

代数

JoJo

jojoid@duck.com

目录

1 初等数论	3
1.1 自然数	3
1.2 整数	3
1.3 线性丢番图方程	4
2 初探范畴论	5
2.1 范畴与态射	5
2.2 泛性质	6
3 初探群论	11
3.1 群	11
3.2 阶	11
3.3 群的例子	12
3.3.1 对称群	12
3.3.2 二面体群	12
3.3.3 循环群	12
3.4 群范畴 \mathbf{Grp}	13
3.5 交换群范畴 \mathbf{Ab}	14
3.6 群同态	15
3.6.1 例子	15
3.6.2 同态与阶	16
3.6.3 群同构	16
3.6.4 交换群的同态	16
3.7 自由群	17
3.7.1 泛性质	17
3.7.2 具体构造	17
3.7.3 自由交换群	19
3.8 子群	21

1 初等数论

1.1 自然数

定义 1.1 Peano 公理

1. $0 \in \mathbb{N}$
2. $\text{suc} : \mathbb{N} \rightarrow \mathbb{N}_+$
3. suc 是单射
4. $\forall N \subset \mathbb{N}. 0 \in N \wedge (\forall n \in N. \text{suc}(n) \in N) \Rightarrow N = \mathbb{N}.$

定理 1.1 强归纳法

$$\forall N \subset \mathbb{N}. 0 \in N \wedge (\forall n \in \mathbb{N}. \{0, \dots, n\} \subset N \Rightarrow \text{suc}(n) \in N) \Rightarrow N = \mathbb{N}.$$

命题 1.1 存在无穷多的质数.

1.2 整数

定义 1.2 同余

设 $n \in \mathbb{Z}_+$. 定义 \mathbb{Z} 上的二元关系

$$_ \equiv _ \pmod{n} : \mathbb{Z} \times \mathbb{Z} \rightarrow \text{Propo}, (a, b) \mapsto n \mid (a - b)$$

命题 1.2 给定正整数 n , $_ \equiv _ \pmod{n}$ 是等价关系.

定义 1.3 设 $n \in \mathbb{N}_+$. 定义函数

$$[_]_n : \mathbb{Z} \rightarrow \mathbb{Z}/(_ \equiv _ \pmod{n}), a \mapsto [a]_n := \text{等价类 } \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}.$$

定义集合

$$\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/(_ \equiv _ \pmod{n}) = \{[0]_n, \dots, [n-1]_n\}.$$

定义 $\mathbb{Z}/n\mathbb{Z}$ 上的加法

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, ([a]_n, [b]_n) \mapsto [a]_n + [b]_n := [a + b]_n.$$

命题 1.3 $\forall a, b \in \mathbb{Z}. a \equiv a' \pmod{n} \wedge b \equiv b' \pmod{n} \Rightarrow (a + b) \equiv (a' + b') \pmod{n}.$

命题 1.4 $\forall a, b \in \mathbb{Z}. a \equiv b \pmod{n} \Leftrightarrow [a]_n = [b]_n.$

推论 1.1 $\forall a, a', b, b' \in \mathbb{Z}. [a]_n = [a']_n \wedge [b]_n = [b']_n \Rightarrow [a]_n + [b]_n = [a']_n + [b']_n.$

定义 1.4 模运算

定义二元函数

$$_ \text{mod} _ : \mathbb{Z} \times \mathbb{Z}_+ \rightarrow \mathbb{Z}, (a, n) \mapsto a \bmod n := r,$$

其中 r 是唯一使得

$$[r]_n = [a]_n \wedge r \in \{0, \dots, n-1\}$$

成立的整数.

命题 1.5 $\forall n \in \mathbb{Z}_+. 0 \bmod n = 0$

定义 1.5 欧几里得算法 (求最高公因子 (*highest common factor*))

```

let hcf(a : Int, b : Int_pos) :=
  if a mod b = 0
  then b
  else
    hcf(b, a mod b)

```

命题 1.6 $\forall b \in \mathbb{Z}_+. \text{hcf}(0, b) = b$

定理 1.2

$$\forall a \in \mathbb{Z}, b \in \mathbb{Z}_+ \exists x, y \in \mathbb{Z}. xa + yb = \text{hcf}(a, b)$$

1.3 线性丢番图方程

推论 1.2 Bézout 定理

$$\forall a, c \in \mathbb{Z}, b \in \mathbb{Z}_+. (\exists x, y \in \mathbb{Z}. ax + by = c) \Leftrightarrow \text{hcf}(a, b) \mid c$$

引理 1.1 $\forall p \in \mathbb{P}, a, b \in \mathbb{Z}. p \mid ab \Rightarrow p \mid a \vee p \mid b$

定理 1.3 算术基本定理

$\forall n \in \mathbb{Z}_{\geq 2}. n$ 能唯一地表示成质数的乘积 (不考虑顺序).

命题 1.7 $\forall m \in \mathbb{Z}, n \in \mathbb{Z}_+. \text{hcf}(m, n) \cdot \text{lcm}(m, n) = |mn|$, 其中 lcm 是最低公倍数 (*lowest common multiple*).

2 初探范畴论

2.1 范畴与态射

定义 2.1 一个范畴 \mathcal{C} 系指以下资料:

1. 集合 $\text{Obj}(\mathcal{C})$, 其元素称作 \mathcal{C} 的**对象**;
2. 对于每对对象 A 和 B , 给定一个集合 $A \rightarrow B$, 其元素称作 \mathcal{C} 的**态射**, 满足:

$$\forall A, B, C, D \in \text{Obj}(\mathcal{C}). \neg(A = C \wedge B = D) \Rightarrow (A \rightarrow B) \cap (C \rightarrow D) = \emptyset;$$

3. 对于每个对象 A , 给定一个态射 $1_A : A \rightarrow A$, 称为 A 到自身的**恒等态射**;
4. 对于任意 $A, B, C \in \text{Obj}(\mathcal{C})$, 给定态射间的**合成映射**

$$(A \rightarrow B) \times (B \rightarrow C) \rightarrow (A \rightarrow C), (f, g) \mapsto g \circ f,$$

满足:

$$(i) \forall f : A \rightarrow B, g : B \rightarrow C, h : C \rightarrow D. (h \circ g) \circ f = h \circ (g \circ f),$$

$$(ii) \forall A, B \in \text{Obj}(\mathcal{C}), f : A \rightarrow B. f \circ 1_A = f = 1_B \circ f.$$

定义 2.2 对于任意范畴 \mathcal{C} , 其**反范畴** \mathcal{C}^{op} 定义如下:

1. $\text{Obj}(\mathcal{C}^{op}) := \text{Obj}(\mathcal{C})$;
2. $\forall A, B \in \text{Obj}(\mathcal{C}^{op}). A \rightarrow B := (B \rightarrow A)_{\mathcal{C}}$;
3. $\forall f : A \rightarrow B, g : B \rightarrow C. g \circ f := (f \circ g)_{\mathcal{C}}$.

定义 2.3 称 \mathcal{C}' 是 \mathcal{C} 的**子范畴**, 如果

1. $\text{Obj}(\mathcal{C}') \subset \text{Obj}(\mathcal{C})$;
2. $\forall A, B \in \text{Obj}(\mathcal{C}'). A \rightarrow B \subset (A \rightarrow B)_{\mathcal{C}}$;
3. $\forall f : A \rightarrow B, g : B \rightarrow C. g \circ f := (g \circ f)_{\mathcal{C}}$;
4. 恒等态射同 \mathcal{C} .

如果 $\forall A, B \in \text{Obj}(\mathcal{C}'). A \rightarrow B = (A \rightarrow B)_{\mathcal{C}}$, 则称 \mathcal{C}' 是 \mathcal{C} 的**全子范畴**.

定义 2.4 对于态射 $f : A \rightarrow B$, 若存在 $g : B \rightarrow A$ 使得 $g \circ f = 1_A, f \circ g = 1_B$, 则称 f 是**同构** (或称可逆, 写作 $f : A \xrightarrow{\sim} B$), 而 g 则称为 f 的**逆**.

命题 2.1 态射 f 有左逆 g_1 和右逆 $g_2 \Rightarrow f$ 有唯一的逆 $f^{-1} = g_1 = g_2$.

命题 2.2 每个恒等态射都是同构, 且是自己的逆.

命题 2.3 f 是同构 $\Rightarrow f^{-1}$ 是同构 $\wedge (f^{-1})^{-1} = f$.

命题 2.4 $f: A \rightarrow B, g: B \rightarrow A$ 是两个同构 $\Rightarrow g \circ f$ 是同构 $\wedge (g \circ f)^{-1} = f^{-1} \circ g^{-1}$

定义 2.5 若一个范畴 \mathcal{C} 中的所有态射都可逆, 则称之为**群胚**.

定义 2.6 设 A, B 是范畴 \mathcal{C} 中的对象, $f: A \rightarrow B$ 为态射.

1. f 是**单态射**, $:\Leftrightarrow \forall X \in \mathcal{C}, g, h: X \rightarrow A. g \neq h \Rightarrow f \circ g \neq f \circ h$ (即满足左消去律);
2. f 是**满态射**, $:\Leftrightarrow \forall X \in \mathcal{C}, g, h: B \rightarrow X. g \neq h \Rightarrow g \circ f \neq h \circ f$ (即满足右消去律).

命题 2.5 f 左(右)可逆 $\Rightarrow f$ 是单(满)态射.

命题 2.6 单(满)态射的合成是单(满)态射.

2.2 泛性质

定义 2.7 范畴 \mathcal{C} 中的对象 A 称为**始对象**, 如果对所有对象 X , 集合 $A \rightarrow X$ 是单点集. 类似的, 称 A 为**终对象**, 如果对所有对象 X , 集合 $X \rightarrow A$ 是单点集. 若 A 是始对象或终对象, 则称之为**端对象**. 若 A 既是始对象又是终对象, 则称之为**零对象**.

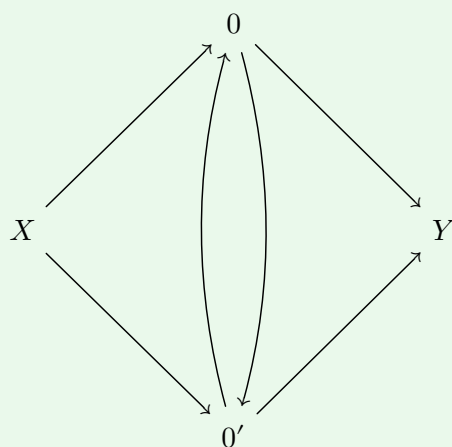
命题 2.7 设 A, A' 为 \mathcal{C} 的始对象, 则存在唯一的同构 $A \xrightarrow{\sim} A'$. 同样的性质对终对象也成立.

命题 2.8 设 A 为 \mathcal{C} 的始对象, $B \in \mathcal{C}$. 则 $A \simeq B \Leftrightarrow B$ 是 \mathcal{C} 的始对象. 同样的性质对终对象也成立.

定义 2.8 设 \mathcal{C} 中有零对象, 记作 0 . 对任意 $X, Y \in \mathcal{C}$ 定义**零态射** $0: X \rightarrow Y$ 为 $X \rightarrow 0 \rightarrow Y$ 的合成

命题 2.9 零态射从左右合成任何态射仍是零态射.

命题 2.10 零态射的定义无关零对象的选取：若 $0, 0'$ 都是零对象，则出入 $0, 0'$ 的箭头都是唯一的，即下图交换



命题 2.11 \emptyset 是 **Set** 的唯一的始对象。

定义 2.9 设 \mathcal{C} 是一个范畴， $*$ 是 \mathcal{C} 的终对象。

定义 \mathcal{C}^* ：

$$\text{Obj}(\mathcal{C}^*) := \{f : * \rightarrow X \mid X \in \mathcal{C}\},$$

$$\forall f : * \rightarrow X, g : * \rightarrow Y. f \rightarrow g := \{\sigma : X \rightarrow Y \mid \sigma \circ f = g\}.$$

\mathcal{C}^* 的对象称为有点对象。

定义 2.10 一个构造满足一个泛性质 \Leftrightarrow 它能被视为一个范畴的端对象。

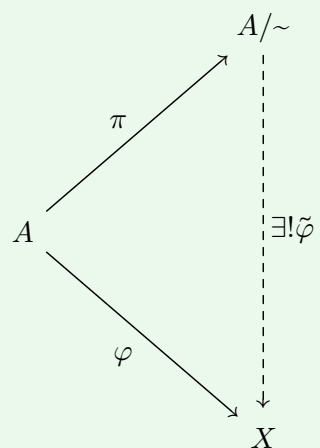
定义 2.11 设 \sim 是集合 A 上的一个等价关系。

定义 **Set**/ \sim ：

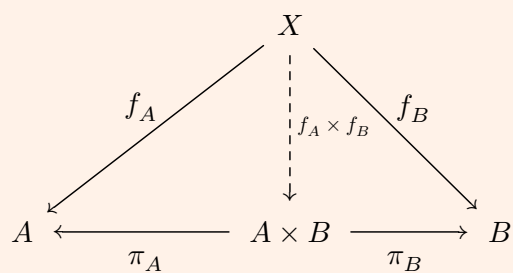
$$\text{Obj}(\mathbf{Set}/\sim) := \{\varphi : A \rightarrow X \mid X \in \text{Obj}(\mathbf{Set}), \forall a, b \in A. a \sim b \Rightarrow \varphi(a) = \varphi(b)\},$$

$$\forall \varphi_1 : A \rightarrow X_1, \varphi_2 : A \rightarrow X_2. \varphi_1 \rightarrow \varphi_2 := \{\sigma : X_1 \rightarrow X_2 \mid \sigma \circ \varphi_1 = \varphi_2\}.$$

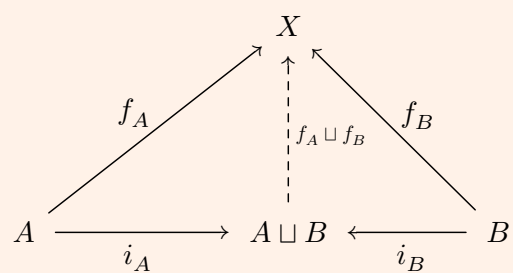
命题 2.12 $\pi : A \rightarrow A/\sim, x \mapsto [x]_\sim$ 是 \mathbf{Set}/\sim 的始对象，如下图



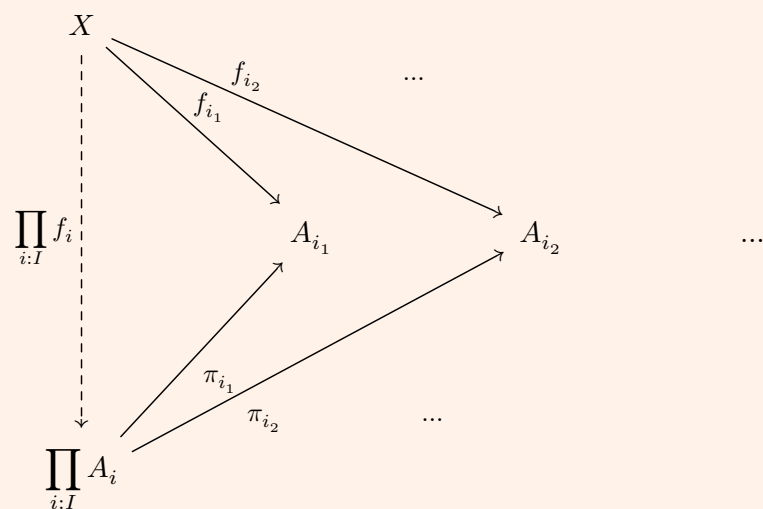
定义 2.12 设 $A, B \in \mathcal{C}$. A 和 B 的积 $A \times B$ (若存在则) 定义如下



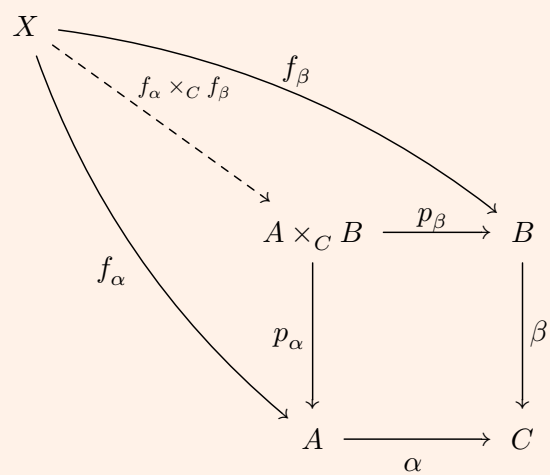
定义 2.13 余积



定义 2.14 积



定义 2.15 拉回



命题 2.13 设 \mathcal{C} 是一个范畴, $G \times G$ 和 $H \times H$ 是 \mathcal{C} 中的积. 则有

$$\begin{array}{ccc}
 G & \xrightarrow{\varphi} & H \\
 \uparrow \pi_G & \nearrow \varphi \circ \pi_G & \uparrow \pi_G \\
 G \times G & \xrightarrow{\exists! \varphi \times \varphi} & H \times H \\
 \downarrow \pi_G & \searrow \varphi \circ \pi_G & \downarrow \pi_G \\
 G & \xrightarrow{\varphi} & H
 \end{array}$$

命题 2.14 设 \mathcal{C} 是一个范畴, $G \times G, H \times H, K \times K$ 是 \mathcal{C} 中的积, 且有态射 $G \xrightarrow{\varphi} H \xrightarrow{\psi} K$. 则 $(\psi \circ \varphi) \times (\psi \circ \varphi) = (\psi \times \psi) \circ (\varphi \times \varphi)$.

3 初探群论

3.1 群

笑话 3.1 一个群是一个只有一个对象的群胚.

定义 3.1 设 G 是一个非空集合, $\cdot: G \times G \rightarrow G$.

(G, \cdot) 是一个群 \Leftrightarrow

1. 结合律: $\forall g, h, k \in G. (g \cdot h) \cdot k = g \cdot (h \cdot k)$;
2. 存在幺元: $\exists e \in G \forall g \in G. g \cdot e = g = e \cdot g$;
3. 所有元素皆可逆: $\forall g \in G \exists h \in G. g \cdot h = e = h \cdot g$.

命题 3.1 一个群的幺元是唯一的.

命题 3.2 一个元素的逆是唯一的.

命题 3.3 消去律: $\forall g, h, k \in G. g \neq h \Rightarrow g \cdot k \neq h \cdot k \wedge k \cdot g \neq k \cdot h.$

命题 3.4 $\forall g, h \in G. (g \cdot h)^{-1} = h^{-1} \cdot g^{-1}.$

定义 3.2 一个群是交换的： $\Leftrightarrow \forall g, h \in G. g \cdot h = h \cdot g$

3.2 阶

定义 3.3 群 G 的基数 $|G|$ 称为它的阶.

The diagram illustrates the construction of a 5x5 grid from smaller 2x2 and 3x3 grids. The 5x5 grid is composed of a 2x2 block of 2x2 grids in the top-left, a 2x2 block of 3x3 grids in the top-right, and a 3x3 block of 2x2 grids in the bottom-right. The 2x2 grids contain elements like 'e' and '·', while the 3x3 grids contain elements like 'e', 'a', 'b', and '·'.

命题 3.5 所有小于等于 4 阶的群都是交换的.

定义 3.4 群 G 的元素 g 有有限阶 $:\Leftrightarrow \exists n \in \mathbb{N}. g^n = e$.

在此情況下, g 的階 $|g| := \min\{n \in \mathbb{N}_+ \mid g^n = e\}$.

若 g 沒有有限阶, 則記为 $|g| = \infty$.

命题 3.6 如果 $g^n = e$, 则 $|g|$ 是 n 的一个因子 (即 n 是 $|g|$ 的一个倍数).

命题 3.7 $\forall g \in G. |g| \leq |G|.$

命题 3.8 $g \in G$ 有有限阶 $\Rightarrow \forall m \in \mathbb{N}. g^m$ 有有限阶 $\wedge |g^m| = \frac{\text{lcm}(m, |g|)}{m} = |g_{\frac{|g|}{\text{hcf}(m, |g|)}}|.$

命题 3.9 $g \cdot h = h \cdot g \Rightarrow |g \cdot h|$ 整除 $\text{lcm}(|g|, |h|).$

命题 3.10 $(\forall g \in G. |g| = 2) \Rightarrow G$ 是交换的.

命题 3.11 $\forall g, h \in G. |g \cdot h| = |h \cdot g|.$

命题 3.12 $g \cdot h = h \cdot g \wedge |g|$ 和 $|h|$ 互质 $\Rightarrow |g \cdot h| = |g| \cdot |h|.$

命题 3.13 设 G 是一个交换群, $g \in G$ 有有限阶且 $\forall h \in G. h$ 有有限阶 $\Rightarrow |h| \leq |g|$. 则 $\forall h \in G. h$ 有有限阶 $\Rightarrow |h|$ 整除 $|g|$.

3.3 群的例子

3.3.1 对称群

定义 3.5 设 $A \in \text{Set}$. A 的对称群 S_A 定义为群 $\text{Aut}_{\text{Set}}(A)$.

命题 3.14 $|S_n| = n!.$

命题 3.15 $|S_0| = |S_1| = 1.$

命题 3.16 $\forall n \geq 3. S_n$ 是非交换的.

命题 3.17 $\forall d \in \{0, \dots, n\} \exists \sigma \in S_n. |\sigma| = d.$

命题 3.18 $\forall n \in \mathbb{N}_+ \exists \sigma \in S_{\mathbb{N}}. |\sigma| = n.$

3.3.2 二面体群

定义 3.6 一个对称是一个保持结构的变换.

定义 3.7 一个正 n 边形有 $2n$ 个不同的对称: n 个旋转对称和 n 个反射对称. 相应的旋转和反射组成了二面体群 D_{2n} .

3.3.3 循环群

定义 3.8 一个群 G 是循环的: $\Leftrightarrow \exists a \in G \forall b \in G \exists m \in \mathbb{Z}. b$ 可以表示为 a^m , 即 $G = \{a^m \mid m \in \mathbb{Z}\}$. 其中 a 被称为 G 的一个生成元.

命题 3.19 设 G 是 n 阶循环群, a 是 G 的一个生成元. 则 $G = \{a^0 = e, a, a^2, \dots, a^{n-1}\}.$

定义 3.9 无限循环群

$$\langle a \rangle := \{ \dots, a^{-2}, a^{-1}, a^0 = e, a, a^2, \dots \}.$$

命题 3.20 设 G 是一个 n 阶群. 则 G 是循环的 $\Leftrightarrow \exists g \in G. |g| = n$.

命题 3.21 \mathbb{Z} 和 $\mathbb{Z}/n\mathbb{Z}$ 都是循环群, 它们的生成元分别是 1 和 $[1]_n$.

命题 3.22 $\forall m \in \mathbb{Z}, n \in \mathbb{Z}_+. |[m]_n| = \frac{n}{\text{hcf}(m, n)}.$

推论 3.1 $\forall m \in \mathbb{Z}, n \in \mathbb{Z}_+. [m]_n$ 生成 $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \text{hcf}(m, n) = 1$.

定义 3.10 整数模 n 乘法群

$$(\mathbb{Z}/n\mathbb{Z})^* := \{ [m]_n \in \mathbb{Z}/n\mathbb{Z} \mid [m]_n \text{ 生成 } \mathbb{Z}/n\mathbb{Z} \},$$

$$\cdot : (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/n\mathbb{Z})^*, ([a]_n, [b]_n) \mapsto [a]_n \cdot [b]_n := [ab]_n.$$

引理 3.1 $\forall a, a', b, b' \in \mathbb{Z}. [a]_n = [a']_n \wedge [b]_n = [b']_n \Rightarrow [a]_n \cdot [b]_n = [a']_n \cdot [b']_n.$

命题 3.23 $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ 是群.

3.4 群范畴 Grp

定义 3.11 集合函数 $\varphi : G \rightarrow H$ 是一个群同态 $:\Leftrightarrow$

图

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & H \times H \\ \downarrow \cdot_G & & \downarrow \cdot_H \\ G & \xrightarrow{\varphi} & H \end{array}$$

交换, 即 $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

定义 3.12 群范畴 Grp

$$\text{Obj}(\mathbf{Grp}) := \{ \text{所有群} \},$$

$$\forall G, H \in \text{Obj}(\mathbf{Grp}). G \rightarrow H := \{ \text{从 } G \text{ 到 } H \text{ 的群同态} \}.$$

定义 3.13 设 $G \in \mathbf{Grp}$. 定义函数 $\iota_G : G \rightarrow G, g \mapsto g^{-1}$.

命题 3.24 设 $\varphi: G \rightarrow H$ 是一个群同态. 则

1. $\varphi(e_G) = e_H$;

2. 图

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \downarrow \iota_G & & \downarrow \iota_H \\ G & \xrightarrow{\varphi} & H \end{array}$$

交换.

命题 3.25 平凡群 $\{e\}$ 是 **Grp** 的零对象.

定义 3.14 给定群 G 和 H , 它们的直积 $G \times H$ 系如下资料:

1. 下层集合: 集合 G 和 H 的积 $G \times H$;
2. 二元运算: $\cdot: (G \times H) \times (G \times H) \rightarrow G \times H, (g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$.

命题 3.26 一个直积是一个群, 且自然投影

$$G \xleftarrow{\pi_G} G \times H \xrightarrow{\pi_H} H$$

是群同态.

命题 3.27 群 G 和 H 的直积 $G \times H$ 是范畴 **Grp** 中的积.

3.5 交换群范畴 **Ab**

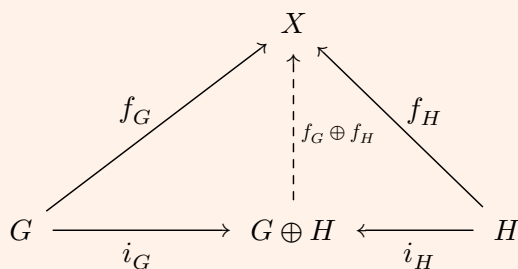
定义 3.15 交换群范畴 **Ab**

$$\begin{aligned} \text{Obj}(\mathbf{Ab}) &:= \{G \in \text{Obj}(\mathbf{Grp}) \mid G \text{ 是交换的}\}, \\ \forall G, H \in \text{Obj}(\mathbf{Ab}), G \rightarrow H &:= (G \rightarrow H)_{\mathbf{Grp}}. \end{aligned}$$

命题 3.28 平凡群是 **Ab** 的零对象.

命题 3.29 群 G 和 H 的直积 $G \times H$ 同时是范畴 **Ab** 中的积和余积.

定义 3.16 作为余积时, 群 G 和 H 的直积 $G \times H$ 被称为它们的**直和**, 并记为 $G \oplus H$, 如下图所示



其中,

$$i_G : G \rightarrow G \oplus H, g \mapsto (g, e_H),$$

$$i_H : H \rightarrow G \oplus H, h \mapsto (e_G, h).$$

3.6 群同态

3.6.1 例子

定义 3.17 设 G 和 H 是群. 定义**平凡态射** $\sigma : G \rightarrow H, g \mapsto e_H$. 显然, 平凡态射一定存在.

定义 3.18 设 \mathcal{C} 是一个范畴, $A \in \mathcal{C}$. 群 G 在 A 上的一个**作用**是一个群同态 $\sigma : G \rightarrow \text{Aut}_{\mathcal{C}}(A)$.

例子 3.2 设 a, b, c 是某个正三角形的三个顶点. 我们知道 $S_3 = \text{Aut}_{\text{Set}}\{a, b, c\}$, 且有群同态 $\sigma : D_{2,3} \rightarrow S_3$. 我们称“群 $D_{2,3}$ 作用于正三角形的顶点”.

定义 3.19 设 G 是一个群, g 是 G 的一个元素. 定义**指数映射** $\varepsilon_g : \mathbb{Z} \rightarrow G, m \mapsto g^m$.

命题 3.30 $\varepsilon_g(a+b) = \varepsilon_g(a) \cdot \varepsilon_g(b)$, 也就是说, 指数映射 ε_g 是一个群同态.

命题 3.31 设 $a \in \mathbb{Z}$. 则指数映射 $\varepsilon_a : \mathbb{Z} \rightarrow \langle a \rangle, m \mapsto a^m$ 是一个群同构.

定义 3.20 给定正整数 n , 定义群同态

$$\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, a \mapsto \varepsilon_{[1]_n}(a) = a[1]_n = [a]_n.$$

命题 3.32 $m \mid n \Rightarrow$ 存在一个群同态 $\pi_m^n : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ 使得图

$$\begin{array}{ccc} \mathbb{Z} & & \\ \pi_n \downarrow & \searrow \pi_m & \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\pi_m^n} & \mathbb{Z}/m\mathbb{Z} \end{array}$$

交换, 即 $\pi_m^n([a]_n) = [a]_m$.

3.6.2 同态与阶

命题 3.33 设 $\varphi : G \rightarrow H$ 为一个群同态, $g \in G$ 是一个有有限阶的元素. 则 $|\varphi(g)|$ 整除 $|g|$.

3.6.3 群同构

定义 3.21 一个群同构 $\varphi : G \rightarrow H$ 是 **Grp** 中的一个同构.

命题 3.34 设 $\varphi : G \rightarrow H$ 为一个群同态. 则 φ 是一个群同构 $\Leftrightarrow \varphi$ 是一个双射.

命题 3.35 设 $\varphi : G \rightarrow H$ 是一个群同构. 则

1. $\forall g \in G. |\varphi(g)| = |g|$;
2. G 是交换的 $\Leftrightarrow H$ 是交换的.

命题 3.36 群 $(\mathbb{Z}, +) \not\cong$ 群 $(\mathbb{Q}, +)$.

命题 3.37 函数 $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot), x \mapsto e^x$ 是群同构.

命题 3.38 群 $(\mathbb{Q}, +) \not\cong$ 群 $(\mathbb{Q}_{>0}, \cdot)$.

3.6.4 交换群的同态

命题 3.39 设 G 和 H 是两个交换群, 定义二元函数

$$\begin{aligned} + : (G \rightarrow H)_{\mathbf{Ab}} \times (G \rightarrow H)_{\mathbf{Ab}} &\rightarrow (G \rightarrow H)_{\mathbf{Set}}, \\ (\varphi, \psi) &\mapsto \varphi + \psi, (\varphi + \psi)(g) := \varphi(g) + \psi(g). \end{aligned}$$

则 $(G \rightarrow H)_{\mathbf{Ab}}$ 对 $+$ 封闭, 且 $((G \rightarrow H)_{\mathbf{Ab}}, +) \in \mathbf{Ab}$.

命题 3.40 设 A 是一个集合, H 是一个交换群. 则 $((A \rightarrow H)_{\mathbf{Set}}, +) \in \mathbf{Ab}$.

命题 3.41 设 G 是一个群. 则

1. 函数 $g \mapsto g^{-1} : G \rightarrow G$ 是一个群同构 $\Leftrightarrow G$ 是交换的;
2. 函数 $g \mapsto g^2 : G \rightarrow G$ 是一个群同态 $\Leftrightarrow G$ 是交换的.

3.7 自由群

3.7.1 泛性质

定义 3.22 自由群

给定集合 S , 定义范畴 \mathcal{F}_S :

$$\text{Obj}(\mathcal{F}_S) := \{ \iota : (S \rightarrow G)_{\text{Set}} \mid G \in \text{Obj}(\mathbf{Grp}) \},$$

$$\iota_1 \rightarrow \iota_2 := \{ \varphi : (\text{codom } \iota_1 \rightarrow \text{codom } \iota_2)_{\mathbf{Grp}} \mid \varphi \circ \iota_1 = \iota_2 \}.$$

$$\begin{array}{ccc} S & \xrightarrow{\iota_1} & \text{codom } \iota_1 \\ & \searrow \iota_2 & \downarrow \varphi \\ & & \text{codom } \iota_2 \end{array}$$

集合 S 上的自由群定义为 \mathcal{F}_S 中的始对象 (如果存在的话; 后面我们会证明它一定存在)

$$\begin{array}{ccc} S & \xrightarrow{\iota} & F(S) \\ & \searrow f & \downarrow \varphi \\ & & G \end{array}$$

命题 3.42 给定集合 S 和平凡群 $\{e\}$, 则 $(\{e\}, s \mapsto e : S \rightarrow \{e\})$ 是范畴 \mathcal{F}_S 的终对象.

3.7.2 具体构造

定义 3.23 对于任何集合 S , 如果我们把它的元素当作字符, 则可称其为一个字符集.

定义 3.24 对于任何字符 a , 定义其逆字符为字符 a^{-1} .

一个字符集 S 的所有字符的逆字符的集合记为 S^{-1} .

定义 3.25 一个字符集 S 上的所有字符串的集合定义如下

1. 如果 $S = \emptyset$, 则 $S^* := \{\text{空字符串}\}$;
2. 如果 S 非空, 则 $S^* := \{\text{空字符串}\} \cup \{a_1 \dots a_n \mid n \in \mathbb{N}_+, a_i \in S\}$.

约定 3.1 1. 对于任何字符 a , 我们可以把 $(a^{-1})^{-1}$ 化简为 a ;

2. 对于任何字符串 x , 其中形如 aa^{-1} 或 $a^{-1}a$ 的部分都能化简为空字符串;
3. 我们不区分字符以及字符串的化简前后的形式.

定义 3.26 自由群

设 S 是一个字符集, $T = S \cup S^{-1}$.

定义 T^* 上的乘法:

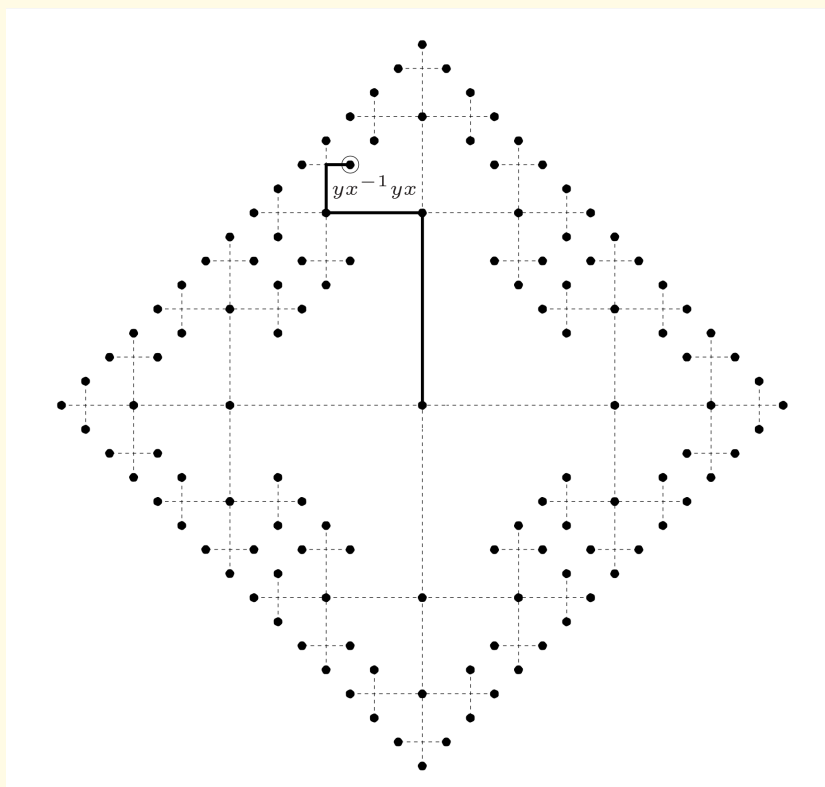
$$\cdot : T^* \times T^* \rightarrow T^*, (x, y) \mapsto xy,$$

即字符串连接.

显然, (T^*, \cdot) 构成一个群结构(乘法符合结合律; 有么元, 即空字符串; 每个字符串都有逆元), 称该群为集合 S 生成的自由群.

命题 3.43 设 S 是一个集合, F_S 是它生成的自由群, 函数 $\iota : S \rightarrow F_S, 'a' \mapsto 'a'$. 则 ι 满足 S 上的自由群的泛性质.

例子 3.3 二元集 $\{x, y\}$ 生成的自由群的 Cayley 图



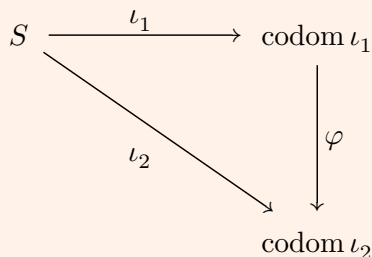
3.7.3 自由交换群

定义 3.27 自由交换群

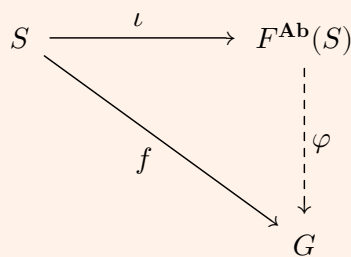
给定集合 S , 定义范畴 $\mathcal{F}_S^{\mathbf{Ab}}$:

$$\text{Obj}(\mathcal{F}_S^{\mathbf{Ab}}) := \{\iota : (S \rightarrow G)_{\text{Set}} \mid G \in \text{Obj}(\mathbf{Ab})\},$$

$$\iota_1 \rightarrow \iota_2 := \{\varphi : (\text{codom } \iota_1 \rightarrow \text{codom } \iota_2)_{\mathbf{Ab}} \mid \varphi \circ \iota_1 = \iota_2\}.$$



集合 S 上的自由交换群定义为 $\mathcal{F}_S^{\mathbf{Ab}}$ 中的始对象(如果存在的话;后面我们会证明它一定存在)。



定义 3.28 $\mathbb{Z}^{\oplus n}$

设 $n \in \mathbb{N}$. 定义 $\mathbb{Z}^{\oplus n}$

1. $\mathbb{Z}^{\oplus 0} := \{\text{空元组}\}$, 令其为平凡群;
2. 如果 $n > 0$, 则 $\mathbb{Z}^{\oplus n} := \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n \text{ 次}}$, 并定义其上二元运算 $\cdot : \mathbb{Z}^{\oplus n} \times \mathbb{Z}^{\oplus n} \rightarrow \mathbb{Z}^{\oplus n}, (x_1, \dots, x_n) \cdot (y_1, \dots, y_n) := (x_1 \cdot y_1, \dots, x_n \cdot y_n)$, 这也构成一个群.

命题 3.44 1. 设函数 $\iota : \emptyset \rightarrow \mathbb{Z}^{\oplus 0}$. 则 ι 满足 \emptyset 上的自由交换群的泛性质.

2. 设 $n \in \mathbb{N}_+$, $S = \{1, \dots, n\}$, 函数 $\iota : S \rightarrow \mathbb{Z}^{\oplus n}, i \mapsto \left(0, \dots, 0, \underbrace{1}_{\text{第 } i \text{ 位}}, 0, \dots, 0 \right)$. 则 ι 满足 S 上的自由交换群的泛性质.

定义 3.29 $H^{\oplus S}$

设 S 是一个集合, H 是一个交换群.

$$H^{\oplus S} := \left\{ \alpha : (S \rightarrow H)_{\text{Set}} \mid \{s \in S \mid \alpha(s) \neq e_H\} \text{ 是有限集} \right\}$$

显然 $(H^{\oplus S}, +)$ 是交换群.

命题 3.45 设 S 是一个集合, 函数 $\iota : S \rightarrow \mathbb{Z}^{\oplus S}, \iota(s) := (x \in S) \mapsto \begin{cases} 1, & x=s \\ 0, & x \neq s \end{cases}$. 则 $(\mathbb{Z}^{\oplus S}, \iota)$ 满足 S 上的自由交换群的泛性质.

3.8 子群

定义 3.30 子群

设 (G, \cdot) 和 (H, \cdot) 是群, 且它们的下层集合间有关系 $H \subset G$.

(H, \cdot) 是 (G, \cdot) 的一个子群 \Leftrightarrow 包含函数 $i : H \hookrightarrow G$ 是一个群同态.

命题 3.46 设 (G, \cdot) 是一个群, H 是 G 的一个非空子集. 则 (H, \cdot) 是 (G, \cdot) 的一个子群 $\Leftrightarrow \forall a, b \in H. ab^{-1} \in H$.

引理 3.2 如果 $\{H_\alpha\}_{\alpha \in A}$ 是群 G 的一族子群, 则 $\bigcap_{\alpha \in A} H_\alpha$ 是 G 的一个子群.

引理 3.3 设 $\varphi : G \rightarrow G'$ 是一个群同态, H' 是 G' 的一个子群. 则 $\varphi^{-1}(H')$ 是 G 的一个子群.

定义 3.31 核

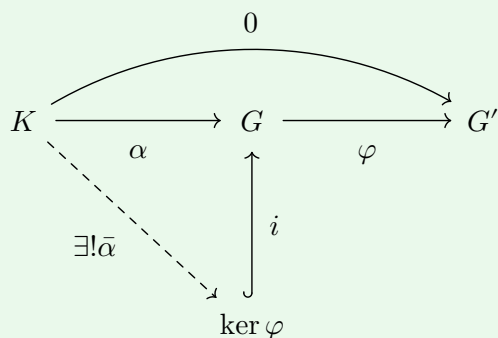
群同态 $\varphi : G \rightarrow G'$ 的核定义为:

$$\ker \varphi := \varphi^{-1}(e_{G'}).$$

命题 3.47 设 $\varphi : G \rightarrow G'$ 是一个群同态. 那么

1. $\ker \varphi$ 是 G 的一个子群.
2. 对于 G 的任何子群 H , $\varphi(H)$ 是 G' 的一个子群.

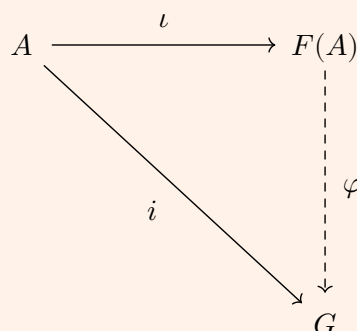
命题 3.48 设 $\varphi: G \rightarrow G'$ 是一个群同态. 定义一个范畴 \mathcal{C} , $\text{Obj}(\mathcal{C}) := \left\{ \alpha: (K \rightarrow G)_{\text{Grp}} \mid K \in \text{Grp}, \varphi \circ \alpha = \text{平凡同态 } 0: K \rightarrow G' \text{ (即 } \alpha(K) \subset \ker \varphi) \right\}$, $\forall \alpha: (K \rightarrow G)_{\text{Grp}}, \beta: (L \rightarrow G)_{\text{Grp}}, \alpha \rightarrow \beta := \left\{ \gamma: (K \rightarrow L)_{\text{Grp}} \mid \alpha = \beta \circ \gamma \right\}$. 则包含函数 $i: \ker \varphi \rightarrow G$ 是范畴 \mathcal{C} 的终对象, 如下图



定义 3.32 生成子群

第 1 种定义:

如果 A 是群 G 的一个子集, $i: A \rightarrow G$ 是包含映射, ι 满足 A 上的自由群的泛性质, 那么我们有一个唯一的群同态 $\varphi: F(A) \rightarrow G$ 使得下图交换



我们称 $\varphi(F(A))$ 为群 G 中由子集 A 生成的子群, 记为 $\langle A \rangle$.

第 2 种定义:

定义 $\langle A \rangle$ 的元素为具有以下形式的对象:

$$a_1 a_2 \dots a_n,$$

其中每个 a_i 是 A 中的元素, 或 A 中的元素的逆, 或幺元.

第 3 种定义:

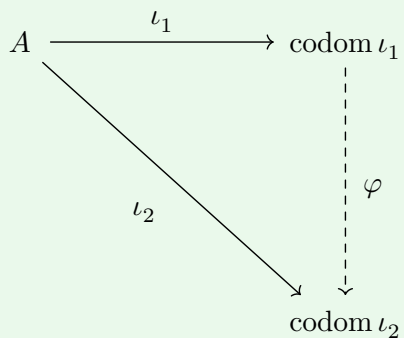
$$\langle A \rangle := \bigcap \{ G \text{ 的包含 } A \text{ 子群} \}.$$

命题 3.49 交换群经过群同态输出的像是交换群.

命题 3.50 给定集合 A , 定义范畴 \mathcal{F}_A :

$$\text{Obj}(\mathcal{F}_A) := \{ \iota : (A \rightarrow G)_{\text{Set}} \mid G \in \text{Obj}(\mathbf{Grp}) \},$$

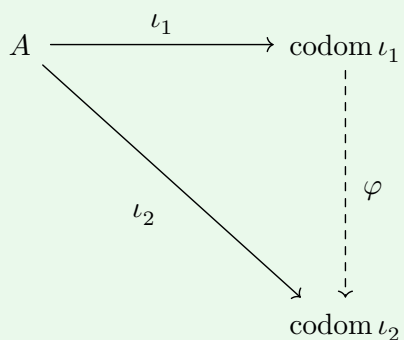
$$\iota_1 \rightarrow \iota_2 := \{ \varphi : (\text{codom } \iota_1 \rightarrow \text{codom } \iota_2)_{\mathbf{Grp}} \mid \varphi \circ \iota_1 = \iota_2 \}.$$



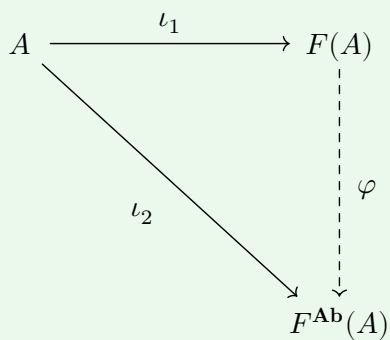
定义它的子范畴 $\mathcal{F}_A^{\mathbf{Ab}}$:

$$\text{Obj}(\mathcal{F}_A^{\mathbf{Ab}}) := \{ \iota : (A \rightarrow G)_{\text{Set}} \mid G \in \text{Obj}(\mathbf{Ab}) \},$$

$$\iota_1 \rightarrow \iota_2 := \{ \varphi : (\text{codom } \iota_1 \rightarrow \text{codom } \iota_2)_{\mathbf{Ab}} \mid \varphi \circ \iota_1 = \iota_2 \}.$$



设 ι_1 和 ι_2 分别是 \mathcal{F}_A 和 $\mathcal{F}_A^{\mathbf{Ab}}$ 的始对象, 且下图交换



那么, φ 是满射.