Algebra:Chapter 0:Group

颜成子游

2022 年 9 月 24 日

目录

1 群的定义

1.1 群与群胚

定义 1.1 群是只有一个元素的群胚。

这与我们平常对群的定义并不一致。但是这是自然的。我们会注意到，群胚可能有多个元素。在群胚的态射集中，并非所有态射都能复合。但是如果群胚只有一个元素，情况就完全不同了：这时所有的态射都是：

$$Hom_G(*,*)$$

这些态射都能相互作用。在这种情况下，态射作为元素就构成了群。也就是说群是单元素群胚的态射集。

群的一般定义不再此处赘述：可逆的半幺集合

群的例子将在之后一起给出。

1.2 群的基础性质

命题 1.1 群的幺元是唯一的。

命题 1.2 群每个元素的逆元都是唯一的。

命题 1.3 设 G 是一个群。对于 $\forall a, gh \in G$，则有：

$$ga = ha \Rightarrow g = h$$

同理，左消去律也是成立的。

命题 1.4 交换群 G 是一个 $\mathbb{Z}-$ 模。

证明 直接使用模的定义即可。只需要定义 $(n, a) \mapsto na$。 □

命题 1.5 有限群的元素的阶是有限的。另一方面，设 g 的阶是 n。若 $g^N = e$，则 $n|N$.

命题 1.6 设 g 是群 G 的有限阶元。那么对于任何 m，g^m 的阶为：

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

命题 1.7 若 $gh = hg$，那么 $|gh|$ 整除 $lcm(|g|, |h|)$

证明 $(gh)^n$ 可以写 $g^n h^n$。因为 g, h 交换。我们只用 gh 的 $\mathrm{lcm}(|g|, |h|)$ 次幂为 e。这是显然的。 □

2 群的例子

例 2.1 平凡群：$\{e\}$。是最简单的群。

例 2.2 $Gl(n,\mathbb{R})$ 表示所有可逆 n 阶矩阵。考虑乘法，其构成群。

2.1 对称群

定义 2.1 设 A 是一个集合。那么 A 的自双射群:

$$Aut_{Set}(A)$$

构成一个群。我们用 S_A 来表示该群，并且称之为对称群。如果 A 是有限集合，元素个数为 n, 那么 S_A 也记为 S_n。

例 2.3 考率集合元素个数为 3 的集合的对称群：S_3。容易得到 S_3 的结构为：

$$e, x, y, y^2, xy, xy^2$$

其中 $x = (12)$,$y = (132)$. 可以验证 x 阶 2，y 阶 3. 并且 $yx = xy^2$。

我们也说 $\{x, y\}$ 生成了 S_3. 生成的定义之后给出。

2.2 二面体群

定义 2.2 对于平面上的正 n 面体，D_{2n} 表示其所有的对称变换所构成的集合，其是一个群。并且可以证明，D_{2n} 的阶为 $2n$。其中包含 n 个对称旋转和 n 个绕某顶点的镜面反射。

例 2.4 观察 D_6. 这是一个典型的 6 元素群。之后会讲到，6 元素的集合有两类。对于 D_6，可以证明与 S_3 同构。证明方法如下：

证明 给三角形的三个顶点标号为 $1, 2, 3$。那么 D_6 中的任何一个元素都把 $1, 2, 3$ 进行了一个置换，即存在映射：

$$\sigma : D_6 \to S_3$$

这是群的同态。我们只需要说明其为单射。这是明显的，因为一旦确定了点的映射关系，这样的对称变换就确定了。 □

推论 2.1 对于 D_{2n}，同样存在一个单同态 $\sigma : D_{2n} \to S_n$。但不是满的。可以想象 $n = 4$ 的时候。此时如果交换的只有领边的两个点，那么实际上已经改变了正方形的结构，这对应不了一种变换。同理，如果取的是三个点，也改变了结构，于是不能对应。正好有 4+12+8 个即 24 个。

2.3 循环群

定义 2.3 形如 $\{e, a, a^2, \ldots, a^{n-1}\}$ 的群被称为循环群。循环群的阶 n 唯一确定了循环群。

关于循环群，有以下结论：

命题 2.1 a^m 的阶是：

$$\frac{n}{\gcd(m,n)}$$

推论 2.2 a^m 生成循环群，当且仅当 $\gcd(m,n)=1$

命题 2.2 考虑 n 阶循环群，去除 e 后构成的集合：

$$\{a, a^2 \ldots, a^{n-1}\}$$

定义运算:$a^m \cdot a^n = a^{m\times n}$。则该集合构成群。

证明 先验证运算的合理性。考虑:

$$m = kn + m'e = jn + e'$$

则 me 与 $m'e'$ 同余。

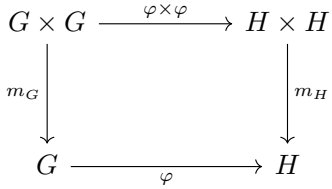
现在验证可逆元。只需要验证对 $\forall m \in \mathbb{N}$, 都存在 n 使得 mn 与 1 同余。这是比较显然的。 □

3 群范畴

根据我们粗浅的范畴论知识，可以把所有的群看为范畴论中“群范畴”的对象。而他们之间的态射则是我们熟知的“群同态”。

3.1 群同态

定义 3.1 集合函数 $\varphi : G \to H$ 定义了一个群同态若下列交换图成立：

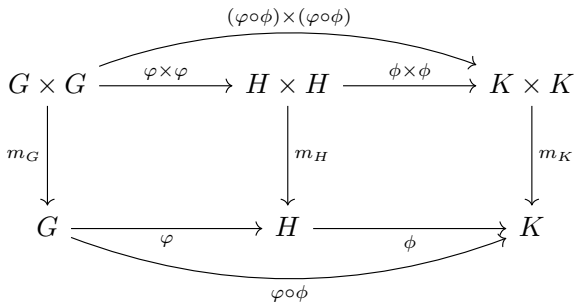


同样这和我们通常关于同态的定义略有不同。但实际仔细比对就会发现他们是一样。只是用交换图更加适应之后的学习。

使用交换图的好处是，我们可以显而易见的得到同态的复合还是同态的结论：

命题 3.1 群同态的复合还是群同态.

证明



□

命题 3.2 群同态把幺元映射到幺元，把逆元映射到逆元.

3.2 群同态的例子

对于任意两个群 G, H, 其同态集合:

$$Hom_{Grp}(G, H)$$

显然不可能是空集. 因为至少有:

$$G \to \{*\} \to H$$

因为 $\{*\}$ 是群范畴的终始对象. 我们把这样的同态称为平凡同态.

例 3.1 *群作用: 群 G 作用在一个对象 A 上, 意味着存在一个同态:*

$$G \to Aut_C(A)$$

如果 C 是集合范畴, 那么 G 的元素就可以对应集合 A 的一个排列.

例如 $D_{2n} \to S_n$. 这就是典型的群作用.D_{2n} 作用在 $1, 2, \ldots, n$ 上进行重排. 这还是一个单同态.

例 3.2 *下列同态也是比较自然的:*

$$\epsilon_g : Z \to G, a \mapsto g^a$$

例 3.3 *对于循环群 $\mathbb{Z}/n\mathbb{Z}$, 定义 π_n:*

$$a \mapsto a[1]_n$$

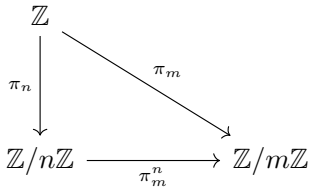
这是满射, 意味着 $[1]_n$ 可以生成 $\mathbb{Z}/n\mathbb{Z}$.

假设 $m|n$(这是必要的), 那么就存在同态 π_m^n:

$$\pi_m^n([a]_n) = [a_m]$$

这个同态需要验证其定义的合理性. 这是容易的.

结合 π_m, π_n, 我们还有交换图:



例 3.4 *如果 m_1, m_2 都是 n 的因子, 那么就有:*

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

的同态. 有时候这样的同态能得到相当好的结果:

$$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

验证这是一个双射即可.

3.3 同态和阶

本节的主要结果为:

命题 3.3 设 $\varphi : G \to H$ 是一个群同态,g 是有限阶元素. 那么 $|\varphi(g)|$ 整除 $|g|$.

用这个结果可以很容易判断一些非平凡的同态的不存在性. 比如不存在从 $\mathbb{Z}/7\mathbb{Z}$ 到 $\mathbb{Z}/4\mathbb{Z}$ 的非平凡同态. 因为前者元素的阶都是 7. 后者元素的阶都不整除 7.

3.4 同构

定义 3.2 群范畴里的同构就是群的同构.

例 3.5 之前我们说循环群时,$G = \{e, a, \ldots, a^{n-1}\}$. 不同的 a 带来的群是不一样的. 但是只要做映射:

$$\varphi : a \mapsto b$$

就可以验证, 所有同阶的循环群都是同构的, 同构于 $\mathbb{Z}/n\mathbb{Z}$.

从而 $C_2 \times C_3$ 是 6 阶循环群, 因为其同构于 C_6. 一般的, 如果 m, n 互素, 那么 $C_m \times C_n$ 也是循环群.

证明 只需要证明其中有一个 mn 阶元. 事实上,$([1]_m, [1]_n)$ 就是 mn 阶元. □

下面这个结论不给出证明, 证明留到之后来说.

命题 3.4 $(\mathbb{Z}/p\mathbb{Z})*$ 是循环群.

同构的群群结构完全一致. 因此:

(1) 交换群的同构是交换的.

(2) 对应元素的阶相同.

下面这个定理也是比较出人意料的:

定理 3.1 两个有限的交换群同构, 当且仅当对于任何的整数 m, 他们都有相同个数的元素的阶是 m.

这个玩意儿现在也没法证, 记住就好.

并且不交换的反例也是有的.

3.5 Abel 群的同态

命题 3.5 设 G, H 是群, 且 H 是交换群. 那么同态集合:

$$Hom_{Grp}(G, H)$$

是一个群.

3.6 群范畴

我们把两个群之间的同态看为态射. 群本身看为对象. 由此我们得到了群范畴:Grp.

群范畴有如下命题:

命题 3.6 *平凡群是终, 始对象.*

证明 终对象是显然的. 对于始对象, 由于群同态保持幺元, 则 $\varphi(*) = e$. □

命题 3.7 *群范畴中的积是两个群的直积.*

证明 对交换图进行验证即可. □

余积也是有的. 但是涉及到代数拓扑, 这里就不讨论了.

对于 Abel 群, 也形成了 Abel 范畴. 在 Abel 范畴下, 余积和积恰好重合. 但是就算 G, H 都交换, 也不能说明其 $G \times H$ 是群范畴下的余积.

4 自由群

4.1 动机

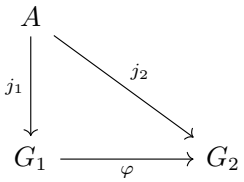
自由群的动机是什么? 什么是自由? 在物理世界里面, 纯粹的自由是没有任何物理规律的自由. 同样, 在群里面, 自由是没有任何外加等式的自由.

给定一个普通集合 A, 它所构造的自由群是里面的元素自由组合的结构.

4.2 Universal property

定义 4.1 *给定集合 A,A 的自由群 $F(A)$ 是 $\mathcal{F}^A$ 范畴中的始对象. 其中 $\mathcal{F}^A$ 的对象为有序对 (j, G). 其中 j 是从 A 到 G 的映射,G 是一个群.*

对象之间态射是从 $G_1 \to G_2$ 的同态, 且满足下列交换图:



根据定义, 很容易推得自由群的唯一性 (同态). 但是存在性呢?

存在性不在此赘述. 其构造本身没有太大意义. 有意义还是自由群的抽象含义和具体含义.

4.3 自由 Abel 群

我们也可以用同样的方式给出自由 Abel 群的定义.

对于自由 Abel 群的存在性, 问题显得简单得多.

命题 4.1 *对于元素个数为 n 的有限集合 A, 其对应的自由 Abel 群为:*

$$\mathbb{Z}^{\oplus n}$$

命题 4.2 假设 A 是任意给定的集合. 我们已经知道,H^A(从 A 到 H 的所有映射) 是一个自然的 *Abel* 群, 如果 H 是一个 *Abel* 群.

我们定义 H^A 的子集:

$$H^{\oplus A} = \{\alpha : A \to H | \alpha(a) \neq e_H for\ only\ finitely\ many\ elements \quad a \in A\}$$

则 $F^{ab}(A)$ 存在, 且一种构造方法是 $\mathbb{Z}^{\oplus A}$

证明 注意到 $\mathbb{Z}^{\oplus A}$ 中的任何一个元素都可以写为:

$$\sum_{a \in A} m_a j_a$$

且其中的 m_a 只有有限个不为零.(因为目前代数只能处理有限和).

对于任何一个 H 为 Abel 群,$k : A \to H$ 是伴随的映射. 我们定义映射 $\varphi : \mathbb{Z}^{\oplus A} \to H$:

$$\varphi(\sum_{a \in A} m_a j_a) = \sum_{a \in A} m_a k(a)$$

容易验证这是一个同态.

为了说明这个同态是唯一的, 我们可以考虑:

$$\varphi(j_a) = k(a)$$

为了满足交换图, 这是必须的. 而为了满足同态, 就必须按照上述方式定义所有的元素像. 从而该同态唯一. □

5 子群

5.1 定义, 判定

定义 5.1 称 $(H, *)$ 是 $(G, \cdot)$ 的子群, 若映入映射 $i : H \to G$ 是群同态.

命题 5.1 G 是一个群. 其子集 H 是其的子群, 当且仅当 $\forall a, b \in H, ab^{-1} \in H$.

命题 5.2 子群的任意交还是子群.

证明 交都包含 e, 非空. 根据上面命题可得. □

命题 5.3 设 $\varphi : G \to G'$ 是群同态,H' 是 G' 的子群, 那么 $\varphi^{-1}(H')$ 是 G 的子群.

证明 只需验证即可. □

5.2 核与像

5.2.1 定义

每个同态都能生成两个子群:

定义 5.2 $\varphi : G \to G'$ 的核定义为:

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

由于子群的原像也是子群. 因此同态的核也是子群.

命题 5.4 群同态如上定义. 则 G 的任何子群的像都是 G' 的子群.

证明 取 $\varphi(a), \varphi(b) \in G'$, 则 $\varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(H)$ □

从上述命题知, 同态的像也是子群.

对于核和像, 下面的性质是重要的:

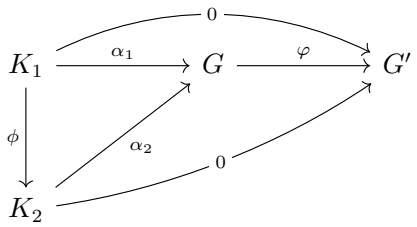
定理 5.1 设 $\varphi : G \to G'$ 是同态. 则映入映射 $i : ker\varphi \hookrightarrow G$ 是范畴 C:

对象: 所有使得 $\varphi \circ \alpha$ 是平凡同态的群同态:$\alpha : K \to G$;

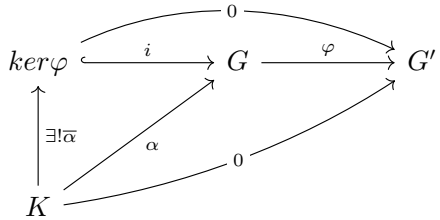
态射:K_1, K_2 之间的同态 ϕ, 并且使得:$\alpha_2 \circ \phi$ 与 α_1 在 K_1 上相同.

的终对象.

我们用下列交换图来表示这个范畴:



证明 要证明的是下列交换图:



对于 $\overline{\alpha}$, 由于 $\alpha(K) \subset \ker G$, 所以其与 α 没有本质的差别. 从而存在性显然. 而对于唯一性, 考虑到交换图成立, 因此 $\overline{\alpha}(k) = \alpha(k)$. 因此这也是其唯一的定义方式. □

这个定理展示了如何在极度抽象的情况下定义核. 或者对于其他的代数结构, 能否定义核.

任何一个集合函数 $\alpha : K \to G$ 使得 $\varphi \circ \alpha$ 是平凡同态, 作为集合函数必须通过 $\ker\varphi$ 分解.

5.3 子群的例子

6 共轭作用

群其中一个“闪耀”的点在于其可以产生群作用，使其与非群的集合也能产生联系。虽然其本质是从 G 到 S 的对称群的群同态。

由于任何一个可递的作用都可以被看成是对群中某子群左陪集集合的左乘作用。其中子群是任何一个 $a \in S$ 的稳定子：$Stab_G(a)$。

如果我们就此研究特殊的群作用——共轭作用，会得到什么样的结果呢？

为了简便，我们记 G_a 是 $a \in S$ 的稳定子。

$$Z = \{a \in S | \forall g \in G, ga = a\}$$

为所有固定点的集合。如果 $a \in Z$, 那么其稳定子是整个群。如果 $a \in Z$, 那么其轨道也是平凡的。

6.1 稳定子定理

命题 6.1 设 S 是一个有限集合，G 作用在 S 上。那么：

$$|S| = |Z| + \sum_{a \in A} [G : G_a]$$

证明 我们注意到轨道是 S 上的一个等价关系。S 上的点分为平凡轨道和一些非平凡的轨道。平凡轨道的个数 $|Z|$。每个非平凡的轨道的元素个数为 $[G : G_a]$。因此 A 表示所有轨道中代表元的集合。 □

这个公式在我们已知 G 的阶数，尤其是素数或者素数的方后变得很有用。

定义 6.1 称 G 是一个 p 群，如果其的阶是 p 的某次方。p 是素数。

命题 6.2 条件与上述命题相同，G 是 p 群。则 S 与 Z 关于 p 同余。

从而我们可以借此证明 $|Z|$ 的一些情况。比如如果 S 不是 p 的倍数，那么 Z 不是空集。

6.2 中心子，共轭类

我们现在考虑群 G 到自身的作用——共轭作用。即：

$$(g, h) \mapsto ghg^{-1}$$

共轭作用的固定点集合，即 G 中在任何 g 作用下都保持不变：

$$ghg^{-1} = h \Rightarrow gh = hg$$

定义 6.2 G 的中心子 $Z(G)$ 被定义为共轭作用中的 G 的固定点集合。同时其也是 $\sigma : G \to S_G$ 的核。$Z(G)$ 的元素与群的任何元素都交换。

作为核，中心子天然是正规子群，这也很容易手动验证。交换群的中心子是其本身。此时共轭作用 σ 变为平凡同态。

引理 6.1 有限群 G。若 $G/Z(G)$ 是循环群，那么 G 是交换群。

证明 考虑 G 中的元素都可以写为 $g^m h.h$ 是中心的元素。于是：

$$g^n h_1 g^m h_2 = g^{m+n} h_2 h_1 = g^m h_2 g^n h_1$$

现在考虑单个元素的稳定子：

定义 6.3 $Z_G(a)$ 表示共轭作用下 a 的稳定子。其包含所有与 a 交换的元素。其个数大于 a 的阶。

定义 6.4 a 在共轭作用下的轨道称为 a 的共轭类。我们记为 $[a]$。a 的共轭类是 a 本身，如果其属于 $Z(G)$。

6.3 Class Formula

我们把群 G 和共轭作用带入稳定子定理：

命题 6.3 设 G 是有限群。则：

$$|G| = |Z(G)| + \sum_{a \in A} [G : Z(a)]$$

于是我们可以得到以下关于 $|G|$ 的推论：

推论 6.2 G 是非平凡 p 群。那么 G 有非平凡的中心。

推论 6.3 若 G 的阶是 p^2，那么其是交换群。

证明 中心不可能平凡，则只可能为 p 或者 p^2 个。因为中心是正规子群。若为 p, 则 $G/Z(G)$ 是 p 阶群，为循环群，从而 G 是交换群，与 p 矛盾。 □

使用这个公式我们还可以得到 6 阶非循环群的性质。实际上其只可能与 S_3 同构。

命题 6.4 6 阶非交换群只可能为 S_3

证明 首先考虑其 class formula 的写法。由于非交换，则中心只能是 1. 那么剩下只能写为 $2 + 3\,6 = 1 + 2 + 3$.

其次，我们断言群中一定有 3 阶元。若不然，则除幺元外都是 2 阶元：

$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$$

矛盾。

设 y 为 3 阶元。我们考虑其所在的共轭类。显然 y 的中心子至少有 3 个。因此其只能在 2 中，y^2 也是如此。

对于 $1+2+3$，我们断言 3 中有 2 阶元。这很容易说明。设 x 是一个 2 阶元。于是 xy, xy^2, yx, y^2x 表示了最后两个元。显然 $xy \neq yx$，因为 y 的中心子只有 e, y, y^2。于是剩下两个元为 xy, xy^2 且：

$$yx = xy^2$$

这正好是 S_3 的结构。 □

6.4 子集和子群的共轭类

定义 6.5 A 的正规化子 $N_G(A)$ 是其在共轭作用下的稳定子。即：

$$N_G(A) = \{g \in G | gAg^{-1} = A\}$$

A 的中心子 $Z_G(A)$ 是保持 A 中每个元素在共轭作用下都不变的子群。显然 $Z_G(A) \subset N_G(A)$.

显然 $A \subset N_G(A)$，若 A 是子群。下列关系式是常用的：

$$[G : A] = [G : N_G(A)][N_G(A) : A]$$

$N_G(A)$ 是一个正规子群。这一点可以很容易验证。

命题 6.5 H 作为子群的共轭类个数等于 $[G : N_G(H)]$ 的个数。

从而可以看到 H 的共轭类个数是要小于左陪集个数的。