n.$$

由于 $\gcd(p^n, r) = 1$, 因为 $p \in \mathbb{P}$. 故 $|g^{p^m} h^s| = |g^{p^m}| |h^s| = p^n r > |g|$, 矛盾! □

2.2

SECTION

一些群

2.2.1 对称（置换）群 (symmetric groups)

「DEF

对称群

对称群是一个对集合 S_A 的置换 $\text{Aut}_{\text{SET}}(S_A)$ ，一个对 $\{1, \dots, n\}$ 的置换群记为 S_n 。

很显然 $|S_n| = n!$ ，这里指的是群元素数量而不是阶。

☞ 低阶对称群们 S_2 只有两个元素 e, f :

$$e = (1, 2), f = (2, 1).$$

易证是交换的 (双元素群都是交换的)

S_3 有六个元素:

$$\left\{ \begin{array}{l} (1, 2, 3), (2, 1, 3), (3, 2, 1), \\ (1, 3, 2), (3, 1, 2), (2, 3, 1) \end{array} \right\}.$$

S_3 是不交换的。

☞ 群的生成初探 在 S_3 的例子中，令 $x = (2, 1, 3), y = (3, 1, 2)$ ，则 S_3 中六各元素可以只用 x, y 表示:

$$S_3 = \{e, x, y, y^2, xy, xy^2\}.$$

其中 $x^2 = e, y^3 = e$. 我们称 $A \subset G$ 生成 G 若每个 G 中元素都可以表示成 A 中元素与 A 中元素的逆的乘积。

2.2.2 二面体群 (Dihedral groups)

「DEF

二面体群

一个正 n 边形有以下 $2n$ 种对称情况:

- 绕中心旋转 $\frac{2i\pi}{n}$ ，其中 $i \in \{0, 1, \dots, n-1\}$ 有 n 种。
- 若 $n \in \text{Odd}$ ，则有 n 种翻转 (沿着中心与 n 个顶点的连线，同时也连接对应边的中点)。
- 若 $n \in \text{Even}$ ，则有 $\frac{n}{2}$ 种沿着中心到顶点的翻转， $\frac{n}{2}$ 种中心到边中点的翻转，总共 n 个。

故加起来总共有 $2n$ 种对称性, 因此二面体群记为 D_{2n} . 」

如果给每个顶点标号, 则 $D_{2n} \subseteq S_n$. 一些特殊的情况是 $D_6 = S_3, D_4 = S_2$ (因为群元素数量相同).

2.2.3 循环群和一些同余算术 (Cyclic groups and modular arithmetic)

「 DEF

循环群

建立在 \mathbb{Z} 上的等价关系如下:

$$(\forall a, b \in \mathbb{Z}) : a \equiv b \pmod{n} \iff n \mid (b - a).$$

这称为 n 的 congruence modulo. 我们记商集 $\mathbb{Z}/\equiv_n = \mathbb{Z}/n\mathbb{Z}$.

则此是一个元素为同余等价类的集合:

$$[0]_n, \dots, [n-1]_n.$$

定义此集合上的运算 $+$:

$$[a]_n + [b]_n := [a + b]_n.$$

(由于同余保持加法) 这个运算是良定义的, 在此运算的基础上, 集合的单位元为 $[0]_n$, $[m]_n$ 的逆元为 $[-m]_n$, 保持交换律、结合律, 因此是个交换群, 不妨记作 $\mathbb{Z}/n\mathbb{Z}$. 」

以下是一些推论:

- $|[m]_n| = \frac{n}{\text{lcm}(m, n)}$. 由于 $|g^m| = \frac{|g|}{\text{lcm}(|g|, m)}$, 因此将 $[m]_n$ 看成 $m[1]_n$ 即可.

- 在上面推论的前提下得到一个关于循环群的重要性质:

同余等价类 $[m]_n$ 可以生成整个 $\mathbb{Z}/n\mathbb{Z} \iff \gcd(m, n) = 1$, 因为阶刚好和群元素数量相等.

同余也保持乘法, 但是没法在 $\mathbb{Z}/n\mathbb{Z}$ 上面建立群 (因为有 $[0]_n$), 因此考虑:

$$(\mathbb{Z}/n\mathbb{Z})^* := \{[m]_n \in \mathbb{Z}/n\mathbb{Z} : \gcd(m, n) = 1\}.$$

则 $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ 是个群. 以下是一些证明:

- 首先证明这个集合关于乘法封闭:

$$\gcd(a, n) = 1 \wedge \gcd(b, n) = 1 \implies \gcd(ab, n) = 1 \implies [ab]_n \in (\mathbb{Z}/n\mathbb{Z})^*.$$

- 群的单位元显然是 $[1]_n$, 接下里是逆元的存在性:

由于 $\gcd(m, n) = 1$, 则 $[m]_n$ 可以生成整个 $\mathbb{Z}/n\mathbb{Z}$, 故 $(\exists a \in \mathbb{N}) a[m]_n = [1]_n \implies [am]_n = [1]_n$, 因此 $[m]_n$ 在 $(\mathbb{Z}/n\mathbb{Z})^*$ 中的逆元为 $[a]_n$.

2.3

SECTION

群范畴 GRP

2.3.1 群同态 (Group homomorphisms)

DEF

群同态

群同态是一个态射:

$$\psi: G \rightarrow H.$$

不妨再定义:

$$\psi \times \psi: G \times G \rightarrow H \times H, \psi \times \psi((a, b)) = (\psi(a), \psi(b)).$$

则满足下图交换的态射 ψ 就是 $G \rightarrow H$ 的群同态 $\in \text{Hom}_{\text{GRP}}(G, H)$:

$$\begin{array}{ccc} G \times G & \xrightarrow{\psi \times \psi} & H \times H \\ \downarrow \circ_G & & \downarrow \circ_H \\ G & \xrightarrow{\psi} & H \end{array}$$

为了使上图交换必须有:

$$\begin{array}{ccc} (a, b) & & (a, b) \xrightarrow{\psi \times \psi} (\psi(a), \psi(b)) \\ \downarrow \circ_G & & \downarrow \circ_H \\ a \circ_G b & \xrightarrow{\psi} & \boxed{\psi(a \circ_G b)} \quad = \quad \boxed{\psi(a) \circ_H \psi(b)} \end{array}$$

即 $\psi(ab) = \psi(a)\psi(b)$: 群同态保持群结构.

DEF

GRP

- $\text{Obj}(\text{GRP}) :=$ 所有的群.
- $\text{Hom}_{\text{GRP}}(G, H) :=$ 所有 $G \rightarrow H$ 的群同态.

群同态的一些性质如下:

- 群同态保持逆、幺元和阶

PROOF 2.3.1: 群同态保持逆、幺元

◦ 设 $f: G \rightarrow H$ 是群同态, 则:

$$0_H \circ_H f(0_G) = f(0_G) = f(0_G \circ_G 0_G) = f(0_G) \circ_H f(0_G) \xrightarrow{\text{消去律}} f(0_G) = 0_H.$$

$$\circ f(g) \circ_H f(g^{-1}) = f(g \circ_G g^{-1}) = f(0_G) = 0_H \implies f(g^{-1}) = f(g)^{-1}.$$

□

「DEF

群的直积 (Direct product)

按照集合积的方法有：

$$G \times H = \{(a, b) : a \in G \wedge b \in H\}.$$

而 $G \times H$ 上的运算定义为：

$$\circ_{G \times H} : (G \times H) \times (G \times H) \rightarrow G \times H, ((a, b), (c, d)) \mapsto (a \circ_G c, b \circ_H d).$$

同时还有两个标准投影：

$$\begin{array}{ccc} & G \times H & \\ \pi_G \swarrow & & \searrow \pi_H \\ G & & H \end{array}$$

」

PROOF 2.3.2: 群的直积就是 GRP 中两个群 G, H 的积：

$$\begin{array}{ccccc} & & \psi_G & \rightarrow & G \\ & \nearrow & & & \nearrow \pi_G \\ Z & \xrightarrow{\exists! \psi_G \times \psi_H} & G \times H & & \\ & \searrow & & & \searrow \pi_H \\ & & \psi_H & \rightarrow & H \end{array}$$

存在唯一一个态射 $\psi_G \times \psi_H$ 满足条件。证明与集合积的证明相同：

$$\begin{aligned} \psi_G \times \psi_H(ab) &= (\psi_G(ab), \psi_H(ab)) = (\psi_G(a)\psi_G(b), \psi_H(a)\psi_H(b)) \\ &= (\psi_G(a), \psi_H(a))(\psi_G(b), \psi_H(b)) = \psi_G \times \psi_H(a) \psi_G \times \psi_H(b) \end{aligned}$$

故该态射也是一个群同态。

□

群的余积一般表示为 $G * H$ ，也被称为自由积 (free product)，此处按下不表。**一些关于交换群的东西**

「DEF

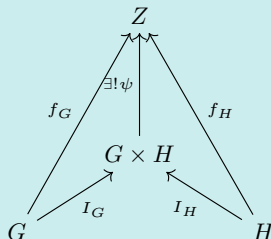
Ab

- $\text{Obj}(\text{Ab}) :=$ 所有的交换群.
- $\text{Hom}_{\text{Ab}}(G, H) :=$ 所有 $G \rightarrow H$ 的群同态.

这样一个范畴会比普通的 GRP 更为好看，一个特点是：

PROOF 2.3.3: Ab 中群的余积也是群的直积

考虑一下交换图：



其中 I_G, I_H 是嵌入映射 $I_G : g \mapsto (g, 0_H), I_H : h \mapsto (0_G, h)$. 则 (由于图要交换)：

$$\psi((g, 0_H)) = f_G(g), \psi((0_G, h)) = f_H(h).$$

另外 ψ 是一个群同态，因此有：

$$\psi((a, b)) = \psi((a, 0_H) + (0_G, b)) = \psi((a, 0_H)) + \psi((0_G, b)) = f_G(a) + f_H(b).$$

这是 ψ 唯一的定义 (若存在)，接下来是要满足群同态的性质 (上面那个只是特殊的)：

$$\begin{aligned} \psi((a, b) + (c, d)) &= \psi((a + c, b + d)) = f_G(a + c) + f_H(b + d) \\ &= f_G(a) + f_G(c) + f_H(b) + f_H(d) \\ &\stackrel{\text{交换群}}{=} f_G(a) + f_H(b) + f_G(c) + f_H(d) \\ &= \psi((a, b)) + \psi((c, d)). \end{aligned}$$

那的确是个群同态.

□

• \mathbb{Q} 不是任意两个非平凡群的直积.

不妨设 G, H 是非平凡的，且 $G \times H = \mathbb{Q}$ ，讨论群 $G \times \{0_H\}$ 和 $\{0_G\} \times H$ ，显然这俩群非平凡. 则讨论集合 $G \times \{0_H\} \setminus \{0_{\mathbb{Q}}\}$ ，则必然非空，设 $\frac{a}{b} \in G \times \{0_H\} \setminus \{0_{\mathbb{Q}}\}, a \neq 0$ ，同理设 $\frac{c}{d} \in \{0_G\} \times H \setminus \{0_{\mathbb{Q}}\}, c \neq 0$ ，故 $ac = ad \cdot \frac{c}{d} = cb \cdot \frac{a}{b}$ ，故 (由于 $G \times \{0_H\}, \{0_G\} \times H$ 是群，因此 $\frac{a}{b}, \frac{c}{d}$ 的倍数必然在对应的群里) $ac \in G \times \{0_H\} \cap \{0_G\} \times H = \{0_H, 0_G\} = 0_{\mathbb{Q}}$ ，则 $ac = 0$ 矛盾！

因此 $G \times \{0_H\}$ 和 $\{0_G\} \times H$ 必然有一个是平凡的，故 $G.H$ 有一个是平凡的.

• 存在这样的例子： H 非平凡， $G \times H \cong G$.

一个著名的例子是：

$$\mathbb{Z} \times \mathbb{Z}[x] \cong \mathbb{Z}[x].$$

该群同态为 $(n, (a_0, a_1, \dots)) \mapsto (n, a_0, a_1, \dots)$. 易验证是可逆的群同态.

2.4

SECTION

群同态们

一些例子

- 由于群同态只需满足保持运算, 那么将群 G 所有的元素全部映射到 0_H 的群同态 ψ 必然存在. 该群态可以分解为 G 到 GRP 中的 Z 对象、再从该 Z 对象到 H 的群同态的复合. 这种群同态被称为平方群同态.
- 指数 (Exponential) 群同态: $\epsilon_g: \mathbb{Z} \rightarrow G, n \mapsto g^n$, 注意到如果这个群同态是全射, 那么 G 中所有元素都可以用 g 的幂来表示, 即 g 生成了 G .
- 对待整数集, 有一个投影商映射: $\pi_n: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, a \mapsto [a]_n$, 很显然这是全射, 因为 $a \mapsto a[1]_n$, 而 $[1]_n$ 生成了整个 $\mathbb{Z}/n\mathbb{Z}$.

群同态与阶相关的例子 注意到 $\psi(g^{|g|}) = \psi(0) = \psi(g)^{|g|} = 0$, 故 $|\psi(g)| \mid |g|$.

群同构

DEF

群同构

群同构就是在 GRP 范畴中的同构, 也就是群同态 ψ 必须要有一个群同态的逆 ψ^{-1} .

PROOF 2.4.1: 一个群同态是群同构与该群同态是双的相互蕴含

显然只有双射有逆, 因此只需证明该逆是群同态:

$$\psi^{-1}(AB) = \psi^{-1}(\psi(\psi^{-1}(A))\psi(\psi^{-1}(B))) = \psi^{-1}(\psi(\psi^{-1}(A)\psi^{-1}(B))) = \psi^{-1}(A)\psi^{-1}(B).$$

□

因此指数函数 $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \times)$ 实际上是一个群同构. 当然此时可以说 $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \times)$.


DEF

循环群

一个群 G 是循环群若 $\exists n \in \mathbb{N} \text{ st } G \cong C_n \text{ 或 } G \cong \mathbb{Z}$

群同构比普通的群同构保留了更多群的性质，比如阶、交换性等等：

- 若 $G \xrightarrow[f]{} H$ ，则 $(\forall g \in G)|g| = |f(g)|$.
- 若 G 交换， $G \cong H$ ，则 H 也交换.

 **交换群上的群同态** 此时 $f : G \rightarrow H$ ，可以诱导出一个群若 H 是交换的，这个群是 $\text{Hom}_{\text{GRP}}(G, H)$ ：

$$(\psi + \phi)(z) := \psi(z) + \phi(z).$$

现在要满足一些性质：

- 封闭性，即 $\psi + \phi$ 也是群同态.：

$$\begin{aligned} (\psi + \phi)(a + b) &= \psi(a + b) + \phi(a + b) = \psi(a) + \psi(b) + \phi(a) + \phi(b) \\ &\stackrel{\text{交换}}{=} \psi(a) + \phi(a) + \psi(b) + \phi(b) \\ &= (\psi + \phi)(a) + (\psi + \phi)(b). \end{aligned}$$

- 结合律、逆元、单位元自然取自 H 中的. 因此整个群 $\text{Hom}_{\text{GRP}}(G, H)$ 都由交换群 H 诱导（与 G 是否交换无关）.

2.5

SECTION


自由群 (Free groups)

2.5.1 自由群的描述和泛性质

自由群是一个群以“特定的方式”包含了某个没有任何结构的集合 A . 下面是一个例子：

$$\mathcal{F}(\{a\}) := \{a^n : n \in \mathbb{Z}\} \cong \mathbb{Z}.$$

故 $\{*\}$ 的自由群是一个无限循环群. 而空集 \emptyset 的自由群则是任意的平凡群.

 **自由群的泛性质** 自由群是这样的一个范畴 \mathcal{F}^A 中的 I 对象，这个范畴可以如下定义：

\ulcorner DEF

\mathcal{F}^A

- $\text{Obj}(\mathcal{F}^A) := \{j \in \text{Hom}_{\text{SET}}(A, G) : G \in \text{Obj}(\text{GRP})\},$

- $\text{Hom}_{\mathcal{F}A}(j_1, j_2) := \{\sigma : \sigma j_1 = j_2 \wedge \sigma \in \text{Hom}(\text{GRP})\}.$

」

以下是一个对 $\mathcal{F}(\{a\})$ 同构与 \mathbb{Z} 的验证：

对 $\mathcal{F}(\{a\})$ 同构与 \mathbb{Z} 的验证

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\exists! \psi} & G \\ j \uparrow & \nearrow f & \\ \{a\} & & \end{array}$$

a 必然是被映射到 \mathbb{Z} 中的 ‘1’，代表着 a^1 ，而接下来，由于 ψ 是群同态，因此 $n \in \mathbb{Z}$ 会被映射到 $f(a)^n$ 。这样就决定了 ψ 的整个 Graph.

2.5.2 自由群的具体构造

由于集合 A 没有任何结构，我们不妨认为 A 中元素在自由群里的逆元不存在于 A 中（其实存在也无所谓）。以下将给出一个自由群的具体构造：

「DEF

自由群

1. 给定一个新的集合 $A^{-1} \stackrel{f}{\cong} A, f: a \mapsto a^{-1}$ ，此时只是记号阶段，只有这些到了自由群里才会真正起到“逆”的作用。
2. 给出“字 (Word)”的定义：

「DEF

字

我们可以将 $W(A)$ 定义如下：

$$W(A) := \{f \in \text{Hom}_{\text{SET}}(\{1, \dots, n\}, A) : n \in \mathbb{N}\}.$$

其实就是用 A 中元素组合而成的有限字符串。其中 n 被称为字符串的长度，我们不妨用 $L(w)$ 来表示字符串 w 的长度。

顺带一提的是，长度为 0 的字符串也算，称为空字符串。

」

3. 字符串里面有些特殊的存在，比如：

$$xyy^{-1}x \text{ 和 } x^2.$$

在群里我们认为是相同的，我们可以将其商掉，但为了方便我们构造个函数来解决这一困扰：

构造“约化”函数 $r: W(A) \rightarrow W(A)$ ，它的作用是从左到右找到第一个 aa^{-1} 或者 $a^{-1}a$ 的组合，然后将它删去。显然有以下两点：

- 如果 $r(w) = w$, 则我们认为这个字串已经被化简到最简了.
- $r^{\lfloor L(w)/2 \rfloor}(w)$ 必然是最简的, 因为如果连续有效化简 $\left\lfloor \frac{L(w)}{2} \right\rfloor$ 那么多次, 则字串的长度会被减到小于零, 矛盾.

那不妨定义 $R: W(A) \rightarrow W(A), w \mapsto r^{\lfloor L(w)/2 \rfloor}(w)$.

4. 解下来我们认为将 $W(A)$ 中的元素全部 R 之后就可以得到自由群, 即 $\text{im } R$. 定义自由群上的运算:

$$a \sim b := R(ab).$$

这里的 ab 指的是字符串接合.

$$ab: n \mapsto \begin{cases} a(n), & \text{if } n \leq L(a), \\ b(n), & \text{if } L(a) + L(b) \geq n > L(a). \end{cases}$$

接下来是验证:

- 结合律. 这个是明显的, 因为只需一次 R 就可以化到最简.
- 么元就是空字符串.
- 逆元就是将每一个元素都变成其“逆”然后再将字符串顺序颠倒.

这样就给出了对任意一个集合 A , 其自由群的定义. ┘

PROOF 2.5.1: 自由群的泛性质

$$\begin{array}{ccc} W(A) & \xrightarrow{\exists! \psi} & G \\ j \uparrow & \nearrow f & \\ A & & \end{array}$$

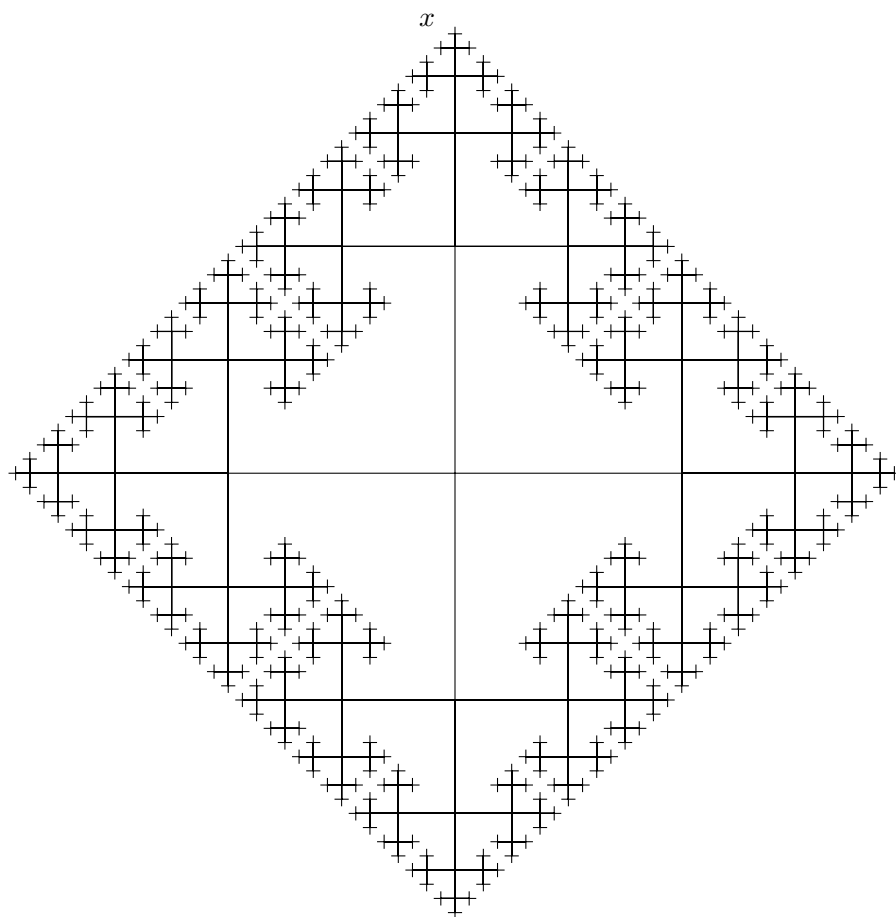
不妨考虑 $\mathcal{F}(A)$ 的超集 $W(A)$, 由于交换性, 必然有:

$$\psi j(a) = f(a) \implies \psi(j_a) = f(a).$$

其中 $j_a: 1 \rightarrow a$. 同时, 由于是群同态有

$$\psi \left(\sim_{i=1}^n j_{a_i} \right) = \prod_{i=1}^n f(a_i).$$

而 $W(A)$ 中的所有元素都可以用 $\sim_{i=1}^n j_{a_i}$ 来表示, 因此将 ψ 限制到 $\mathcal{F}(A)$ 上即可. □



只可意会的二阶自由群 Cayley 图

2.5.3 自由交换群 (Free abelian group)

自由交换群和自由群类似，只不过群变成了交换群：

$$\begin{array}{ccc} \mathcal{F}^{\text{ab}}(A) & \xrightarrow{\psi} & G \\ j \uparrow & \nearrow f & \\ A & & \end{array}$$

考虑 \mathbb{Z} 的 n 次直积（在交换的前提下记为直和） $\mathbb{Z}^{\oplus n}$ ，则面对元数数量为 n 的群 A 时， $\mathbb{Z}^{\oplus n} \cong \mathcal{F}^{\text{ab}}(A)$.

PROOF 2.5.2: $\mathbb{Z}^{\oplus |A|} \cong \mathcal{F}^{\text{ab}}(A)$

$$\begin{array}{ccc} \mathbb{Z}^{\oplus |A|} & \xrightarrow{\psi} & G \\ \uparrow j & \nearrow f & \\ A & & \end{array}$$

j 定义为:

$$j : a_i \mapsto (0, \dots, \underbrace{1}_i, \dots, 0).$$

则我们可以仿照自由群那样让 $j(a)$ 生成整个群 (其实上也是的确如此):

$$+_{\mathbb{Z}^{\oplus |A|}} : ((m_1, \dots, m_n), (k_1, \dots, k_n)) \mapsto (m_1 + k_1, \dots, m_n + k_n).$$

因此:

$$(m_1, \dots, m_n) = \sum_{1 \leq i \leq n} m_i j(a_i).$$

由于图表的交换性, 那么有:

$$\psi \left((0, \dots, \underbrace{1}_i, \dots, 0) \right) = f(a_i).$$

和群同态的性质——

$$\psi((m_1, \dots, m_n)) = \prod_{1 \leq i \leq n} f(a_i)^{m_i}.$$

最后验证这确实是个群同态:

$$\begin{aligned} \psi((m_1, \dots, m_n) + (k_1, \dots, k_n)) &= \psi((m_1 + k_1, \dots, m_n + k_n)) \\ &= \prod_{1 \leq i \leq n} f(a_i)^{m_i + k_i} \\ &\stackrel{\text{Abelian}}{=} \prod_{1 \leq i \leq n} f(a_i)^{m_i} \prod_{1 \leq i \leq n} f(a_i)^{k_i} \\ &= \psi((m_1, \dots, m_n)) \psi((k_1, \dots, k_n)) \end{aligned}$$

□

在此之上, 我们定义针对集合的群直和:

「DEF

直和

设 H 是一个交换群, A 是一个集合, 则 $\text{Hom}_{\text{SET}}(A, H) = H^A$ 是一个交换群. 直和是 H^A 的子集, 定义如下:

$$H^{\oplus A} := \{f \in H^A : |\{a \in A : f(a) \neq 0_H\}| < \infty\}.$$

这解决了不可数集合的自由群问题, 如下:

- 定义 $J_a : A \rightarrow H^{\oplus A}, x \mapsto \begin{cases} 1, & \text{if } x = a, \\ 0, & \text{if } x \neq a. \end{cases}$ 则我们可以将 $H^{\oplus A}$ 中的元素以下表示:

$$\sum_{a \in A} m_a J_a.$$

则显然有 $\psi : \sum_{a \in A} m_a J_a \mapsto \sum_{a \in A} m_a f(a).$

当然 m_a 只有有限个不为零.

2.5.4 子群 (Subgroups)

「DEF

子群

群 (H, \bullet) 是 G 上的子群若存在一个单射的群同态:

$$i : H \hookrightarrow G.$$

」

另一个看待子群的方法是考虑 G 的子集:

- H 是 G 的非空子集, 则 H 是 G 的子群当且仅当:

$$(\forall a, b \in H) ab^{-1} \in H.$$

PROOF 2.5.3

- (\Leftarrow) 由于 H 非空, 则 $\exists h \in H$, 故有:

$$e_G = hh^{-1} \in H.$$

同时 $\forall a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H$, 即 H 对逆运算封闭.

$\forall a, b \in H \Rightarrow ab = a(b^{-1})^{-1} \in H$, 故 H 对群乘法封闭, 剩下的结合律什么的继承自 G , 综上, H 是群.

- (\Rightarrow) 显然.

□

一些关于子群的东西

- 若 $\{H_a\}_{a \in A}$ 是 G 上的子群族, 则

$$H = \bigcap_{a \in A} H_a.$$

也是一个子群.

PROOF 2.5.4

$$g, h \in H \implies (\forall a \in A) g, h \in H_a \implies (\forall a \in A) gh^{-1} \in H_a \implies gh^{-1} \in H. \quad \square$$

2. 如果 $\psi: G \rightarrow G'$ 是一个群同态, H 是 G' 中的子群, 则

$$\psi^{-1}(H) := \{g \in G : \psi(g) \in H\}.$$

也是一个子群.

PROOF 2.5.5

只需要证明 $\forall a, b \in \psi^{-1}(H)$ 都有 $ab^{-1} \in \psi^{-1}(H)$, 即 $\psi(ab^{-1}) \in H$.

这是显然的, 因为 $\psi(ab^{-1}) = \psi(a)\psi(b)^{-1} \in H$, 因为 H 是子群. \square

3. 两个特殊的子群设 $\psi: G \rightarrow G'$ 是群同态, 则 $\text{im } \psi, \ker \psi$ 都是子群.

- $\ker \psi := \psi^{-1}(e_{G'})$, 由于 $\{e_{G'}\}$ 是一个子群, 因此有上面的证明知晓 $\ker \psi$ 是子群.
- $\text{im } \psi$ 是子群, 因为若 $a, b \in \text{im } \psi \implies \exists A, B \in G, \psi(A) = a, \psi(B) = b$, 则 $ab^{-1} = \psi(A)\psi(B)^{-1} = \psi(AB^{-1}) \in \text{im } \psi$.
- $\ker \psi$ 的泛性质:
考虑这个范畴 \mathbf{C} , 则 $\ker \psi$ 是 \mathbf{C} 的 F 对象:
 - $\text{Obj}(\mathbf{C}) = \{(K, a) \mid a: K \rightarrow G \wedge \psi a = e_{K \rightarrow G'}\}$.
 - $\text{Hom}_{\mathbf{C}}((K_1, a_1), (K_2, a_2)) = \{\sigma: a_2 \sigma = a_1\}$.

$$\begin{array}{ccccc} & & e_{K \rightarrow G'} & & \\ & \nearrow & & \searrow & \\ K & \xrightarrow{a} & G & \xrightarrow{\psi} & G' \\ & \searrow \exists! f & \uparrow i & & \\ & & \ker \psi & & \end{array}$$

其中 i 是嵌入映射, 将 $\ker \psi$ 中的元素映射到 G 中的相同元素, 又 $\psi a = e_{K \rightarrow G'}$, 则 $\text{im } a \subset \ker \psi$. 则:

$$if(x) = f(x) \implies f(x) = a(x), \forall x \in K.$$

即 ψ 与 a 将 K 中的元素映射到分别属于 G 和 $\ker \psi$ 的同一元素.

4. 由子集生成的子群设 $A \subset G$, 由自由群的泛性质:

$$\begin{array}{ccc} \mathcal{F}(A) & \xrightarrow{\exists! \psi} & G \\ i \uparrow & \nearrow f & \\ A & & \end{array}$$

则 $\text{im } \psi$ 是子群, 将这个群记为 $\langle A \rangle$, 或者 $\langle \{a_i\}_{a_i \in A} \rangle$.

- $\langle A \rangle$ 是所有包含 A 的子群之交.

$$\langle A \rangle = \bigcap_{H \text{ is subgroup of } G, A \subset H} H.$$

PROOF 2.5.6

显然, $\langle A \rangle$ 是包含 A 的子群, 只需证明其最小即可.

$$\begin{array}{ccc} \mathcal{F}(A) & \xrightarrow{\psi} & \text{im } \psi \\ \uparrow & & \downarrow f \\ A & \hookrightarrow & H \end{array}$$

只需证明 f 是单射即可, 其中 $\psi : \mathcal{F}(A) \rightarrow \text{im } \psi, a_1 \sim a_n \mapsto \prod_{i=1}^n a_i, f\left(\prod_{i=1}^n a_i\right) = \prod_{i=1}^n a_i \in H$.

由于 f 将 $\prod_{i=1}^n a_i \in H$ 映为自身, 故为单射. \square

5. 一些关于循环群的讨论

「**DEF**

有限生成 (Finitely generate)

一个群 G 若是有限生成的, 若存在一个有限子集 A 使得 $G \cong \langle A \rangle$. 换言之, 由于 $|A|$ 有限, 则可以用:

$$\mathcal{F}(\{1, \dots, |A|\}) \twoheadrightarrow G.$$

这样一个全态射来判定. \rfloor

- 对于循环群 \mathbb{Z} , 其子群必然是循环群, 或者是平凡群.

PROOF 2.5.7

若 G 是 \mathbb{Z} 的子群, 则必然非空, 若 G 非平凡, 则必然存在 $g \in G \wedge d > 0$, 设 $a = \inf_{g \in G, g > 0} g$, 则必然有 $a\mathbb{Z} \subset G$, 现在证明 $G \subset a\mathbb{Z}$.

设 $h \in G$, 将 h 分解为:

$$h = ka + b.$$

其中 $k \in \mathbb{Z}, b \in \{0, \dots, a-1\}$. 又 $a \in G$, 则 $h - k \cdot a \in G \implies b \in G$, 若 $b > 0$ 则与 a 的 inf 条件矛盾, 故 $b = 0$, 因此 $a \mid h \implies G \subset a\mathbb{Z}$. \square

- 若 $G \subset \mathbb{Z}/n\mathbb{Z}$ 的一个子群, 则 G 是由某个 $[d]_n$ 生成的循环群.

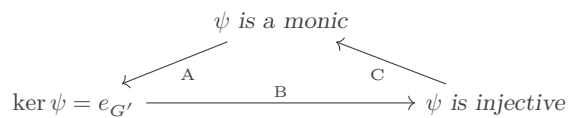
PROOF 2.5.8

上面已经证明 \mathbb{Z} 的子群都是循环群, 考虑商映射 $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ 这样一个群同态, 由于 G 是子群, 因此 $\pi_n^{-1}(G)$ 是 \mathbb{Z} 的子群, 即 $\pi_n^{-1}(G)$ 是循环群, 则必然由某个 d 生成 (包括 $d = 0$), 因此:

$$\begin{aligned} G &= \pi_n(G) = \{\pi_n(g) : g \in G\} = \{\pi_n(kd) : d \in \mathbb{Z}\} \\ &= \{n[d]_n : n \in \mathbb{Z}\} = \langle [d]_n \rangle. \end{aligned}$$

\square

6. GRP 中的单态射



上面三者是等价的：

PROOF 2.5.9

A. 不妨认为存在两个态射 i, e ：

$$\begin{array}{ccc}
 & i & \\
 \ker \psi & \xrightarrow{\quad} & G \\
 & e & \\
 & \xrightarrow{\quad} & G'
 \end{array}$$

其中 i 是恒等映射， e 是平凡群态射。则由单同态有：

$$i, e \in \ker \psi \implies \psi i = \psi e \implies i = e.$$

也就是 $\ker \psi$ 中所有元素都是 e_G 。

B. 若 $\ker \psi = e_G$ ，则 $\psi(g_1) = \psi(g_2) \implies \psi(g_1)\psi(g_2)^{-1} = e'_G$ ，然后

$$\psi(g_1 g_2^{-1}) = e'_G \implies g_1 g_2^{-1} \in \ker \psi \implies g_1 = g_2.$$

即 $\psi(g_1) = \psi(g_2) \implies g_1 = g_2$ ，因此 ψ 是单的。

C. 在 SET 里面，单射必然是单态射，而 GRP 是 SET 的子范畴，证毕。

□