代数

JoJo
jojoid@duck.com

目录

1 初等数论

1.1 自然数

定义 1.1 ***Peano* 公理**

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

定理 1.1 **强归纳法**

$$\forall N \subset \mathbb{N}.\ 0 \in N \land (\forall n \in \mathbb{N}.\ \{0, ..., n\} \subset N \Rightarrow \mathrm{suc}(n) \in N) \Rightarrow N = \mathbb{N}.$$

命题 1.1 存在无限多的质数.

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

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

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

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

定义集合

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

定义 $\mathbb{Z}/n\mathbb{Z}$ 上的加法

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

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

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

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

定义 1.4 模运算

定义二元函数

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

其中 r 是唯一使得

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

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
    b
  else
    hcf(b, a mod b)
```

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

定理 1.2

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

1.3 线性丢番图方程

推论 1.2 *Bézout* 定理

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

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

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 $\forall m \in \mathbb{Z}, n \in \mathbb{Z}_+.\ \operatorname{hcf}(m, n) \cdot \operatorname{lcm}(m, n) = |mn|$，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 $\mathrm{Obj}(\mathcal{C})$，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 $A \to B$，其元素称作 $\mathcal{C}$ 的**态射**，满足：

$$\forall A, B, C, D \in \mathrm{Obj}(\mathcal{C}).\ \neg(A = C \land B = D) \Rightarrow (A \to B) \cap (C \to D) = \emptyset;$$

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

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

满足：

$$\text{(i) } \forall f : A \to B, g : B \to C, h : C \to D.\ (h \circ g) \circ f = h \circ (g \circ f),$$

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

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

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

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

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

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

定义 2.4 对于态射 $f : A \to B$，若存在 $g : B \to A$ 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 $\land \left(f^{-1}\right)^{-1} = f$.

命题 2.4 $f: A \to B, g: B \to A$ 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，$f: A \to B$ 为态射.

1. f 是**单态射**，$:\Leftrightarrow \forall X \in \mathcal{C}, g, h: X \to A.\ g \neq h \Rightarrow f \circ g \neq f \circ h$（即满足左消去律）;
2. f 是**满态射**，$:\Leftrightarrow \forall X \in \mathcal{C}, g, h: B \to X.\ g \neq h \Rightarrow g \circ f \neq h \circ f$（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 $A \to X$ 是单点集. 类似的，称 A 为**终对象**，如果对所有对象 X，集合 $X \to A$ 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** $0: X \to Y$ 为 $X \to 0 \to Y$ 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

$$\begin{tikzcd}
 & 0 \arrow[dd, bend left] \arrow[dr] & \\
X \arrow[ur] \arrow[dr] & & Y \\
 & 0' \arrow[uu, bend left] \arrow[ur] &
\end{tikzcd}$$

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 $\mathcal{C}^*$：

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

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

$\mathcal{C}^*$ 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 $\mathbf{Set}/\!\sim$

设 $\sim$ 是集合 A 上的一个等价关系. 定义范畴 $\mathbf{Set}/\!\sim$：

$$\mathrm{Obj}(\mathbf{Set}/\!\sim) := \Big\{(X, \varphi) \mid X \in \mathrm{Obj}(\mathbf{Set}),\ \varphi : (A \to X)_{\mathbf{Set}},\ \forall a, b \in A.\ a \sim b \Rightarrow \varphi(a) = \varphi(b)\Big\},$$

$$(X_1, \varphi_1) \to (X_2, \varphi_2) := \Big\{\sigma : (X_1 \to X_2)_{\mathbf{Set}} \mid \sigma \circ \varphi_1 = \varphi_2\Big\}.$$

命题 2.12 设 $\pi : A \to A/\sim, x \mapsto [x]$. 则 $(A/\sim, \pi)$ 是 $\mathbf{Set}/\sim$ 的始对象，如下图：

$$
\begin{tikzcd}
A \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & A/\sim \arrow[d, dashed, "\exists!\tilde{\varphi}"] \\
 & X
\end{tikzcd}
$$

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

$$
\begin{tikzcd}
 & X \arrow[dl, "f_A"'] \arrow[d, dashed, "f_A \times f_B"] \arrow[dr, "f_B"] & \\
A & A \times B \arrow[l, "\pi_A"] \arrow[r, "\pi_B"'] & B
\end{tikzcd}
$$

定义 2.13 **余积**

$$
\begin{tikzcd}
 & X & \\
A \arrow[ur, "f_A"] \arrow[r, "i_A"'] & A \sqcup B \arrow[u, dashed, "f_A \sqcup f_B"'] & B \arrow[ul, "f_B"'] \arrow[l, "i_B"]
\end{tikzcd}
$$

定义 2.14 **积**

$$
\begin{tikzcd}
X \arrow[dd, dashed, "\prod_{i:I} f_i"'] \arrow[dr, "f_{i_1}"] \arrow[drr, "f_{i_2}"] \arrow[drrr, phantom, "\cdots"] & & & \\
& A_{i_1} & A_{i_2} & \cdots \\
\prod_{i:I} A_i \arrow[ur, "\pi_{i_1}"] \arrow[urr, "\pi_{i_2}"'] \arrow[urrr, phantom, "\cdots"'] & & &
\end{tikzcd}
$$

定义 2.15 **拉回**

$$
\begin{tikzcd}
X \arrow[dr, dashed, "f_\alpha \times_C f_\beta"] \arrow[drr, bend left, "f_\beta"] \arrow[ddr, bend right, "f_\alpha"'] & & \\
& A \times_C B \arrow[r, "p_\beta"] \arrow[d, "p_\alpha"'] & B \arrow[d, "\beta"] \\
& A \arrow[r, "\alpha"'] & C
\end{tikzcd}
$$

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

$$\begin{tikzcd}
G \arrow[r, "\varphi"] & H \\
G \times G \arrow[u, "\pi_G"] \arrow[r, dashed, "\exists!\varphi \times \varphi"] \arrow[ur, bend left, "\varphi \circ \pi_G"] \arrow[d, "\pi_G"'] \arrow[dr, bend right, "\varphi \circ \pi_G"'] & H \times H \arrow[u, "\pi_G"'] \arrow[d, "\pi_G"] \\
G \arrow[r, "\varphi"'] & H
\end{tikzcd}$$

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，$\cdot : G \times G \to G$.

$(G, \cdot)$ 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**.

例子 3.1

$\cdot$	e
e	e

$\cdot$	e	a
e	e	a
a	a	e

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

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** $:\Leftrightarrow \exists n \in \mathbb{N}.\ g^n = e$.

在此情况下，g 的**阶** $|g| := \min\{n \in \mathbb{N}_+ \mid g^n = e\}$.

若 g 没有有限阶，则记为 $|g| = \infty$.

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 $\wedge\ |g^m| = \frac{\mathrm{lcm}(m,\ |g|)}{m} = |g \frac{|}{\mathrm{hcf}(m,\ |g|)}$.

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

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 $A \in \mathbf{Set}$. A 的**对称群** S_A 定义为群 $(\mathrm{Aut}_{\mathbf{Set}}(A), \circ)$.

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

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** $:\Leftrightarrow \exists a \in G\ \forall b \in G\ \exists m \in \mathbb{Z}$ 使得 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 $G = \{a^0 = e, a, a^2, ..., a^{n-1}\}$.

定义 3.9 **无限循环群**

称群 G 是**无限循环群**当且仅当 $G \cong (\mathbb{Z}, +)$.

显然无限循环群也是循环群.

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

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

定义 3.10 **整数模 n 乘法群**

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

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

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 $\varphi : G \to H$ 是一个**群同态** $:\Leftrightarrow$

图

$$\begin{tikzcd}
G \times G \arrow[r, "\varphi \times \varphi"] \arrow[d, "\cdot_G"'] & H \times H \arrow[d, "\cdot_H"] \\
G \arrow[r, "\varphi"'] & H
\end{tikzcd}$$

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

定义 3.12 **群范畴 Grp**

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

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

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

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

1. $\varphi(e_G) = e_H$;
2. 图

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\iota_G"'] & H \arrow[d, "\iota_H"] \\ G \arrow[r, "\varphi"'] & H \end{tikzcd}$$

交换.

命题 3.25 平凡群 $\{e\}$ 是 $\mathbf{Grp}$ 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：$\cdot : (G \times H) \times (G \times H) \to G \times H, (g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$.

命题 3.26 一个直积是一个群，且自然投影

$$\begin{tikzcd} G & G \times H \arrow[l, "\pi_G"'] \arrow[r, "\pi_H"] & H \end{tikzcd}$$

是群同态.

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

3.5 交换群范畴 Ab

定义 3.15 **交换群范畴 Ab**

$$\mathrm{Obj}(\mathbf{Ab}) := \{G \in \mathrm{Obj}(\mathbf{Grp}) \mid G \text{ 是交换的}\},$$

$$\forall G, H \in \mathrm{Obj}(\mathbf{Ab}), G \to H := (G \to H)_{\mathbf{Grp}}.$$

命题 3.28 平凡群是 $\mathbf{Ab}$ 的零对象.

命题 3.29 群 G 和 H 的直积 $G \times H$ 同时是范畴 $\mathbf{Ab}$ 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

$$
\begin{tikzcd}
 & X & \\
G \arrow[ur, "f_G"] \arrow[r, "i_G"'] & G\oplus H \arrow[u, dashed, "f_G\oplus f_H"'] & H \arrow[ul, "f_H"'] \arrow[l, "i_H"]
\end{tikzcd}
$$

其中，

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

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

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** $\sigma : G\to H, g\mapsto e_H$. 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 $\sigma : G\to \mathrm{Aut}_{\mathcal{C}}(A)$.

例子 3.2 设 a,b,c 是某个正三角形的三个顶点. 我们知道 $S_3=\mathrm{Aut}_{\mathbf{Set}}\{a,b,c\}$，且有群同态 $\sigma : D_{2\cdot 3}\to S_3$. 我们称"群 $D_{2\cdot 3}$ 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** $\varepsilon_g : \mathbb{Z}\to G, m\mapsto g^m$.

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 $\varepsilon_a : \mathbb{Z}\to\langle a\rangle, m\mapsto a^m$ 是一个群同构.

定义 3.20 给定正整数 n，定义群同态

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

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

$$\begin{tikzcd}
\mathbb{Z} \arrow[d, "\pi_n"'] \arrow[dr, "\pi_m"] & \\
\mathbb{Z}/n\mathbb{Z} \arrow[r, "\pi_m^n"'] & \mathbb{Z}/m\mathbb{Z}
\end{tikzcd}$$

交换，即 $\pi_m^n\left([a]_n\right) = [a]_m$.

3.6.2 同态与阶

命题 3.33 设 $\varphi : G \to H$ 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** $\varphi : G \to H$ 是 $\mathbf{Grp}$ 中的一个同构.

命题 3.34 设 $\varphi : G \to H$ 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 $\varphi : G \to H$ 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 n 阶循环群 $\cong (\mathbb{Z}/n\mathbb{Z}, +)$；无限循环群 $\cong (\mathbb{Z}, +)$.

命题 3.37 群$(\mathbb{Z}, +) \not\cong$ 群$(\mathbb{Q}, +)$.

命题 3.38 函数 $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), x \mapsto e^x$ 是群同构.

命题 3.39 群$(\mathbb{Q}, +) \not\cong$ 群$(\mathbb{Q}_{>0}, \cdot)$.

3.6.4 交换群的同态

命题 3.40 设 G 和 H 是两个交换群，定义二元函数

$$+ : (G \to H)_{\mathbf{Ab}} \times (G \to H)_{\mathbf{Ab}} \to (G \to H)_{\mathbf{Set}},$$

$$(\varphi, \psi) \mapsto \varphi + \psi, (\varphi + \psi)(g) := \varphi(g) + \psi(g).$$

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

命题 3.41 设 A 是一个集合，H 是一个交换群. 则 $\left((A \to H)_{\mathbf{Set}}, +\right) \in \mathbf{Ab}$.

命题 3.42 设 G 是一个群. 则

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

命题 3.43 交换群经过群同态输出的像是交换群.

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 $\boldsymbol{\mathcal{F}_S}$:

$$\operatorname{Obj}(\mathcal{F}_S) := \left\{(G, \iota) \mid G \in \operatorname{Obj}(\mathbf{Grp}), \iota : (S \to G)_{\mathbf{Set}}\right\},$$

$$(G_1, \iota_1) \to (G_2, \iota_2) := \left\{\varphi : (G_1 \to G_2)_{\mathbf{Grp}} \mid \varphi \circ \iota_1 = \iota_2\right\}.$$

$$\begin{tikzcd}
S \arrow[r, "\iota_1"] \arrow[dr, "\iota_2"'] & G_1 \arrow[d, "\varphi"] \\
 & G_2
\end{tikzcd}$$

集合 S 上的**自由群** $\boldsymbol{F(S)}$ 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)

$$\begin{tikzcd}
S \arrow[r, "\iota"] \arrow[dr, "f"'] & \boldsymbol{F(S)} \arrow[d, dashed, "\varphi"] \\
 & G
\end{tikzcd}$$

命题 3.44 给定集合 S 和平凡群 $\{e\}$, 则 $\{e\}$ 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 $S^* := \{\text{空字符串}\} \cup \{a_1...a_n \mid n \in \mathbb{N}_+, a_i \in S\}$.

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：

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

即**字符串连接**.

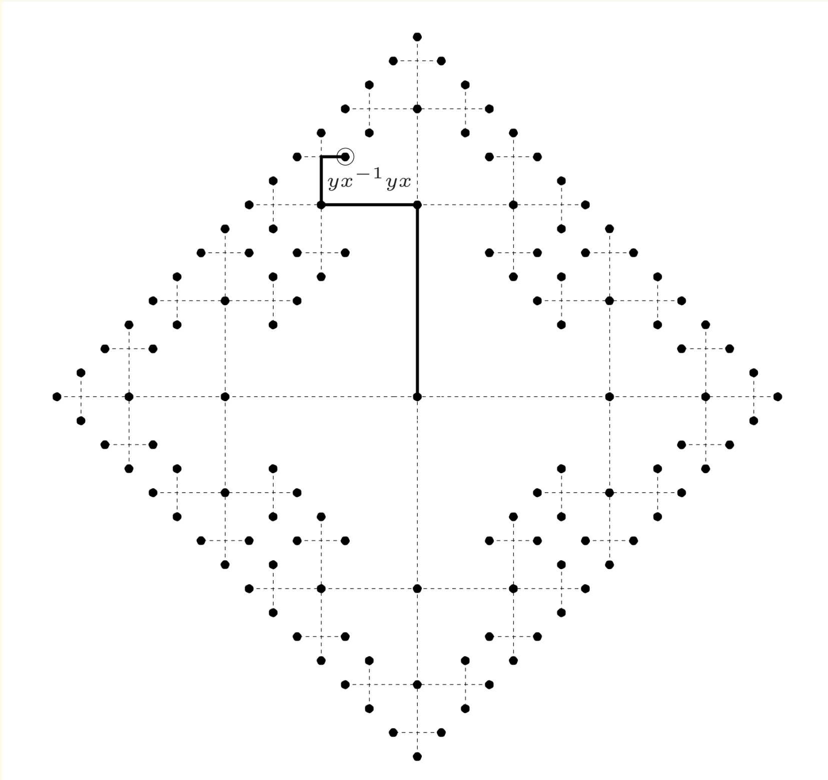
显然，$(T^*, \cdot)$ 构成一个群结构（乘法符合结合律；有幺元，即空字符串；每个字符串都有逆元），称该群为集合 S 生成的**自由群**.

命题 3.45 设 S 是一个集合，F_S 是它生成的自由群，函数 $\iota : S \to F_S, \text{'}a\text{'} \mapsto \text{"}a\text{"}$. 则 (F_S, ι) 满足 S 上的自由群的泛性质.

命题 3.46 $F(\emptyset)$ 是平凡群.

命题 3.47 $F(\{*\}) \cong$ 无限循环群 $\cong (\mathbb{Z}, +)$.

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 $\mathcal{F}_S^{\mathbf{Ab}}$：

$$\operatorname{Obj}(\mathcal{F}_S^{\mathbf{Ab}}) := \left\{(G,\iota) \mid G \in \operatorname{Obj}(\mathbf{Ab}), \iota : (S \to G)_{\mathbf{Set}}\right\},$$

$$(G_1,\iota_1) \to (G_2,\iota_2) := \left\{\varphi : (G_1 \to G_2)_{\mathbf{Ab}} \mid \varphi \circ \iota_1 = \iota_2\right\}.$$

$$\begin{tikzcd}
S \arrow[r, "\iota_1"] \arrow[dr, "\iota_2"'] & G_1 \arrow[d, "\varphi"] \\
& G_2
\end{tikzcd}$$

集合 S 上的**自由交换群** $\boldsymbol{F}^{\mathbf{Ab}}(\boldsymbol{S})$ 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）.

$$\begin{tikzcd}
S \arrow[r, "\iota"] \arrow[dr, "f"'] & \boldsymbol{F}^{\mathbf{Ab}}(\boldsymbol{S}) \arrow[d, dashed, "\varphi"] \\
& G
\end{tikzcd}$$

定义 3.28 $\mathbb{Z}^{\oplus n}$

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

1. $\mathbb{Z}^{\oplus 0} := \{$空元组$\}$，令其为平凡群；

2. 如果 $n > 0$，则 $\mathbb{Z}^{\oplus n} := \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{\text{n 次}}$，并定义其上二元运算 $+ : \mathbb{Z}^{\oplus n} \times \mathbb{Z}^{\oplus n} \to \mathbb{Z}^{\oplus n}, (x_1,\dots,x_n) + (y_1,\dots,y_n) := (x_1+y_1,\dots,x_n+y_n)$.

显然，这构成一个群.

命题 3.48 1. 设函数 $\iota : \emptyset \to \mathbb{Z}^{\oplus 0}$. 则 $(\mathbb{Z}^{\oplus 0},\iota)$ 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 $\iota : S \to \mathbb{Z}^{\oplus n}, i \mapsto \left(0,\dots,0,\underbrace{1}_{\text{第 i 位}},0,\dots,0\right)$. 则 $(\mathbb{Z}^{\oplus n},\iota)$ 满足 S 上的自由交换群的泛性质.

定义 3.29 $\boldsymbol{H}^{\oplus S}$

设 S 是一个集合，$(H,+)$ 是一个交换群.

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

显然 $\left(\boldsymbol{H}^{\oplus S}, +\right)$ 是交换群.

命题 3.49 设 S 是一个集合，函数 $\iota : S \to \mathbb{Z}^{\oplus S}, \iota(s) := (x \in S) \mapsto \begin{cases} 1, x=s \\ 0, x\neq s \end{cases}$. 则 $\left(\mathbb{Z}^{\oplus S}, \iota\right)$ 满足 S 上的自由交换群的泛性质.

3.8 子群

3.8.1 定义和例子

定义 3.30 **子群**

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

$(H,\bullet)$ 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 3.50 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 $\varphi : G \to G'$ 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 $\varphi : G \to G'$ 的**核**定义为：

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

命题 3.51 设 $\varphi : G \to G'$ 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'，$\varphi^{-1}(H')$ 是 G 的一个子群.

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

命题 3.52 设 $\varphi : G \to G'$ 是一个群同态. 定义一个范畴 $\mathcal{C}$:

$$\mathrm{Obj}(\mathcal{C}) := \left\{ (K, \alpha) \mid K \in \mathrm{Obj}(\mathbf{Grp}),\ \alpha : (K \to G)_{\mathbf{Grp}},\ \alpha(K) \subset \ker\varphi \right\},$$

$$(K, \alpha) \to (L, \beta) := \left\{ \gamma : (K \to L)_{\mathbf{Grp}} \mid \alpha = \beta \circ \gamma \right\}.$$

设 $i : \ker\varphi \to G$ 是包含映射.

则 $(\ker\varphi, i)$ 是范畴 $\mathcal{C}$ 的终对象，如下图：

$$\begin{tikzcd}
K \arrow[r, "\alpha"'] \arrow[rr, bend left, "0"] \arrow[dr, dashed, "\bar{\alpha}"'] & G \arrow[r, "\varphi"'] & G' \\
& \ker\varphi \arrow[u, hook, "i"'] &
\end{tikzcd}$$

定义 3.32 **生成子群**

第 1 种定义：

如果 A 是群 G 的一个子集，$i : A \to G$ 是包含映射，$(F(A), \iota)$ 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 $\varphi : F(A) \to G$ 使得下图交换

$$\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[dr, "i"'] & F(A) \arrow[d, dashed, "\varphi"] \\
& G
\end{tikzcd}$$

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：

$$a_1 a_2 ... a_3,$$

其中每个 a_i 是 A 中的元素，或 A 中的元素的逆，或 G 的幺元.

第 3 种定义：

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

命题 3.53 设 A 是交换群 G 的一个子集，$i: A \to G$ 是包含映射，$(F(A), \iota_1)$ 和 $\left(F^{\mathbf{Ab}}(A), \iota_2\right)$ 分别是范畴 $\mathcal{F}_A$ 和 $\mathcal{F}_A^{\mathbf{Ab}}$ 的始对象，$\varphi_1: (F(A), \iota_1) \to (G, i)$，$\varphi_2: \left(F^{\mathbf{Ab}}(A), \iota_2\right) \to (G, i)$，$\varphi_3: (F(A), \iota_1) \to \left(F^{\mathbf{Ab}}(A), \iota_2\right)$. 那么我们有

$$\varphi_2 \circ \varphi_3 = \varphi_1.$$

命题 3.54 设 A 是交换群 G 的一个子集，$i: A \to G$ 是包含映射，$\left(F^{\mathbf{Ab}}(A), \iota\right)$ 是范畴 $\mathcal{F}_A^{\mathbf{Ab}}$ 的始对象，下图交换：

$$\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[dr, "i"'] & F^{\mathbf{Ab}}(A) \arrow[d, dashed, "\varphi"] \\
 & G
\end{tikzcd}$$

那么，$\varphi\left(F^{\mathbf{Ab}}(A)\right)$ 是群 G 中由子集 A 生成的子群.

定义 3.33 称一个群 G 是**有限生成**的，当且仅当存在有限子集 $A \subset G$ 使得 $G = \langle A \rangle$.

命题 3.55 对于任意循环群 G，都存在 $g \in G$ 使得 $G = \langle g \rangle$.

命题 3.56 设 G 是一个群. 则以下 2 个命题等价：

1. G 是有限生成的.
2. 存在满群同态 $F(\{1, ..., n\}) \twoheadrightarrow G$（$n \geq 0$）.

命题 3.57 设 G 是一个交换群. 则以下 3 个命题等价：

1. G 是有限生成的.
2. 存在满群同态 $F(\{1, ..., n\}) \twoheadrightarrow G$（$n \geq 0$）.
3. 存在满群同态 $F^{\mathbf{Ab}}(\{1, ..., n\}) \twoheadrightarrow G$（$n \geq 0$）.

命题 3.58 设 $A = \{'1', ..., 'n'\}$（$n \geq 0$），G 是一个群且 $|G| \geq n$，$\varphi: F(A) \to G$ 是一个满群同态. 那么 $|\varphi(\{"1", ..., "n"\})|$ **不一定**等于 n.

命题 3.59 设 $A = \{1, ..., n\}$（$n \geq 0$），G 是一个交换群且 $|G| \geq n$，$\varphi: F^{\mathbf{Ab}}(A) \to G$ 是一个满群同态. 那么 $|\varphi(\{(1,0,...,0), (0,1,...,0), ..., (0,0,...,1)\})|$ **不一定**等于 n.

定义 3.34 设 $d \in \mathbb{Z}$. 我们定义

$$d\mathbb{Z} := \{m \in \mathbb{Z} \mid m \text{ 是 } d \text{ 的整数倍}\}.$$

命题 3.60 设 G 是 $(\mathbb{Z},+)$ 的一个子群. 那么存在 $d\in\mathbb{Z}$ 使得 $G=d\mathbb{Z}$.

命题 3.61

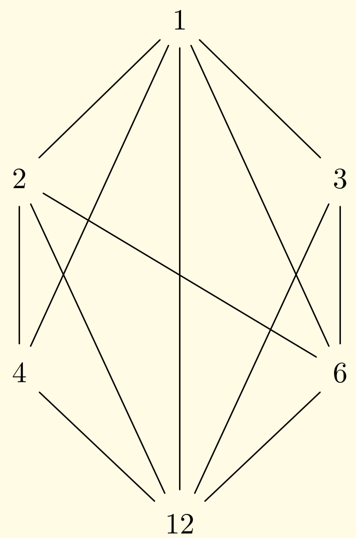
1. n 阶循环群 $\cong(\mathbb{Z}/n\mathbb{Z},+)$;
2. $F(\{*\})\cong$ 无限循环群 $\cong(\mathbb{Z},+)$ 的所有非平凡子群.
3. 从 n 阶循环群到无限循环群的群同态有且只有平凡同态.

命题 3.62 $F(\{*\})$ 的任何子群都是自由群.

命题 3.63 设 G 是某个 n 阶循环群的一个子群. 那么存在 n 的因子 d，使得 G 是由 $[d]_n$ 生成的 n/d 阶循环群.

命题 3.64 如果 d_1,d_2 都整除 n，且 d_1 整除 d_2，那么 $\langle[d_1]_n\rangle\supset\langle[d_2]_n\rangle$.

例子 3.4 上个命题中的整除关系和包含关系分别构成了一个**格**结构，且这两个格是同构的. 以 12 阶循环群为例，我们有下图所示的格：



命题 3.65 设 G 是一个群，$g\in G$. 则指数映射 $\varepsilon_g:\mathbb{Z}\to G$ 的像是一个循环群.

3.8.2 单态射

命题 3.66 设 $\varphi:(G\to G')_{\mathbf{Grp}}$. 则以下命题等价：

1. φ 是单态射;
2. $\ker\varphi=\{e_G\}$;
3. φ 是单射.

命题 3.67 设 $\varphi:(G\to G')_{\mathbf{Grp}}$. 则 φ 是单态射 $\Rightarrow\varphi$ 有左逆.

3.9 商群

3.9.1 商群

定义 3.35 **兼容**

设 $G \in \mathbf{Grp}$，$\sim$ 是 G 上的一个等价关系.

如果该关系满足：

$$\forall a, a' \in G.\ (a \sim a') \Rightarrow \forall g \in G.\ (ga \sim ga') \wedge (ag \sim a'g),$$

那么我们称在群 G 中，等价关系 $\sim$ **兼容**于群结构.

定义 3.36 **商群**

设 $G \in \mathbf{Grp}$，$\sim$ 是 G 上的一个兼容的等价关系.

那么我们可以定义二元运算 $\bullet : (G/{\sim}) \times (G/{\sim}) \to (G/{\sim})$,

$$[a]\bullet[b] := [ab].$$

显然这使得 $(G/{\sim})$ 成为一个群. 我们称群 $(G/{\sim})$ 是群 G 关于等价关系 $\sim$ 的**商群**.

定义 3.37 $\mathbf{Grp}/{\sim}$

设 $G \in \mathbf{Grp}$，$\sim$ 是 G 上的一个兼容的等价关系.

定义范畴 $\mathbf{Grp}/{\sim}$：

$$\mathrm{Obj}(\mathbf{Grp}/{\sim}) := \left\{(G', \varphi) \mid G' \in \mathrm{Obj}(\mathbf{Grp}),\ \varphi : (G \to G')_{\mathbf{Grp}},\ \forall a, b \in G.\ a \sim b \Rightarrow \varphi(a) = \varphi(b)\right\},$$

$$(G_1, \varphi_1) \to (G_2, \varphi_2) := \left\{\sigma : (G_1 \to G_2)_{\mathbf{Grp}} \mid \sigma \circ \varphi_1 = \varphi_2\right\}.$$

命题 3.68 设 $G \in \mathbf{Grp}$，$\sim$ 是 G 上的一个兼容的等价关系，$\pi : G \to G/{\sim}, x \mapsto [x]$.

则 $(G/{\sim}, \pi)$ 是 $\mathbf{Grp}/{\sim}$ 的始对象，如下图：

$$\begin{tikzcd}
G \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & \mathbf{Grp}/{\sim} \arrow[d, dashed, "\tilde{\varphi}"] \\
& G'
\end{tikzcd}$$

命题 3.69 给定集合 A，设 $(F(A), \iota_1)$ 和 $\left(F^{\mathbf{Ab}}(A), \iota_2\right)$ 分别是范畴 $\mathcal{F}_A$ 和 $\mathcal{F}_A^{\mathbf{Ab}}$ 的始对象.

定义 $F(A)$ 上的一个等价关系：

$$\sim : F(A) \times F(A) \to \mathbf{Propo},$$

$$a \sim b :\Leftrightarrow \text{字符串 } a \text{ 和 } b \text{ 中的字符种类和数量相同，唯一可能的不同是字符的顺序.}$$

则我们有：

1. $\sim$ 兼容于 $F(A)$ 的群结构.

2. 存在同构 $\alpha : F^{\mathbf{Ab}}(A) \xrightarrow{\sim} F(A)/{\sim}$ 使得下图交换：

$$\begin{tikzcd}
A \arrow[r, "\iota_1"] \arrow[dr, "\iota_2"'] & F(A) \arrow[r, "\pi"] \arrow[d, dashed, "\varphi"'] & F(A)/{\sim} \arrow[dl, "\alpha"] \\
& F^{\mathbf{Ab}}(A) &
\end{tikzcd}$$

3.9.2 正规子群

定义 3.38 **正规子群**

称群 G 的一个子群 N 是**正规的**，当且仅当

$$\forall g \in G.\ gNg^{-1} \subset N.$$

命题 3.70 交换群的任何子群都是正规的.

引理 3.4 设 $\varphi : (G \to G')_{\mathbf{Grp}}$. 则 $\ker \varphi$ 是 G 的正规子群.

3.9.3 陪集