群论基础

朱彬

中山大学智能工程学院

zhub26@mail.sysu.edu.cn

2023 年 5 月 – 6 月

References

基础部分主要参考：Lang, Undergraduate Algebra, third edition, Ch. II, Springer.

Burnside 引理（难点）参考：Rotman, An Introduction to the Theory of Groups, fourth edition, Ch. 3, pp. 58–61, GTM 148, Springer（国内有影印版）.

群论的简要历史

See, e.g., Rotman, pp. 1–2.

动机：二次方程求根公式的推广。

重要的名字：

- J. L. Lagrange (1770)
- P. Ruffini, P. Abbati (~1800)
- A. L. Cauchy (1815)
- N. H. Abel (1824，当时 22 岁)
- E. Galois (1830，当时 19 岁)

定义 (群 (group))

群 G 包括一个集合和一条规则（也称“运算”，叫做**复合律**，law of composition），该规则把 G 中每对元素 x, y 都关联到一个 G 中元素，后者用 xy 表示，且满足如下性质：

1. 对于任意 G 中元素 x, y, z，我们有结合律 (associativity)：
$$(xy)z = x(yz).$$
2. G 中存在一个元素 e，使得 $ex = xe = x$ 对于所有 $x \in G$ 都成立。
3. 如果 $x \in G$，那么存在一个元素 $y \in G$，使得 $xy = yx = e$。

严格地说，上面定义的群 G 称为**乘法群** (multiplicative group)。

如果我们把 G 中的规则写作加法形式，即 $(x, y) \mapsto x + y$，那么性质 1–3 需要改写为：

1. 对于任意 G 中元素 x, y, z，我们有

$$(x + y) + z = x + (y + z).$$

2. G 中存在一个元素 0，使得 $0 + x = x + 0 = x$ 对于所有 $x \in G$ 都成立。
3. 给定任意 $x \in G$，那么存在一个元素 $y \in G$，使得 $x + y = y + x = 0$。

如此，我们称 G 为**加法群** (additive group)，称 $x + y$ 为**和** (sum)。

但是，我们只在群 G 满足一个额外的性质时才会使用 $+$ 记号。该规则称为**交换律** (commutativity)，即对于任意元素 $x, y \in G$ 有

$$x + y = y + x.$$

该性质用乘法记号写作：对于任意 $x, y \in G$，有 $xy = yx$。

如果 G 拥有这个性质，我们称它为**交换群** (commutative group) 或**阿贝尔群** (abelian group)。

例 (1)

用 $\mathbb{Q}$ 表示有理数的集合，它包含所有的分数 m/n，其中 m, n 为整数且 $n \neq 0$。那么

- $\mathbb{Q}$ 在加法运算下是一个群。
- $\mathbb{Q}$ 中的非零元素在乘法运算下构成一个群，用 $\mathbb{Q}^*$ 来表示。

例 (2)

实数集（实直线）$\mathbb{R}$ 和复数集（复平面）$\mathbb{C}$ 在加法运算下都是群。非零实数和非零复数在乘法运算下构成群，分别用 $\mathbb{R}^*$ 和 $\mathbb{C}^*$ 来表示。

例 (3)

绝对值（模，modulus）为 1 的复数在乘法运算下构成一个群，即复平面上的单位圆 $\mathbb{T} = \{e^{i\theta} = \cos\theta + i\sin\theta : \theta \in [0, 2\pi)\}$。

例 (4)

由 $1, -1$ **两个**元素构成的集合在乘法运算下是一个群。

例 (5)

由数字 $1, -1, i, -i$ 构成的集合在乘法运算下是一个群，它有**四个**元素。

群的一些简单性质。

Proposition

令 G 为一个群，那么由群的性质 2 保证存在的元素 e 是唯一确定的。

证明.

如果 e, e' 都满足群的性质 2，那么有

$$e' = ee' = e.$$

□

该元素称为 G 的**单位元** (unit element)。在加法记号下，我们称之为**零元** (zero element)。

Proposition

令 G 为一个群，且 $x \in G$。那么满足 $yx = xy = e$ 的元素 y 能被唯一确定。

证明.

如果（某个）z 也满足 $zx = xz = e$，那么有

$$z = ez = (yx)z = y(xz) = ye = y.$$

□

我们称元素 y 为 x 的**逆** (inverse)。在加法记号下，它写作 $y = -x$。

例 (6. 直积 (direct product))

令 G, G' 为群，定义笛卡尔积 (Cartesian product)

$$G \times G' := \{(x, x') : x \in G, x' \in G'\}$$

为所有有序元素对 (x, x') 的集合。对于 $(x, x'), (y, y') \in G \times G'$，定义两者的乘积为 $(xy, x'y')$，如此 $G \times G'$ 成为一个群。

容易验证群的 3 个性质都被满足（课后练习）。我们称 $G \times G'$ 为 G 和 G' 的直积。

类似地，我们可以取有限个群的直积：如果 $G_1, \ldots, G_n$ 是群，令

$$\prod_{i=1}^{n} G_i = G_1 \times \cdots \times G_n := \{(x_1, \ldots, x_n) : x_i \in G_i,\ i = 1, \ldots n\},$$

定义逐分量乘积，则 $G_1 \times \cdots \times G_n$ 成为一个群。其单位元为 $(e_1, \ldots, e_n)$，其中 e_i 为 G_i 的单位元。

例 (7)

欧氏空间 (Euclidean space) $\mathbb{R}^n$ 就是 $\mathbb{R}$ 和它自己的 n 次直积

$$\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}.$$

此时，我们把 $\mathbb{R}$ 看作一个加法群。

- 由单个元素（哪个 ?）构成的群称为**平凡的** (trivial)。
- 一般而言，一个群可能有无限多个元素，也可能只有有限个元素。
  - 如果 G 只有有限个元素，称之为**有限群** (finite group)，其元素个数称为 G 的**阶** (order)。
  - 例 4 中群的阶为 2，而例 5 中群的阶为 4。

- 例 1 至例 5 包含的群刚好都满足交换律。
- 后面我们会碰到非交换 (noncommutative) 群，例如置换群 (groups of permutations)、矩阵群等。

令 G 为一个群，$x_1, \ldots, x_n$ 为其元素。那么我们可以通过（数学）归纳法定义他们的乘积：

$$x_1 \cdots x_n = (x_1 \cdots x_{n-1})x_n.$$

利用群的性质 1（结合律），我们可以证明：无论如何插入括号，只要不改变因子顺序，那么乘积的结果都不会改变。例如对于 $n = 4$，有

$$(x_1x_2)(x_3x_4) = x_1(x_2(x_3x_4)),$$
$$(x_1x_2)(x_3x_4) = ((x_1x_2)x_3)x_4.$$

一般情形的证明需要用到归纳法，此处从略。（作为练习？）

- 上述乘积写作 $\prod_{i=1}^{n} x_i$.

- 如果 G 为加法群，我们把 n 项之和写作

$$\sum_{i=1}^{n} x_i = (x_1 + \cdots + x_{n-1}) + x_n = x_1 + \cdots + x_n.$$

如果 G 是一个交换加法群，那么可以用归纳法证明（过程从略）：上述求和的结果和 $x_1, \ldots, x_n$ 的出现顺序无关。

例如 $n = 4$，

$$\begin{aligned}(x_1 + x_2) + (x_3 + x_4) &= x_1 + (x_2 + x_3 + x_4) \\ &= x_1 + (x_3 + x_2 + x_4) \\ &= x_3 + (x_1 + x_2 + x_4)\end{aligned}$$

令 G 为一个群，H 为 G 的子集。如果

1. H 包含单位元，
2. 且对于任何 $x, y \in H$，我们有 $xy \in H$ 和 $x^{-1} \in H$（群运算的封闭性）。

则称 H 为 G 的**子群**。

- 对于加法群，我们把规则 2 写作 $x + y \in H$ 和 $-x \in H$。

如此，H 本身就是一个群：其上的运算和 G 中相同。

- G 的单位元 $\{e\}$（单元素集，singleton）构成一个子群，称为**平凡子群** (trivial subgroup)。
- G 本身也是它自己的一个子群。

（类比向量空间和子空间，vector/linear space and subspace）

例 (8)

- 有理数加法群 $\mathbb{Q}$ 是实数加法群 $\mathbb{R}$ 的子群。
- 由绝对值为 1 的复数构成的乘法群 $\mathbb{T}$ 是非零复数群 $\mathbb{C}^*$ 的子群。
- 乘法群 $\{1,-1\}$ 是 $\{1,-1,i,-i\}$ 的子群。

我们有一个一般的方法构造群 G 的子群。

- 令 S 为 G 的一个非空子集（不一定构成子群）。
- 令 H 为如下 G 的子集

$$\{x_1 \cdots x_n \text{（乘积）} : \text{对所有} i,\ x_i \in S \text{ 或 } x_i^{-1} \in S\},$$

  则 H 必然包含单位元 $e \in G$。（为什么？）
- 且容易验证：H 是 G 的子群，称为由 S **生成**的子群 (the subgroup generated by S)。

- 我们也说：S 的元素是 H 的生成元 (generators)。
- 如果 S 是 H 的生成元组成的集合，则我们使用记号

$$H = \langle S \rangle.$$

- 因此，如果集合 $\{x_1, \ldots, x_r\}$ 中的元素是群 G 的生成元，我们写作

$$G = \langle x_1, \ldots, x_r \rangle.$$

例 (9)

数字 1 整数加法群 $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ 的生成元，因为每个整数都能写成

$$1 + 1 + \cdots + 1,$$

或

$$-1 - 1 - \cdots - 1,$$

或 0。

注意到在加法记号下，S 是群 G 生成元集合的条件为：每一个群 G 的（非 0）元素都能写作

$$x_1 + \cdots + x_n,$$

其中 $x_i \in S$ 或 $-x_i \in S$。

例 (10)

令 G 为一个群，$x \in G$。如果 n 为一个正整数，我们定义 x^n 为

$$\underbrace{xx\cdots x}_{n\text{个}x}.$$

如果 $n = 0$，定义 $x^0 = e$。如果 $n = -m$，其中整数 $m > 0$，定义

$$x^{-m} = (x^{-1})^m.$$

那么通过常规推理，我们可以验证规则

$$\boxed{x^{m+n} = x^m x^n}$$

对于所有整数 m, n 都成立。验证过程比较冗长乏味，例如：

- 假定 m, n 都是正整数，那么

$$x^m x^n = \underbrace{x \cdots x}_{m\text{个}x} \underbrace{x \cdots x}_{n\text{个}x} = \underbrace{x \cdots x}_{m+n\text{个}x} = x^{m+n}.$$

- 仍然假定 m, n 都是正整数且 $m < n$，那么（作为练习题）

$$x^{-m} x^n = \underbrace{x^{-1} \cdots x^{-1}}_{m\text{个}x^{-1}} \underbrace{x \cdots x}_{n\text{个}x} = x^{n-m},$$

- 其他情形的证明类似。我们也可以通过归纳法进行证明（从略）。

类似地，我们也有另一条关于指数的规则，即

$$\boxed{(x^m)^n = x^{mn}.}$$

证明同样乏味，但它适用于（抽象）群中的乘法，就像它适用于数字乘法：我们只需要用到群运算及其结合律和乘逆。

- 例如，如果 m, n 为正整数，那么

$$(x^m)^n = \underbrace{x^m \cdots x^m}_{n\text{个}x^m} = x^{mn}.$$

- 如果 m 或 n 为负，那么我们必须通过定义来证明该规则仍然成立（作为练习）。

对于加法群，我们把 x^n 写作 $nx := x + \cdots x$，此时两条规则写作：

$$\boxed{(m+n)x = mx + nx \quad \text{和} \quad (mn)x = m(nx).}$$

我们观察到如下规则也成立

$$\boxed{(x^n)^{-1} = (x^{-1})^n.}$$

验证：

- 假定 n 为正整数，那么

$$\underbrace{x \cdots x}_{n\text{个}x}\underbrace{x^{-1} \cdots x^{-1}}_{n\text{个}x^{-1}} = e,$$

  其中我们重复使用了定义 $xx^{-1} = e$。
- 如果 n 为负，那么我们能够使用定义 $x^{-m} = (x^{-1})^m$ 给出证明，其中 $m > 0$。

令 G 为一个群且 $a \in G$。定义 H 为 G 的如下子集，

$$\{a^n : n \in \mathbb{Z}\}$$

那么 H 是由 a 生成的（G 的）子群。事实上，

- H 包含单位元 $e = a^0$。
- 令 $a^n, a^m \in H$，则有

$$a^m a^n = a^{m+n} \in H.$$

- 最后，$(a^n)^{-1} = a^{-n} \in H$.
- 所以 H 满足成为子群的条件，且 H 由 a 生成。

令 G 为群。如果存在元素 $a \in G$ 使得任意 G 的元素 x 都能写作 a^n，其中 n 为整数，那么称 G 为**循环的** (cyclic)。

- 上例中的子群 H 就是由 a 生成的循环子群。

例 (11)

考虑整数加法群 $\mathbb{Z}$。那么

- $\mathbb{Z}$ 是由 1 生成的循环群。
- $\mathbb{Z}$ 的子群在之前叫做**理想** (ideal, Lang Ch. I)。
- Ch. I 的定理 3.1 可以被转述如下：

定理

令 H 为 $\mathbb{Z}$ 的一个子群。如果 H 不是平凡子群，令 d 为 H 中最小的正整数。那么 H 由所有形如 nd 的元素组成，其中 $n \in \mathbb{Z}$。所以 $H = \langle d \rangle$ 是循环的。

下面我们进一步考察循环群。

令 G 为一个循环群，a 为其一个生成元（不一定唯一）。两种情况可能发生：

1. 不存在正整数 m 使得 $a^m = e$。
   - 那么对于每个整数 $n \neq 0$，我们有 $a^n \neq e$。（为什么？）
   - 此时，我们称 G 为**无限循环的** (infinite cyclic)，或称 a 有**无穷阶** (infinite order)。
   - 事实上，集合
   $$\{a^n : n \in \mathbb{Z}\}$$
   中元素都不相同（两两不同）。
   证明：假定对于 $r, s \in \mathbb{Z}$ 有 $a^r = a^s$，那么...
   - 例如，数字 2 生成了复数乘法群 C^* 的一个无限循环子群，其元素为
   $$\ldots, 2^{-5}, 2^{-4}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 2^4, 2^5, \ldots.$$

2 存在一个正整数 m 使得 $a^m = e$。

- 此时，我们说 a 具有**有限阶** (finite order)，并称 m 为 a 的一个**指数** (exponent)。
- 令 J 为如下集合

$$\{n \in \mathbb{Z} : a^n = e\},$$

则 J 为 $\mathbb{Z}$ 的子群。

证明 (常规)：(i) $0 \in J$；(ii) 如果 $m, n \in J$，则 $m + n \in J$；(iii) 如果 $m \in J$，则 $-m \in J$。

- 根据 Ch. I 定理 3.1，J 中最小的正整数 d 是它的一个生成元。
- 根据 J 的定义，该数字 d 是满足 $a^d = e$ 的最小正整数，称之为 a 的**周期** (period)。
- 如果 $a^n = e$，即 $n \in J$，那么 $n = ds$，其中 s 为某个整数。

假定 a 是一个具有周期 d 的元素。令 n 为一个整数，则根据欧几里得算法，我们可以写下

$$n = qd + r, \quad \text{其中 } q, r \in \mathbb{Z} \text{ 且 } 0 \leq r < d.$$

所以

$$a^n = a^r.$$

定理

令 G 为一个群且 $a \in G$。假定 a 具有有限阶，令 d 为 a 的周期。那么 a 生成一个 d 阶循环子群，其元素为 $e, a, \ldots, a^{d-1}$。

证明.

定理前的论述表明该循环子群由乘方 $e, a, \ldots, a^{d-1}$ 构成，我们还需证明这些元素各不相同。

- 假定 $a^r = a^s$，其中 $0 \leq r \leq d-1$, $0 \leq s \leq d-1$。

证明（续）.

- 不妨设 $r \leq s$，那么 $a^{s-r} = e$。
- 由于 $0 \leq s - r \leq d - 1$，所以必须有 $s - r = 0$，即 $s = r$。
- 因此循环群 $\langle a \rangle$ 的阶数为 d。

□

例 (12)

乘法群 $\{1, -1\}$ 是 2 阶循环的。

例 (13)

复数 $\{1, i, -1, -i\}$ 构成一个 4 阶循环群，其中数字 i 是一个生成元。(数字 $-i$ 也是一个生成元吗 ?)

Lang, Sec. II. 2 映射 (mappings)

令 S, S' 为集合。**一个从 S 到 S' 的映射** (mapping or map) 是一种关联，它把 S 中的每个元素都关联到 S' 中一个元素，写作 $f : S \to S'$。(函数概念的推广)

若 $f : S \to S'$ 是一个映射，$x \in S$，那么我们用 $f(x)$ 表示 S' 中通过 f 关联到 x 的元素。

- 我们称 $f(x)$ 为 f 在 x 处的**值** (value)，或 x 在 f 下的**像** (image)。
- 集合 $\{f(x) : x \in S\}$ 称为 f 的**像** (也称**值域**，range)。
- 若 T 是 S 的子集，则称集合 $\{f(x) : x \in T\}$ 是 T 在 f 下的像，用 $f(T)$ 表示。

若 f 为如上定义的映射，则我们用符号 $x \mapsto f(x)$ 表示 x 在 f 下的像。

- 注意我们区分两种箭头：$\to$ 和 $\mapsto$。

例 (1)

令 $S = S' = \mathbb{R}$，$f : \mathbb{R} \to \mathbb{R}$ 为映射（函数）$f(x) = x^2$。

- 我们也可以重新表述为：f 是映射 $x \mapsto x^2$。
- f 的像是全体非负实数。

令 $f : S \to S'$ 为一个映射，T 是 S 的一个子集。那么我们可以通过相同的规则 $x \mapsto f(x)$，$x \in T$ 定义一个映射 $T \to S'$。

- 换而言之，我们把 f 看做只定义在 T 上。
- 该映射称为 f 在 T 上的**限制** (restriction)，记作 $f|_T : T \to S'$。

令 S, S' 为集合，$f : S \to S'$ 为一个映射。如果对任意 $x, y \in S$ 且 $x \neq y$ 都有 $f(x) \neq f(y)$，则称 f 为**单射的** (injective)。

- 该条件也可以写作：若 $f(x) = f(y)$ 则 $x = y$。

例 (2, trivial)

例 1 中的映射 $f(x) = x^2$ 不是单射。
令 $g : \mathbb{R} \to \mathbb{R}$ 为映射 $x \mapsto x + 1$，则 g 为单射。

令 S, S' 为集合，$f : S \to S'$ 为一个映射。如果 S 的像 $f(S)$ 等于整个 S'，那么称 f 为**满射的** (surjective)。

- 也就是说，对于任意元素 $x' \in S'$，存在一个元素 $x \in S$ 使得 $f(x) = x'$。
- 我们也说 f 把 S **映上** (onto)S'。

例 (3, trivial)

令 $f : \mathbb{R} \to \mathbb{R}$ 为映射 $f(x) = x^2$，则它不是满射，因为 f 的像不包含负数。
令 $g : \mathbb{R} \to \mathbb{R}$ 为映射 $x \mapsto x + 1$，则 g 为满射。

Remark

令 $\mathbb{R}'$ 为非负实数的集合。我们可以把关联 $x \mapsto x^2$ 看作 $\mathbb{R}$ 到 $\mathbb{R}'$ 映射，如此该映射成为一个满射。

- 因此，我们通常约定：**不把**它看成用相同公式定义的映射 $f : \mathbb{R} \to \mathbb{R}$，后者不是满射。

令 S, S' 为集合，$f : S \to S'$ 为一个映射。如果 f 既是单射又是满射，则称 f 为**双射的** (bijective)。

- 这表明：对于每个 $x' \in S'$，存在唯一的 $x \in S$ 使得 $f(x) = x'$。
- 其中 f 为满射保证了存在性，f 为单射保证了唯一性。

例 (4)

令 $J_n = \{1, 2, \ldots, n\}$。一个 J_n 上的双射 $\sigma : J_n \to J_n$ 叫做整数 1 到 n 的**一个置换** (permutation)。J_n 上所有置换的集合记作 S_n。

- 因此，每个置换 $\sigma \in S_n$ 都是一个映射 $i \mapsto \sigma(i)$。

本章后续将仔细研究此类置换。

例 (5)

令 S 为一个非空集合，

$$I : S \to S$$

为映射 $I(x) = x,\ \forall x \in S$。

- 称 I 为**单位**映射 (identity mapping)，也记作 id。它显然为双射。
- 通常我们需要在记号中指出集合 S，写作 I_S 或 id_S。

令 T 为 S 的一个子集。对于任意 $t \in T$，我们把单位映射 $t \mapsto t$ 看作 $T \to S$ 的一个映射，称为**包含** (inclusion)，有时记为

$$T \hookrightarrow S.$$

令 S, T, U 为集合，

$$f : S \to T \quad \text{和} \quad g : T \to U$$

为映射。那么我们可以建立**复合映射** (composite mapping)

$$g \circ f : S \to U,$$

它对所有 $x \in S$ 的关联规则为

$$(g \circ f)(x) = g(f(x)).$$

例 (6)

令 $f : \mathbb{R} \to \mathbb{R}$ 为映射 $f(x) = x^2$，$g : \mathbb{R} \to \mathbb{R}$ 为映射 $g(x) = x + 1$，则 $g(f(x)) = x^2 + 1$。注意：此时我们也可以建立 $f(g(x)) = f(x + 1) = (x + 1)^2$，因此

$$f \circ g \neq g \circ f.$$

Proposition

映射的复合满足集合律，其含义如下：令 S, T, U, V 为集合，

$$f : S \to T, \quad g : T \to U, \quad h : U \to V$$

为映射。那么

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

证明.

证明非常简单 (SKIP in class)。取任意元素 $x \in S$，根据定义，我们有

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

另一方面，

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

根据定义，这表明 $h \circ (g \circ f) = (h \circ g) \circ f$。 □

Proposition

令 S, T, U 为集合，$f : S \to T$，$g : T \to U$ 为映射。

- 如果 f 和 g 均为单射，那么 $g \circ f$ 也是单射；
- 如果 f 和 g 均为满射，那么 $g \circ f$ 也是满射；
- 如果 f 和 g 均为双射，那么 $g \circ f$ 也是双射。

证明.

- 关于第一条陈述，假设 f, g 均为单射。
  - 令 $x, y \in S$ 且 $x \neq y$，于是有 $f(x) \neq f(y)$，因为 f 为单射。
  - 进一步有 $g(f(x)) \neq g(f(y))$，因为 g 也是单射。
  - 根据复合映射的定义，我们得出 $g \circ f$ 是单射。
- 第二条陈述留作练习题。
- 第三条陈述是前两条和双射定义的推论。

令 $f : S \to S'$ 为一个映射。如果存在一个映射

$$g : S' \to S$$

满足

$$g \circ f = \mathrm{id}_S \quad \text{且} \quad f \circ g = \mathrm{id}_{S'},$$

则称 g 为 f 的**一个逆映射** (inverse mapping)。

证明（练习题）：若 f 的逆映射存在，则它是唯一的。也就是说，如果 g_1, g_2 都是 f 的逆映射，那么 $g_1 = g_2$。

因此，我们用 f^{-1} 来表示逆映射 g。根据定义，刻画逆映射 f^{-1} 的性质是：对于所有 $x \in S$ 和 $x' \in S'$，我们有

$$f^{-1}(f(x)) = x \quad \text{和} \quad f(f^{-1}(x')) = x'.$$

Proposition

令 $f : S \to S'$ 为一个映射，则 f 为双射的充要条件为 f 有一个逆映射。

证明.

(必要性) 假定 f 为双射，则我们可以定义一个映射 $g : S' \to S$，其关联规则为：对于 $x' \in S'$，

$$g(x') = S\text{中的唯一元素 } x \text{ 使得 } f(x) = x'.$$

容易验证：g 满足成为 f 逆映射的条件。

充分性的证明留作练习题，即证明：如果 f 有一个逆映射，那么 f 是一个双射。

□

例 (7)

如果 $f : \mathbb{R} \to \mathbb{R}$ 为如下映射

$$f(x) = x + 1,$$

则 $f^{-1} : \mathbb{R} \to \mathbb{R}$ 为映射 $f^{-1} = x - 1$。

例 (8)

用 $\mathbb{R}_+ := \{x \in \mathbb{R} : x > 0\}$ 表示正实数的集合。令 $h : \mathbb{R}_+ \to \mathbb{R}_+$ 为映射 $h(x) = x^2$，则 h 为双射，其逆映射为平方根映射，即

$$h^{-1}(x) = \sqrt{x}, \quad x \in \mathbb{R}_+.$$

Important: 令 S 为一个集合。从 S 到它自己的一个双射 $f : S \to S$ 叫做 S 的一个**置换** (permutation)。由 S 的置换构成的集合写作

$$\mathrm{Perm}(S).$$

Proposition

置换的集合 $\mathrm{Perm}(S)$ 是一个群，其中群运算为映射的复合。

证明.

- 我们已经知道：映射的复合满足结合律。
- $\mathrm{Perm}(S)$ 中包含一个单位元——单位映射 I_S。
- 如果 f, g 是 S 的置换，那么 $f \circ g$ 和 $g \circ f$ 都是双射，故它们都是 S 的置换。
- 最后，置换 f 有一个逆 f^{-1}。

因此，群的所有公理都被满足，证明完毕。 □

如果 σ, τ 都是集合 S 的置换，那么我们通常把

$$\sigma \circ \tau \quad \text{写成} \quad \sigma\tau,$$

也就是说，我们在复合置换的时候省略 $\circ$，由此和抽象的群运算相适应。

Remark

当 f 不是双射时，我们也使用记号 f^{-1}。令 X, Y 为集合，

$$f : X \to Y$$

为一个映射。令 Z 为 Y 的一个子集。我们定义 Z 在映射 f 下的**原像** (preimage, or inverse image)

$$f^{-1}(Z) = \{x \in X : f(x) \in Z\} \subset X.$$

因此，一般而言 f^{-1}不是一个从 Y 到 X 的映射，而是从 Y 子集的集合（幂集，power set）到 X 子集的集合的映射。

Remark (续)

子集 Z 经常只包含一个元素 $y \in Y$。此时，我们把 $f^{-1}(y)$ 定义为所有满足 $f(x) = y$ 的元素 $x \in X$ 的集合。

- 如果 y 不在 f 的像中，那么 $f^{-1}(y)$ 为空集。
- 如果 y 在 f 的像中，那么 $f^{-1}(y)$ 中可能包含多个元素。

例 (10)

令 $f : \mathbb{R} \to \mathbb{R}$ 为映射 $f(x) = x^2$，那么

$$f^{-1}(1) = \{1, -1\},$$

$f^{-1}(-2)$ 为空集。

例 (11)

假定 $f : X \to Y$ 为包含映射，故 X 是 Y 的子集。那么对于 $Z \subset Y$，$f^{-1}(Z)$ 为如下交集：

$$f^{-1}(Z) = Z \cap X.$$

练习题：证明上述结论。

坐标映射

令 Y_i $(i = 1, \ldots, n)$ 为集合。一个从 X 到 Y_i 的笛卡尔积的映射

$$f : X \to \prod Y_i = Y_1 \times \cdots \times Y_n$$

由 n 个映射 $f_i : X \to Y_i$ 构成，其中

$$\text{对于任意 } x \in X, \quad f(x) = (f_1(x), \ldots, f_n(x)).$$

这些映射 f_i 叫做 f 的**坐标映射**。

Lang, Sec. II. 3 同态 (homomorphisms)

令 G, G' 为群。一个从 G 到 G' 的同态

$$f : G \to G'$$

是一个具有如下性质的映射：对于所有的 $x, y \in G$，我们有

$$f(xy) = f(x)f(y).$$

在加法标记下，$f(x+y) = f(x) + f(y)$。

例 (1)

令 G 为一个交换群，那么从 G 到它自己的映射 $x \mapsto x^{-1}$ 是一个同态。

- 在加法记号下，此映射为 $x \mapsto -x$。
- 验证上述结论（容易）。

例 (2)

映射

$$z \mapsto |z|$$

是从非零复数乘法群 $\mathbb{C}^*$ 到它自己的一个同态。

- 实际上，该映射的到达域 (codomain) 是正实数的乘法群 $\mathbb{R}_+$。

例 (3)

映射

$$x \mapsto e^x$$

是从实数加法群 $\mathbb{R}$ 到正实数乘法群 $\mathbb{R}_+$ 的一个同态。

它的逆映射——对数函数也是一个同态。

Proposition

令 G, H 为群，并假定 H 为一个直积

$$H = H_1 \times \cdots \times H_n.$$

令 $f : G \to H$ 为一个映射，f_i 为其第 i 个坐标映射。那么 f 为同态当且仅当每个 f_i 都是同态。

证明.

较易，留作练习题。 □

为了表达的简洁，我们有时候说

- “令 $f : G \to G'$ 为一个群同态 (group-homomorphism)”，

而不再说

- “令 G, G' 为群，f 为从 G 到 G' 的一个同态。”

Proposition

令 $f : G \to G'$ 为一个群同态，e, e' 分别为 G, G' 的单位元。那么 $f(e) = e'$。

证明.

根据同态定义，我们有 $f(e) = f(ee) = f(e)f(e)$。等式两边同时乘以 $f(e)^{-1}$ 即给出所需结果。 □

Proposition

令 $f : G \to G'$ 为一个群同态，$x \in G$。那么

$$f(x^{-1}) = f(x)^{-1}.$$

证明.

我们有

$$e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1}).$$

□

Proposition

令 $f : G \to G'$ 和 $g : G' \to G''$ 为群同态。那么复合映射 $g \circ f$ 是一个从 G 到 G'' 的群同态。

证明.

我们有

$$(g \circ f)(xy) = g\left(f(xy)\right) = g\left(f(x)f(y)\right) = g\left(f(x)\right)g\left(f(y)\right).$$

□

Proposition

令 $f : G \to G'$ 为一个群同态。那么 f 的像是 G' 的一个子群。

证明.

任取 $x, y \in G$，令 $x' = f(x)$，$y' = f(y)$，那么

$$x'y' = f(x)f(y) = f(xy)$$

也在 f 的像内。同时，$e' = f(e)$ 和 $x'^{-1} = f(x^{-1})$ 也在像内。因此 f 的像是一个子群。

□

定义

令 $f : G \to G'$ 为一个群同态。定义 f 的**核** (kernel) 为如下集合

$$\{x \in G : f(x) = e'\} = f^{-1}(e').$$

Proposition

一个同态 $f : G \to G'$ 的核是 G 的一个子群。

证明.

较常规，留作练习题。(核包含了单位元 e，因为 $f(e)$ 是 G' 的单位元，等等。) □

例

令 G 为一个群且 $a \in G$。映射

$$n \mapsto a^n$$

是 $\mathbb{Z}$ 到 G 的一个同态。

- 这只是 §1 中指数运算规则的重述。
- 这个同态的核由所有满足 $a^n = e'$ 的整数 n 组成。
  - 如我们在 §1 中所见，这个核要么只包含 0，
  - 要么是由 a 的周期生成的子群。

Proposition

令 $f : G \to G'$ 为一个群同态。如果 f 的核只包含 e，那么 f 为单射。

证明.

令 $x, y \in G$，假定 $f(x) = f(y)$。那么

$$e' = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}).$$

因此 $xy^{-1} = e$，故 $x = y$。这表明 f 为单射。 □

一个单射的同态叫做**嵌入** (embedding)，有时用特殊的箭头表示为

$$G \hookrightarrow G'.$$

一般而言，令 $f : X \to Y$ 为集合之间的映射，Z 为 Y 的子集。在 §2 中我们定义了**原像**：

$$f^{-1}(Z) = \{x \in X : f(x) \in Z\}.$$

Proposition

令 $f : G \to G'$ 为一个群同态，H' 为 G' 的一个子群。令 $H = f^{-1}(H')$ 为 H' 在 f 下的原像。那么 H 是 G 的一个子群。

证明.

本节习题 8。 □

在上面命题中，我们取 $H' = \{e'\}$，即 G' 的平凡子群。那么根据定义，此时 $f^{-1}(H')$ 是 f 的核。

令 $f : G \to G'$ 为一个群同态。如果存在一个同态 $g : G' \to G$ 使得 $f \circ g$ 和 $g \circ f$ 分别是 G' 和 G 上的单位映射，那么我们称 f 是一个**同构** (isomorphism，准确而言，是一个群同构，group-isomorphism)。

我们用如下记号表示同构

$$G \approx G'.$$

Remark

粗略地说，如果群 G 有一个能完全由群运算来定义的性质，那么每一个和 G 同构的群都有这样的性质，例如

- 具有阶数 (order，即元素个数) n，
- 是阿贝尔 (abelian) 群，
- 是循环 (cyclic) 群。
  - 还有一些我们在后面会遇到的性质，如是可解的 (solvable)，是单 (simple) 群，有一个平凡中心 (center)，等等。
  - 当你遇到这些性质的时候，验证它们在同构下不变 (invariant under isomorphisms)。

例 (5)

函数 $\exp$ 是实数加法群 $\mathbb{R}$ 和正实数乘法群 $\mathbb{R}_+$ 之间的一个同构。它的逆为 $\log$。

例 (6)

令 G 为一个交换群，则映射

$$f : x \mapsto x^{-1}$$

是 G 到上 (onto) 它自己的一个同构。$f \circ f$ 是什么？f^{-1} 是什么？

Proposition

一个同时为单射和满射的群同态 $f : G \to G'$ 是一个同构。

证明.

令 $f^{-1} : G' \to G$ 为逆映射。根据同构的定义，我们只需证明 f^{-1} 是一个群同态。

- 任取 $x', y' \in G'$，令 $x, y \in G$ 满足 $f(x) = x'$ 和 $f(y) = y'$，那么 $f(xy) = x'y'$ (Why?)。
- 因此，根据逆映射，我们有

$$f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y').$$

由此说明 f^{-1} 为同态。 □

从上一个命题中同构的条件，我们得到如下使得一个同态成为同构的标准判据：

定理 (3.1)

令 $f : G \to G'$ 为一个群同态。

1. 如果 f 的核是平凡的，那么 f 是 G 和它的像 $f(G)$ 之间的一个同构。
2. 如果 $f : G \to G'$ 是满射的且 f 的核是平凡的，那么 f 是一个同构。

证明.

- 我们在前面已经证明：如果 f 的核是平凡的，那么 f 为单射。
- 由于 f 总是满射到它的像上，利用上一个命题的条件即可得到定理的结论。

□

一个群和它自己的同构称为该群的**自同构** (automorphism)。

- 例 6 中的映射就是交换群 G 的一个自同构。在加法记号下应该如何表示它？
- 自同构的例子会在练习题中给出（本节习题 3、4、5)。

我们用 $\mathrm{Aut}(G)$ 表示 G 的所有自同构组成的集合。

Proposition

$\mathrm{Aut}(G)$ 是 G 的置换群 $\mathrm{Perm}(G)$ 的一个子群，其中群运算为映射的复合。

证明.

作为本节习题 3，仔细验证此结论。 □

下面，我们将看到：每个群都和某个集合的置换群（的一个子群）同构，也就是说，研究置换群和研究所有群相比，并不失一般性。

例 (7，平移，translation)

令 G 为一个群。任取 $a \in G$，令

$$T_a : G \to G$$

为映射 $T_a(x) = ax$。我们把 T_a 叫做**向左平移** a (left translation by a)。

我们声称 T_a 是 G 到它自己的一个双射，也就是 G 的一个置换。

- 如果 $x \neq y$，那么 $ax \neq ay$（两边同时左乘 a^{-1}），故 T_a 为单射。
- 它也是满射，因为任取 $x \in G$，我们有

$$x = T_a(a^{-1}x).$$

显然，T_a 的逆映射为 $T_{a^{-1}}$。

因此映射

$$a \mapsto T_a$$

从群 G 出发，到达集合 G 的置换群 $\mathrm{Perm}(G)$。

- 我们声称这是一个同态。事实上，对于 $a, b, x \in G$ 我们有

$$T_{ab}(x) = abx = T_a\left(T_b(x)\right),$$

因此 $T_{ab} = T_a T_b$。（注意，对于置换的复合，我们省略 $\circ$。）

- 进一步，我们马上注意到该同态为单射 (Why?)，因此映射

$$a \mapsto T_a \quad (a \in G)$$

是 G 和G 的置换群的一个子群（即该映射的像，理解这句话!）之间的同构。

当然，不是每个置换都由平移来给出，换而言之，该映射的像不一定等于 G 的整个置换群。

上例中的结论可以表述为：

定理 (Cayley, 1878)

每一个群 G 都可以被**嵌入** $\mathrm{Perm}(G)$，从而把 G 看成 $\mathrm{Perm}(G)$ 的一个子群。特别地，如果 $|G| = n$，那么 G 可以被嵌入 S_n。

术语“平移”取自欧氏几何。

- 令 $G = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$，把它看作一个平面。

取 $\boldsymbol{a} \in \mathbb{R}^2$，那么平移（映射）

$$T_{\boldsymbol{a}} : \mathbb{R}^2 \to \mathbb{R}^2$$
$$\boldsymbol{x} \mapsto \boldsymbol{x} + \boldsymbol{a}$$

就是通常意义下 $\boldsymbol{x}$ 沿着 $\boldsymbol{a}$ 方向做的平移。

例 (8，共轭，conjugation)

令 G 为一个群，$a \in G$。令

$$c_a : G \to G$$

为映射 $x \mapsto axa^{-1}$，称为关于 a 的**共轭**。

在本节习题 4、5，你将证明如下**命题**：

共轭 c_a 是 G 的一个自同构，称为**内自同构** (inner automorphism)。映射 $a \mapsto c_a$ 是 G 到 $\mathrm{Aut}(G)$ 的一个同态，后者的群运算为映射的复合。

令 A 为一个阿贝尔群并采用加法记号，B, C 为其子群。令 $B + C$ 为集合

$$\{b + c : b \in B,\ c \in C\}.$$

可以证明（作为练习题）：$B + C$ 也是一个子群，叫做 B, C 之**和** (sum)。

我们也可以类似地定义有限个子群之**和**：$B_1 + \cdots + B_r$。

如果 A 中每个元素 x 都可以**唯一地**写成 $x = b + c$ 的形式，其中 $b \in B$，$c \in C$，那么我们称 A 是 B, C 的**直和** (direct sum)，记作

$$A = B \oplus C.$$

类似地，我们可以定义有限个子群的**直和**：如果 A 的每个元素 x 都能唯一地写成如下形式

$$x = \sum_{i=1}^{r} = b_1 + \cdots + b_r,$$

其中元素 b_i 属于子群 B_i，那么我们写作

$$A = \bigoplus B_i = B_1 \oplus \cdots \oplus B_r$$

定理

一个阿贝尔群 A 是子群 B, C 直和的充要条件是 $A = B + C$ 且 $B \cap C = \{0\}$。后者成立当且仅当映射

$$\begin{aligned} B \times C &\to A \\ (b, c) &\mapsto b + c \end{aligned}$$

是一个同构。

证明.

本节习题 14。 □

例 (9，同态群，the group of homomorphisms)

令 A, B 为阿贝尔群并采用加法记号。我们用 $\mathrm{Hom}(A, B)$ 表示 A 到 B 同态的集合。

我们可以通过如下方式把 $\mathrm{Hom}(A, B)$ 变成一个群：如果 f, g 是 A 到 B 的同态，那么对于每个 $x \in A$，定义（群运算）$f + g : A \to B$ 为映射

$$(f + g)(x) = f(x) + g(x).$$

容易验证群的三条公理都被满足。事实上（阅读本例题以下内容），

- 如果 $f, g, h \in \mathrm{Hom}(A, B)$，那么对每个 $x \in A$，有

$$((f + g) + h)(x) = (f + g)(x) + h(x) = f(x) + g(x) + h(x),$$

以及

$$(f + (g + h))(x) = f(x) + (g + h)(x) = f(x) + g(x) + h(x).$$

因此 $f + (g + h) = (f + g) + h$。

- $\mathrm{Hom}(A, B)$ 中有一个加性单位元，即映射 0——它把 A 的每个元素映射到 B 的零元。
- 进一步，定义映射 $-f$ 为 $(-f)(x) := -f(x)$，它具有性质

$$f + (-f) = 0.$$

- 最后，我们当然需要证明 $f + g$ 和 $-f$ 都是同态。实际上，对于任意 $x, y \in A$,

$$\begin{aligned}(f+g)(x+y) &= f(x+y) + g(x+y) = f(x) + f(y) + g(x) + g(y) \\ &= f(x) + g(x) + f(y) + g(y) \\ &= (f+g)(x) + (f+g)(y),\end{aligned}$$

故 $f + g$ 是一个同态。此外，

$$(-f)(x+y) = -f(x+y) = -\left(f(x) + f(y)\right) = -f(x) - f(y),$$

因此 $-f$ 也是一个同态（注意交换律的使用!）。

由此，我们证明了 $\mathrm{Hom}(A, B)$ 是一个群。

Lang, Sec. II.4 陪集和正规子群 (cosets and normal subgroups)

我们首先引入一些简便记号。令 S, S' 为群 G 的子集，定义两个子集的**乘积** (product) 为

$$SS' = \{xx' : x \in S,\ x' \in S'\}.$$

容易验证：如果 S_1, S_2, S_3 是 G 的三个子集，那么

$$(S_1S_2)S_3 = S_1(S_2S_3).$$

上述乘积包含所有形如 xyz 的元素，其中 $x \in S_1$，$y \in S_2$，$z \in S_3$。因此子集的乘积满足结合律。

例 (1)

证明：

- 如果 H 是 G 的一个子群，那么 $HH = H$。
- 同时，如果 S 是 H 的一个非空子集，那么 $SH = H$。
- 子集乘积的其他性质，例如

$$S_1(S_2 \cup S_3) = S_1S_2 \cup S_1S_3$$

等。

令 G 为一个群，H 为一个子群。令 $a \in G$，以下集合

$$\{ax : x \in H\}$$

叫做 H 在 G 中的**陪集** (coset)，按照上面的记号写作 aH（严格来说应是 $\{a\}H$。若采用加法记号，则写作 $a + H$。）

由于群 G 可能不具有交换律，因此事实上我们应该称 aH 为 H 的一个**左陪集** (left coset)。

- 类似地，我们可以定义**右陪集**。
- 但在后续课程中，除非额外说明，否则陪集专指左陪集。

定理 (4.1)

令 aH 和 bH 为 H 在群 G 中的陪集。那么这两个陪集要么相等，要么没有公共元素（即不相交）。

证明.

假定 aH 和 bH 有一个公共元素，我们将证明两个陪集相等。

- 令 x, y 为 H 中的元素使得 $ax = by$。
- 根据例 1，我们有 $xH = H = yH$，因此

$$aH = axH = byH = bH,$$

即为所需结论。 □

假定 G 是一个有限群。每个元素 $x \in G$ 都位于 H 的某个陪集中，即 $x \in xH$。

- 因此 G 是 H 的所有陪集 (有限个！) 的并。
- 根据上述定理，我们可以把 G 写作不同（两两不相交）陪集的并，故

$$G = \bigcup_{i=1}^{r} a_i H,$$

其中陪集 $a_1 H, \ldots, a_r H$ 均不同。

我们称 $G = \bigcup a_i H$ 是 G 的**一个陪集分解** (coset decomposition)，任意元素 ah (其中 $h \in H$) 是 aH 的**一个陪集代表** (coset representative)。

- 在上述陪集分解中，陪集代表 $a_1, \ldots, a_r$ 代表了不同的陪集，它们当然也是两两不同的元素。

如果 a 和 b 是同一陪集的陪集代表，那么（需要证明）

$$aH = bH.$$

事实上，我们可以写下 $b = ah$，其中 $h \in H$。于是（根据例 1）

$$bH = ahH = a(hH) = aH.$$

如果 G 是一个无限群，我们仍然可以把它写作不同陪集的并，但是可能会有无穷多个陪集。此时我们用记号

$$G = \bigcup_{i=I} a_i H,$$

其中 I 为某个指标集，可能包含无穷多个元素。

定理 (4.2)

令 G 为一个群，H 是一个有限子群。那么一个陪集 aH 中的元素个数等于 H 中的元素个数。

证明.

令 x, x' 为 H 中的不同元素，那么 ax 和 ax' 也是不同的元素。

- 否则，如果 $ax = ax'$，那么两边左乘 a^{-1} 得到 $x = x'$。

因此，如果 $x_1, \ldots, x_n$ 是 H 的不同元素，那么 $ax_1, \ldots, ax_n$ 也是 aH 的不同元素。由此定理得证。 □

令 G 为一个群，H 为其子群。H 的所有左陪集构成的集合表示为

$$G/H.$$

（本课程不会涉及右陪集构成的集合，其记号为 $H\backslash G$。）

H 在 G 中不同陪集的个数叫做 H 在 G 中的**指数** (index)。

- 该指数当然可能是无穷大。
- 如果 G 是一个有限群，那么任何子群的指数必为有限值。
- 子群 H 的指数表示为 $(G : H)$，有的作者也用 $[G : H]$ 或 $|G : H|$。

我们用 $\#S$ 表示集合 S 中元素的个数。

- 使用该记号，我们经常写 $\#(G/H) = (G : H)$，以及

$$\#G = (G : 1), \quad \text{其中 } 1 = \{e\}.$$

也就是说，G 的阶等于平凡子群在 G 中的指数。

定理 (Lagrange)

令 G 为一个有限群，H 为其子群。那么：

1. $$\#G = (G : H)\#H.$$
2. 一个子群的阶整除 G 的阶。
3. 令 $a \in G$，则 a 的周期整除 G 的阶。
4. 如果 $G \supset H \supset K$，其中后两者均为子群，那么
$$(G : K) = (G : H)(H : K).$$

证明.

- G 的每个元素都位于某个陪集中。
  - 也就是说，a 位于陪集 aH 中，因为 $a = ae$。
- 根据定理 4.1，每个元素准确位于一个陪集中；
- 由定理 4.2，任意两个陪集的元素个数相同（都等于 $\#H$）。

由此可证明第一点中的公式。 □

证明（续）.

该公式也说明 $\#H$ 整除 $\#G$（第二点）。

元素 a 的周期等于 a 生成的（循环）子群的阶（见 §1 中最后一个定理），因此第三点得证。

最后一个公式：由第一点我们有

$$\#G = (G : H)\#H = (G : H)(H : K)\#K$$

和

$$\#G = (G : K)\#K.$$

结合上两式即证明了第四点。 □

该定理受到 Lagrange 工作 (1770) 的启发，但首先证明它的人很可能是 Galois.

例 (2)

令 S_n 为集合 $\{1, \ldots, n\}$ 的置换群，其中 $n > 1$，$H \subset S_n$ 包含所有使得 $\sigma(n) = n$ 的置换 σ，即所有固定元素 n 的置换。

- 显然 H 是一个子群，
- 并且我们可以把它看做置换群 S_{n-1}。(解释!)

我们想描述 H 的所有陪集。

- 对每一个满足 $1 \leq i \leq n$ 整数 i，定义置换 τ_i 使得 $\tau_i(n) = i$，$\tau_i(i) = n$，且 τ_i 固定其他非 n 或 i 的整数。($\tau_n = ?$)
- 我们声称陪集

$$\tau_1 H, \ldots, \tau_n H$$

两两不同，它们构成了 H 在 S_n 中的所有不同陪集。

为了证明上述论断，令 $\sigma \in S_n$，再假定 $\sigma(n) = i$。那么

$$\tau_i^{-1}\sigma(n) = \tau_i^{-1}(i) = n.$$

因此 $\tau_i^{-1}\sigma \in H$，由此可知 $\sigma \in \tau_i H$。

- 也就是说，我们证明了 S_n 中每个元素都位于某个陪集 $\tau_i H$ 中，故 $\tau_1 H, \ldots, \tau_n H$ 必然包含所有陪集。
- 但我们仍需证明这些陪集各不相同。

如果 $i \neq j$，那么对于任意 $\sigma \in H$，我们有

$$\tau_i\sigma(n) = \tau_i(n) = i \quad \text{和} \quad \tau_j\sigma(n) = \tau_j(n) = j$$

换而言之，$\tau_i H$ 和 $\tau_j H$ 中的置换把 n 映射到不同的元素，因此两个陪集不能有共同元素。定理得证。

根据 Lagrange 定理，我们有

$$\#S_n = n \cdot \#S_{n-1}.$$

通过归纳法，我们马上得到

$$\#S_n = n! = n(n-1)\cdots 1.$$

定理

令 $f : G \to G'$ 为一个群同态，H 为其核。再令 $a' \in G'$ 位于 f 的像中，即存在某个 $a \in G$ 使得 $a' = f(a)$。那么

$$f^{-1}(a') = \{x \in G : f(x) = a'\}$$

正好就是陪集 aH。

证明.

令 $x \in aH$，则有 $x = ah$，其中 $h \in H$。那么

$$f(x) = f(a)f(h) = f(a).$$

反之，假定 $x \in G$ 且 $f(x) = a'$。那么

$$f(a^{-1}x) = f(a)^{-1}f(x) = a'^{-1}a' = e'.$$

因此 $a^{-1}x$ 位于核 H 中，可写作 $a^{-1}x = h$，其中 $h \in H$。由此可知 $x = ah$，即 $x \in aH$。定理得证。 □

令 G 为一个群，H 为它的一个子群。如果 H 满足如下两个等价条件之一，则称 H 是**正规的** (normal)：

1. 对于所有 $x \in G$，我们有 $xH = Hx$（即左陪集等于右陪集），也就是 $xHx^{-1} = H$。
2. 存在某个从 G 到另一个群的同态，H 是它的核。

现在证明这两个条件的等价性。

- （条件 2 $\Longrightarrow$ 条件 1）假定 H 是某个同态 f 的核。那么

$$f(xHx^{-1}) = f(x)f(H)f(x)^{-1} = e'.$$

  因此对于任意 $x \in G$，有 $xHx^{-1} \subset H$。同理（Why?），我们也有 $x^{-1}Hx \subset H$，由此得到 $H \subset xHx^{-1}$。最终 $xHx^{-1} = H$。
- 条件 1 $\Longrightarrow$ 条件 2 的证明见定理 4.5 和推论 4.6.

警告：当 G 不是交换群时，正规子群的条件 1 不等同于 “$xhx^{-1} = h$ 对于所有元素 $h \in H$ 成立”。

- 但是，我们注意到：一个交换群的子群总是正规的，并且满足比前面正规子群的条件 1 更强的条件，即 $xhx^{-1} = h$ 对于所有 $h \in H$ 成立。(trivial)

下面我们证明正规子群的条件 1 $\Longrightarrow$ 条件 2，即构造一个同态使得满足条件 1 的子群为其核。

定理 (4.5)

令 G 为一个群，H 为其子群且具有性质：$xH = Hx$ 对于所有 $x \in G$ 成立。那么：

- 如果 aH 和 bH 为 H 的陪集，那么乘积 $(aH)(bH)$ 也是一个陪集。
- 所有陪集的集合是一个群，群运算为如上定义的乘积。

证明.

我们有 $(aH)(bH) = aHbH = abHH = abH$，因此两个陪集的乘积仍是一个陪集。

下面验证陪集的集合称为群的三个条件：

- 群运算（陪集乘积）的结合律见于本节开始关于 G 的子集乘积的论述。
- 群的单位元为陪集 $eH = H$ 自己。(Ex. 验证这一点)
- aH 的逆为 $a^{-1}H$。(Ex. 同样验证这一点)

由此定理得证。 □

定理 4.5 中陪集组成的群叫做 G 在 H 上的**因子群** (factor group，也称商群，quotient group)，或 G **模** H (G modulo H)。

- 注意：这是一个由左或右陪集构成的群，由于对 H 做的假设，左右在此没有区别。
- 强调：正是这个假设让我们能够定义陪集的乘积；否则，若条件“对所有 $x \in G$ 有 $xH = Hx$”不成立，那么我们将无法定义一个陪集的群。

推论 (4.6)

令 G 为一个群，H 为其子群且具有性质：$xH = Hx$ 对于所有 $x \in G$ 成立。令 G/H（记号）为因子群，定义映射

$$f : G \to G/H,$$

它把每个 $a \in G$ 关联到陪集 $f(a) = aH$。那么 f 是一个同态，并且其核正好为 H。

证明.

f 为同态的事实来自于陪集乘积的性质。(Ex. 验证这一点)

关于 f 的核，显然 H 中的所有元素都在核内。

- 反之，如果 $x \in G$ 且 $f(x) = xH$ 为 G/H 的单位元——陪集 H 本身，则 $xH = H$。这表明 $xe = x \in H$。

因此 H 等于 f 的核，即为定理结论。 □

推论 4.6 中的同态 f 叫做 G 到上 (onto，意为满射) 因子群 G/H 的**标准同态** (canonical homomorphism)。

令 $f : G \to G'$ 为一个群同态，H 为其核。任取 $x \in G$，那么对所有 $h \in H$，我们有

$$f(xh) = f(x)f(h) = f(x).$$

该性质可以被重写为

$$f(xH) = f(x).$$

也就是说，H 的一个陪集中的所有元素在 f 下的像相同。

- 这是一个重要的事实，我们会把它用于下一个结果——这在涉及同态的论证中起到奠基作用。
- 你们应该熟练地掌握这个结果。

推论 (4.7)

令 $f : G \to G'$ 为一个群同态，H 为其核。那么映射

$$\begin{aligned} G/H &\xrightarrow{\approx} \operatorname{Im} f \\ xH &\mapsto f(xH) \end{aligned}$$

是 G/H 和 f 的像之间的一个同构。

证明.

由上一页的论述，我们可以定义一个映射

$$\bar{f} : G/H \to G', \quad xH \mapsto f(xH),$$

其中 G/H 为 H 的陪集的集合。由定理 3.1，我们需要验证三件事：

1. $\bar{f}$ 是一个同态。事实上，

$$\bar{f}(xHyH) = \bar{f}(xyH) = f(xy) = f(x)f(y) = \bar{f}(xH)y\bar{H}.$$

证明（续）.

2. $\bar{f}$ 为单射。根据定义，$\bar{f}$ 的核包含满足 $f(xH) = e'$ 的所有陪集 xH。等式表明 $f(x) = e'$ 即 $x \in H$。因此 $\bar{f}$ 的核由 H 一个陪集（G/H 的单位元）构成（平凡核）。
3. $\bar{f}$ 的像等于 f 的像，这一点由 $\bar{f}$ 的定义直接导出。

至此推论得证。 □

- 我们说推论中的同构 $\bar{f}$ 是由 f **诱导的** (induced)。
- 注意：G/H 和 f 的像是在推论所定义的映射 $\bar{f}$ 意义下同构 (isomorphic)，而不仅是给出了同构 (isomorphism) 的存在性。
- 当我们断言两个群同构时，最好能指出同构映射（构造性证明）。

例 (3)

考虑实数加法群 $\mathbb{R}$ 的子群 $\mathbb{Z}$。因子群 $\mathbb{R}/\mathbb{Z}$ 有时叫做**圆群** (circle group)。

- 两个元素 $x, y \in \mathbb{R}$ 若满足 $x - y \in \mathbb{Z}$，则称它们**模** $\mathbb{Z}$ **同余** (congruent mod $\mathbb{Z}$)。
- 这个同余是一个等价关系，同余类 (congruence class) 正好是 $\mathbb{Z}$ 在 $\mathbb{R}$ 中的陪集。
- 如果 $x \equiv y \mod \mathbb{Z}$，那么 $e^{2\pi i x} = e^{2\pi i y}$；反之也成立。

因此映射

$$x \mapsto e^{2\pi i x}$$

定义了 $\mathbb{R}/\mathbb{Z}$ 和绝对值为 1 的复数构成的乘法群 $\mathbb{T}$ 之间的一个同构。

- 为了证明这些陈述 (Ex.)，我们当然需要知道指数函数的一些解析性质。

例 (4)

令 $\mathbb{C}^*$ 为非零复数的乘法群，$\mathbb{R}_+$ 为正实数的乘法群。给定一个复数 $\alpha \neq 0$，我们可以写下

$$\alpha = ru,$$

其中 $r \in \mathbb{R}_+$，u 的绝对值为 1。（令 $u = \alpha/|\alpha|$。）上述表达式能被唯一决定，映射

$$\alpha \mapsto \frac{\alpha}{|\alpha|}$$

是一个从 $\mathbb{C}^*$ 到 $\mathbb{T}$ 的同态。其核为 $\mathbb{R}_+$，因此 $\mathbb{C}^*/\mathbb{R}_+$ 同构于 $\mathbb{T}$。（本节习题 14）

关于上述两个例子中的陪集代表，参考本节习题 15 和 16。

习题罗列了许多关于正规子群和同态的基本事实，其证明比较简单，推荐课后自行完成。

- 特别地，你将会找到一个关于子群是否正规的有用判据：

例 (5)

令 H 为一个有限群 G 的子群。假定指数 $(G : H)$ 等于能整除 G 的阶的最小质数，那么 H 是正规的。

- 特别地，一个指数为 2 的子群是正规的 (Why?)。
- 参考本节习题 29 和 30（有一定挑战性）

下面我们描述一些同态和同构的标准情形，最简单的如下。

Proposition

令 $K \subset H \subset G$ 为群 G 的正规子群，那么映射

$$xK \mapsto xH, \quad \text{其中} \quad x \in G$$

是一个满射同态

$$G/K \to G/H.$$

我们也把它叫做**标准** *(canonical)* 同态，其核为 H/K。

证明.

作为练习题，容易验证结论。 □

注意到：根据推论 4.7，我们有公式

$$G/H \approx (G/K)/(H/K),$$

和算术的一条基本规则很像。

例

令 $G = \mathbb{Z}$ 为整数加法群。$\mathbb{Z}$ 的子群就是形如 $n\mathbb{Z}$ 的集合（见 Ch. I 定理 3.1）。

- 令 m, n 为正整数，则 $n\mathbb{Z} \subset m\mathbb{Z}$ 当且仅当 m 整除 n。（证明？）
- 因此，如果 $m|n$，我们得到一个标准同态

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}.$$

- 若我们写下 $n = md$，那么标准同态也写作

$$\mathbb{Z}/md\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}.$$

Lang, Sec. II.6 置换群

本节更深入讨论 n 元素集合 $\{1, \ldots, n\} = J_n$ 的置换群 S_n，后者也叫做**对称群** (symmetric group)。

若 $\sigma \in S_n$，那么回想起 $\sigma^{-1} : J_n \to J_n$ 也是一个置换使得

$$\sigma^{-1}(k) = \text{唯一的整数 } j \in J_n \text{ 使得 } \sigma(j) = k.$$

只交换两个数字而固定其他的置换 τ 叫做一个**对换** (transposition)，也就是说，存在整数 $i, j \in J_n$，$i \neq j$ 使得

$$\tau(i) = j,\ \tau(j) = i,\ \text{且 } \tau(k) = k \text{ 若 } k \neq i,\ k \neq j.$$

- 我们马上知道，如果 τ 是一个对换，那么 $\tau^{-1} = \tau$ 且 $\tau^2 = I$。
- 特别地，一个对换的逆仍然是对换。

我们将证明：（所有）对换能够生成 S_n。

定理

每个 J_n 的置换可以被表达为若干个对换的乘积（复合）。

证明.

我们将对 n 归纳进行证明。

- 对于 $n = 1$，没什么需要证明。
- 令 $n > 1$ 并假设上述论断已经在 $n - 1$ 情形得到了证明。
  - 令 $\sigma \in S_n$，设 $\sigma(n) = k$。
  - 再令 τ 为 J_n 的一个对换使得 $\tau(k) = n$, $\tau(n) = k$。
  - 则 $\tau\sigma$ 是一个置换，且满足

$$\tau\sigma(n) = \tau(k) = n.$$

    也就是说，$\tau\sigma$ 固定了 n。
  - 因此，我们可以把 $\tau\sigma$ 看作 J_{n-1} 的一个置换。

证明（续）.

- （续）
  - 根据归纳假设，存在 J_{n-1} 的对换 $\tau_1, \ldots, \tau_s$，它们固定 n，使得

$$\tau\sigma = \tau_1 \cdots \tau_s.$$

  - 现在我们可以写下

$$\sigma = \tau^{-1}\tau_1 \cdots \tau_s,$$

由此证明定理。

□

一个 $\{1, \ldots, n\}$ 的置换 σ 有时表示为（不是矩阵！）

$$\begin{bmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{bmatrix}.$$

例如，

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

表示置换 σ 使得 $\sigma(1) = 2,\ \sigma(2) = 1,\ \sigma(3) = 3$。事实上，这是一个对换。

令 $i_1, \ldots, i_r$ 为 J_n 中的不同整数。符号

$$[i_1 \cdots i_n]$$

表示置换 σ 使得

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots, \quad \sigma(i_r) = i_1,$$

且 σ 固定所有其他整数。

- 这样的置换叫做一个**轮换** (cycle)，更准确而言，一个 r-轮换。
- 相比较笨重的双行记号，轮换是一个更好的记号——它更有利于揭示置换的一些重要特征。

例如

$$[132]$$

表示置换 σ 使得 $\sigma(1)=3,\ \sigma(3)=2,\ \sigma(2)=1$ 且 σ 固定所有其他整数(如有)。

如果 $\sigma=[i_1\cdots i_r]$ 是一个轮换，那么容易验证 σ^{-1} 也是一个轮换，事实上 (Ex.)，

$$\sigma^{-1}=[i_r\cdots i_1].$$

因此，如果 $\sigma=[132]$，那么

$$\sigma^{-1}=[231].$$

- 注意到一个 2-轮换 $[ij]$ 就是一个对换，后者使得 $i\mapsto j$ 且 $j\mapsto i$。

QU'UNE FONCTION PEUT ACQUÉRIR, ETC. 79

Nous observerons d'abord que, si dans la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$ formée par deux permutations prises à volonté dans la suite

$$A_1, \quad A_2, \quad A_3, \quad \ldots, \quad A_N,$$

les deux termes A_s, A_t renferment des indices correspondants qui soient respectivement égaux, on pourra, sans inconvénient, supprimer les mêmes indices pour ne conserver que ceux des indices correspondants qui sont respectivement inégaux. Ainsi, par exemple, si l'on fait $n = 5$, les deux substitutions

$$\begin{pmatrix} 1.2.3.4.5 \\ 2.3.1.4.5 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1.2.3 \\ 2.3.1 \end{pmatrix}$$

seront équivalentes entre elles. Je dirai qu'une substitution aura été réduite à sa plus simple expression lorsqu'on aura supprimé, dans les deux termes, tous les indices correspondants égaux.

Soient maintenant $\alpha, \beta, \gamma, \ldots, \zeta, \eta$ plusieurs des indices $1, 2, 3, \ldots, n$ en nombre égal à p, et supposons que la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$ réduite à sa plus simple expression prenne la forme

$$\begin{pmatrix} \alpha & \beta & \gamma & \ldots & \zeta & \eta \\ \beta & \gamma & \delta & \ldots & \eta & \alpha \end{pmatrix},$$

en sorte que, pour déduire le second terme du premier, il suffise de ranger en cercle, ou plutôt en polygone régulier, les indices $\alpha, \beta, \gamma, \delta, \ldots, \zeta, \eta$ de la manière suivante :

et de remplacer ensuite chaque indice par celui qui, le premier, vient prendre sa place lorsqu'on fait tourner d'orient en occident le polygone

A. Cauchy, Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme, *J. de l'École Poly XVII Cahier*, tome X (1815), pp. 1–28.
From: *Oeuvres Completes d'Augustin Cauchy*, II Serie, Tome I, Gauthier-Villars, Paris, 1905.

轮换的乘积容易确定。例如，

$$[132][34] = [2134].$$

我们使用定义计算：若 $\sigma = [132]$，$\tau = [34]$，则（建议）计算顺序为

$$\begin{aligned}
\sigma\tau(1) &= \sigma(\tau(1)) = \sigma(1) = 3, \\
\sigma\tau(3) &= \sigma(\tau(3)) = \sigma(4) = 4, \\
\sigma\tau(4) &= \sigma(\tau(4)) = \sigma(3) = 2, \\
\sigma\tau(2) &= \sigma(\tau(2)) = \sigma(2) = 1.
\end{aligned}$$

把一个置换分解为不相交的轮换 (factorization of a permutation into disjoint cycles, cf. Rotman, Ch. 1, pp. 5–7)

例 (另一个轮换的乘积)

设 $n = 5$，计算 $\gamma = \alpha\beta$，其中 $\alpha = [1\ 2]$，$\beta = [1\ 3\ 4\ 2\ 5]$。

由于置换乘积是映射（函数）的复合，故

$$\begin{aligned}\gamma(1) = (\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(3) = 3,\\ \gamma(3) = \alpha(\beta(3)) = \alpha(4) = 4,\\ \gamma(4) = \alpha(\beta(4)) = \alpha(2) = 1.\end{aligned}$$

回到 1 之后，我们再计算 $\gamma(2)$，因为 2 是 γ 的函数值尚未被计算的最小的整数。最终我们得到

$$[1\ 2]\,[1\ 3\ 4\ 2\ 5] = [1\ 3\ 4]\,[2\ 5].$$

等式右边的两个轮换是**不相交的**，定义如下。

定义

令 $i \in J_n = 1, \ldots, n$ 且 $\alpha \in S_n$。若 $\alpha(i) = i$，则称 α **固定** (fixes) i，此时也称 i 是 α 的**不动点** (fixed point)；若 $\alpha(i) \neq i$，则称 α **移动** (moves) i。

定义

给定两个置换 $\alpha, \beta \in S_n$，如果被一个置换移动的 i 都是另一个置换的不动点，则称 α, β **为不相交的** (disjoint)。用符号表述：

$$\text{若 } \alpha(i) \neq i, \text{ 则 } \beta(i) = i;$$
$$\text{若 } \beta(j) \neq j, \text{ 则 } \alpha(j) = j.$$

当然，有可能存在 $k \in J_n$ 使得 $\alpha(k) = k = \beta(k)$。

给定一组置换 $\alpha_1, \alpha_2, \ldots, \alpha_m$，如果它们中的任意一对都是不相交的，则称这一组置换为不相交的。

我们来把 $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{bmatrix}$ 分解为不相交轮换的乘积。

- 首先 $\alpha(1) = 6$，因此 α 开头为 $[1\ 6$;
- 由于 $\alpha(6) = 3$，我们继续写下 $[1\ 6\ 3$;
- 因为 $\alpha(3) = 1$，因此方括号合上，α 的开头为 $[1\ 6\ 3]$。
- 尚未出现的最小整数为 2，故写下 $[1\ 6\ 3]\ [2$，然后是 $[1\ 6\ 3]\ [2\ 4$;
- 如此继续，我们最终得到分解（几个不相交轮换的乘积）

$$\alpha = [1\ 6\ 3]\ [2\ 4]\ [5]\ [7\ 8\ 9].$$

定理

每个置换 $\alpha \in S_n$ 要么是一个轮换，要么是几个不相交轮换的乘积。

证明.

证明对被 α 移动的点数 k 做归纳。

- 定理结论对基础步骤 $k = 0$ 成立，因为此时 α 为单位置换，是一个 1-轮换。
- 若 $k > 0$，令 i_1 为被 α 移动的一个点。
  - 定义 $i_2 = \alpha(i_1)$，$i_3 = \alpha(i_2)$，$\ldots$，$i_{r+1} = \alpha(i_r)$，其中 r 是使得 $i_{r+1} \in \{i_1, i_2, \ldots, i_r\}$ 成立的最小整数；
  - 注意：序列 $i_1, i_2, \ldots, i_k, \ldots$ 不可能无限地、不重复地继续下去，因为它们只有 n 个可能的取值。
  - 我们声称 $\alpha(i_r) = i_1$；否则，$\alpha(i_r) = i_j$ 对于某个 $2 \le j \le r$ 成立，但同时 $\alpha(i_{j-1}) = i_j$，这和 α 为单射的假设相矛盾。
  - 令 σ 为 r-轮换 $[i_1\ i_2\ \cdots\ i_r]$。若 $r = n$，则 α 就是轮换 σ。
  - 若 $r < n$，令集合 Y 由剩下的 $n - r$ 个点构成，则 $\alpha(Y) = Y$ 且 σ 固定 Y 中的点。

证明（续）.

- 对 $k > 0$ 做归纳（续）
  - 现在映射的限制 $\sigma|_{\{i_1,\ldots,i_r\}} = \alpha|_{\{i_1,\ldots,i_r\}}$。
  - 定义置换 α' 使其满足 $\alpha'|_Y = \alpha|_Y$ 且固定 $\{i_1, \ldots, i_r\}$，那么 σ 和 α' 不相交且 $\alpha = \sigma\alpha'$。
  - 由于 α' 移动的点数（它们位于 Y 中）少于 α，故归纳假设表明 α' 是不相交轮换的乘积，且结论对 α 亦成立。

在 α 的轮换分解中，我们经常省略所有的 1-轮换（如有），因为 1-轮换都是单位置换 (Why?)；另一方面，有时候展示所有的轮换会带来便利。

定义

置换 α 的一个**完整分解** (complete factorization) 是指把 α 分解为若干个不相交轮换的乘积并满足：对每个被 α 固定的 i，该分解包含一个 1-轮换 $[i]$。

于是在置换 α 的一个完整分解中，每个 $i \in J_n$ 出现在其中一个且仅一个轮换中。

定理

令 $\alpha \in S_n$ 且 $\alpha = \beta_1 \cdots \beta_t$ 为一个不相交轮换的完整分解。那么此分解除了因子出现的顺序之外，是唯一的。

证明.

根据以下引理，

引理 (习题 1.8，作为作业)

若 α 和 β 是不相交的置换，则 $\alpha\beta = \beta\alpha$，即 α 和 β **可交换** *(commute)*。

不相交的轮换可交换，因此一个完整分解中因子的顺序不是唯一确定的；但是，我们将看到所有因子的集合（无序对象）是唯一确定的。

由于每个被 α 固定的 i 恰好对应一个 1-轮换，因此我们只需证明长度至少为 2 的轮换组成的集合是唯一的。

□

证明（续）.

设 $\alpha = \gamma_1 \cdots \gamma_s$ 是另一个由不相交轮换组成的完整分解。

- 如果 β_t 移动 i_1，则根据如下引理，

引理 (习题 1.14(i)，作为作业)

令 S_n 中的 $\alpha = \beta\gamma$，其中 β 和 γ 不相交。如果 β 移动 i，则 $\alpha^k(i) = \beta^k(i)$ 对所有（整数）$k \geq 0$ 成立。*(Hint:* $\alpha^k = \beta^k\gamma^k$*.)*

我们有 $\beta_t^k(i_1) = \alpha^k(i_1)$ 对所有 $k \geq 0$ 成立。

- 现在某个 γ_j 必须移动 i_1；由于不相交的轮换可交换，故我们不妨设 $\gamma_j = \gamma_s$。
- 做和上面类似的推理，我们知道 $\gamma_s^k(i_1) = \alpha^k(i_1)$ 对所有 $k \geq 0$ 成立，从而有

$$\gamma_s^k(i_1) = \beta_t^k(i_1), \quad \forall k \geq 0.$$

□

证明（续）.

- 根据下述引理，

引理 (习题 1.14(ii)，作为作业)

令 α 和 β 为 S_n 中的轮换（我们不假设它们具有相同的长度）。如果存在 i_1 使得它同时被 α 和 β 移动，且对所有正整数 k 满足 $\alpha^k(i_1) = \beta^k(i_1)$，那么有 $\alpha = \beta$。

我们有 $\beta_t = \gamma_s$。

- 由消去律，

引理 (习题 1.6，作为作业)

置换的乘积（复合）满足**消去律** *(cancellation law)*：若 $\alpha\beta = \alpha\gamma$ 或 $\beta\alpha = \gamma\alpha$ 成立，则有 $\beta = \gamma$。

我们得到 $\beta_1 \cdots \beta_{t-1} = \gamma_1 \cdots \gamma_{s-1}$。

- 最后通过对 $\max\{s, t\}$ 做归纳 (How?)，证明得以完成。

置换的正负号 (sign) 或奇偶性 (parity)

作为课后阅读，参考 Lang, Sec. II.6, pp. 62–65 或 Rotman, Ch. 1, pp. 7–9.

Lang, Sec. II.8 群对集合的作用 (operation of a group on a set)

在某种意义上，本节是对 §6 的延续。我们将定义一个一般的概念，它把置换群囊括为一个特殊情形，并早在 §3 和 §4 的习题中已经出现。

令 G 为一个群，S 为一个集合。G 在 S 上的一个**作用** (an operation or an action) 指的是一个从 G 到 S 的置换群的同态

$$\pi : G \to \mathrm{Perm}(S).$$

- 我们把和 $x \in G$ 相关联的置换表示为 π_x，因此该同态也写做

$$x \mapsto \pi_x.$$

- 给定 $s \in S$，它在置换 π_x 下的像是 $\pi_x(s)$.

从这样一个群作用中，我们得到一个映射

$$G \times S \to S,$$

它把每一对 (x, s)，其中 $x \in G$，$s \in S$，映射到 S 中的元素 $\pi_x(s)$。

有时我们把 $\pi_x(s)$ 简写为 xs。在此简化记号下，群作用满足两个性质：

1. 对于所有的 $x, y \in G$ 和 $s \in S$，我们有结合律

$$x(ys) = (xy)s.$$

2. 如果 e 是 G 的单位元，那么对于所有 $s \in S$ 有 $es = s$。

注意到性质 1 中的公式就是性质

$$\pi_{xy} = \pi_x \pi_y$$

的简化记号。（即映射 $\pi : G \to \mathrm{Perm}(S)$ 是一个同态！）

类似地，性质 2 的简化记号表明 π_e 是单位置换，即

$$\forall s \in S, \quad \pi_e(s) = s.$$

反之，如果我们有一个映射

$$G \times S \to S \quad \text{表示为} \quad (x, s) \mapsto xs,$$

满足上属性质 1、2，那么对于每个 $x \in G$，映射 $s \mapsto xs$ 是一个 S 的置换，可以写作 $\pi_x(s)$。如此，$x \mapsto \pi_x$ 是一个从 G 到 $\mathrm{Perm}(S)$ 的同态。(证明见 Rotman, Theorem 3.18, p. 55, or Ex.)

所以群 G 在集合 S 上的一个作用可以被等价地定义为一个满足性质 1 和 2 的映射 $G \times S \to S$，因此我们经常使用简化记号 xs 表示群作用而不写成 $\pi_x(s)$。

此时我们也称 S 是一个**G-集合** (G-set, Rotman 书中用语)。

下面给出群作用的一些例子。

例 (1. 平移 (translations))

我们已经在 §3 的例 7 中见过平移：对每个 $x \in G$，定义

$$T_x : G \to G \quad \text{为} \quad T_x(y) = xy.$$

由此我们得到一个从 G 到 $\mathrm{Perm}(G)$ 的同态 $x \mapsto T_x$。当然 T_x 不是一个群同态（思考!），它只是一个 G 的置换。

类似地，G 也能通过平移作用于 (operates by translation on) 其子集构成的集合（幂集）：如果 $A \subset G$，那么 $T_x(A) = xA$ 也是一个子集。

- 如果 H 是 G 的一个子群，那么 $T_x(H) = xH$ 是 H 的一个陪集。

例 (2. 共轭 (conjugation))

对于每个 $x \in G$，令 $\boldsymbol{c}(x) : G \to G$ 为映射 $\boldsymbol{c}(x)(y) = xyx^{-1}$（含参映射）。那么我们已经在 §3 例 8 中见过：映射

$$x \mapsto \boldsymbol{c}(x)$$

是一个从 G 到 $\mathrm{Aut}(G) \subset \mathrm{Perm}(G)$ 的同态。所以此映射给出了 G（以共轭的方式）对它自己的作用。

- 该同态的核为
$$\{x \in G : xyx^{-1} = y \ \forall y \in G\},$$
称为 G 的**中心** (center)。

注意到：G 也可以通过共轭作用于 (operates by conjugation on)G 的所有子群构成的集合——因为一个子群的共轭仍是子群 (Why?)。

- 我们不用简化记号表示共轭，因为把共轭写作 xH 会引起歧义。
- 保留记号 xH 用来表示 H 沿着 x “方向” 做平移；同时把 H 关于 x 做共轭写为 $\boldsymbol{c}(x)(H)$。

例 (3. 线性代数中的例子)

令 $\mathbb{R}^n$ 为 n 维列向量构成的向量空间，G 为 $n \times n$ 可逆矩阵组成的集合。则 G 是一个群，群运算为矩阵乘法，且 G 作用于 $\mathbb{R}^n$。

- 具体地，对于 $A \in G$ 和 $\boldsymbol{x} \in \mathbb{R}^n$，我们有线性映射 $L_A : \mathbb{R}^n \to \mathbb{R}^n$ 使得

$$L_A(\boldsymbol{x}) = A\boldsymbol{x}.$$

  映射 $A \mapsto L_A$ 是从 G 到 $G' \subset \mathrm{Perm}(\mathbb{R}^n)$ 的一个同态，其中 G' 为从 $\mathbb{R}^n$ 到他自己的可逆线性映射构成的（乘法）群。
- 由于我们经常把 $L_A(\boldsymbol{x})$ 写成 $A\boldsymbol{x}$，简化记号

$$(A, \boldsymbol{x}) \mapsto A\boldsymbol{x}$$

  在这个例子中特别有用——从中我们直接看到性质 1、2 被满足。

其他例子见 Lang, Ch. VI, §3。

假定我们有一个 G 在 S 上的作用。令 $s \in S$（固定），我们定义 s 的**稳定子** (stablizer，也叫各向同性群，isotropy group) 为集合

$$G_s := \{x \in G : \pi_x(s) = s\}.$$

Ex. 验证 G_s 确实是 G 的一个子群，也称为“稳定子群”。

例

令 G 为一个群，H 为其子群。令 G 通过平移作用于 H 的陪集构成的集合 S，那么 $H \in S$ 的稳定子群为 H 自己，因为：若 $x \in G$，那么 $xH = H$ 当且仅当 $x \in H$。

接下来，假定 G 通过共轭作用于它自己，那么元素 $a \in G$ 的稳定子群叫做 a 的**中心化子** (centralizer)。此时，中心化子包含所有和 a 可交换的 $x \in G$，即

$$xax^{-1} = a \quad \text{或} \quad xa = ax.$$

例 (续)

如果我们把 G 看成通过共轭作用在所有子群的集合上，那么一个子群 H 的稳定子群叫做 H 的**正规化子** (normalizer)。

问：一个正规子群 H 的正规化子是？

令 G 作用于集合 S。我们使用性质 1、2 的简化记号。令 $s \in S$（固定），S 的子集

$$\{xs : x \in G\}$$

叫做 s 在 G 下的**轨道** (the orbit of s under G，Rotman 称为 G-orbit)，记为 Gs（类似群的子集的乘积，见 §4 开头）。

- 我们再把这个轨道记为 O。令 $t \in O$，则有

$$O = Gs = Gt.$$

- 容易证明上式：因为 $t \in O = Gs$ 表明存在 $x \in G$ 使得 $xs = t$，然后（Ex. 验证）

$$Gt = Gxs = Gs, \quad \text{原因是} \quad Gx = G.$$

（任何）一个元素 $t \in O$ 叫做该轨道的**一个代表** (representative)，我们称 t **代表** (represents) 该轨道。注意到，

- 轨道的概念类似陪集的概念，同时轨道代表的概念类似陪集代表的概念。
- 比较轨道的定义和 §4 中陪集的定义。

例

令 G 通过共轭作用于它自己。那么一个元素 x 的轨道叫做一个**共轭类** (conjugacy class)，即

$$\{yxy^{-1} : y \in G\}.$$

我们称该集合中的元素和 x 共轭。

一般而言，令 G 作用于一个集合 S。令 $s \in S$（固定）。如果 x, y 位于稳定子群 G_s 的同一个陪集中，那么 $xs = ys$。

- 事实上，我们可以写下 $y = xh$，其中 $h \in G_s$，所以

$$ys = xhs = xs, \quad \text{原因是根据稳定子群的定义有} \quad hs = s.$$

因此，我们可以定义一个映射

$$\bar{f} : G/G_s \to S, \quad \bar{f}(xG_s) = xs,$$

其像不依赖于陪集代表的选取。我们称 $\bar{f}$ 是 $f : G \to S,\ x \mapsto xs$ 的**导出** (induced) **映射**。

Proposition (8.1)

令 G 作用于集合 S，（任意地）固定一个元素 $s \in S$。

1. 映射 $x \mapsto xs$ 导出了 G/G_s 和轨道 Gs 之间的一个双射，即上述 $\bar{f}$。
2. 轨道 Gs 的阶（元素个数）等于指数 $(G : G_s)$。

证明.

- 容易说明：$\bar{f}$ 的像正是 s 的轨道。
- $\bar{f}$ 是单射的，因为如果两个陪集 xG_s 和 yG_s 在 f 下的像相同 (其中 $x, y \in G$)，即 $xs = ys$，那么 $x^{-1}ys = s$，故 $x^{-1}y \in G_s$，由此得 $y \in xG_s$，因此 x, y 位于 G_s 的同一个陪集中，即 $xG_s = yG_s$。

特别地，

- 当 G 通过共轭作用于子群的集合且 H 是一个子群时，
- 或者当 G 通过共轭作用于它自己时，

我们从命题 8.1 和定义得到：

Proposition (8.2)

(a) 和 H 共轭的子群个数等于 H 的正规化子的指数。

(b) 令 $x \in G$，x 的共轭类中包含的元素个数等于中心化子的指数 $(G : G_x)$。

下面一个结果给出了一个非常好的子群正规性判据（之前的一个习题）。

Proposition (8.3)

令 G 为群，H 为一个指数为 2 的子群。那么 H 是正规的。

证明.

令 S 为 H 陪集的集合，且 G 通过平移作用于 S。

- 对每个 $x \in G$，令 $T_x : S \to S$ 为平移使得 $T_x(aH) = xaH$。

那么

$$x \mapsto T_x \text{ 是 } G \to \mathrm{Perm}(S) \text{ 的一个同态.}$$

令 K 为其核（一个正规子群）。

- 若 $x \in K$，则 $T_x = \mathrm{id}_S$；特别地，$T_x(H) = H \implies xH = H$，故 $x \in H$。因此 $K \subset H$。
- 根据 Lang, p. 46, Corollary 4.7，G/K 能作为一个子群被嵌入 $\mathrm{Perm}(S)$，其中 $\mathrm{Perm}(S)$ 的阶为 2，因为 S 中只包含两个元素（根据题设 index $= 2$）。因此 $(G : K) = 1$ 或 2。

证明.

- 但是根据 Lagrange 定理 (Lang, Theorem 4.3)，我们有

$$(G : K) = (G : H)(H : K),$$

再加上题设 $(G : H) = 2$，故 $(H : K) = 1$，由此得 $H = K$。

- 这表明 H 是正规的，因为我们已知 K 是正规的。

Proposition (8.4)

令 G 作用于一个集合 S，则 G 的两个轨道要么不相交，要么相等。

证明.

设 Gt 和 Gs 为两个轨道，且有一个公共元素，则该元素能被写作

$$xs = yt \quad \text{其中 } x, y \in G.$$

因此

$$Gs = Gxs = Gyt = Gt,$$

即两个轨道相等。证明完成。 □

以上命题表明，S 是不同轨道的不相交并 (disjoint union)，写作

$$S = \bigcup_{i \in I} Gs_i \quad (\text{不相交}),$$

其中 I 为某个指标集，s_i 代表不同的轨道。

假定 S 是一个有限集，用 $\#(S)$ 或 $|S|$ 表示其中的元素个数，称为 S 的**阶** (order)。

由此我们可以把 $\#(S)$ 分解为若干个轨道之阶的和，称为**轨道分解公式** (orbit decomposition formula)；根据命题 8.1：

$$\#(S) = \sum_{i=1}^{r} (G : G_{s_i}).$$

例

令 G 通过共轭作用于它自己，那么，一个元素 $x \in G$ 位于 G 的**中心**当且仅当 x 的轨道是 x 自己，即该轨道只有一个元素（运用定义理解！）。

一般而言，x 的轨道之阶等于 x 的**中心化子**之指数（命题 8.1）。由此我们得到下一个命题（证明作为练习题）：

Proposition (8.5)

令 G 为一个有限群，G_x 为 x 的中心化子。再令 Z 为 G 的中心，$y_1, \ldots, y_m$ 代表包含多于一个元素的共轭类。那么，

$$(G:1) = (Z:1) + \sum_{i=1}^{m} (G:G_{y_i}),$$

其中 $(G:G_{y_i}) > 1$ 对 $i = 1, \ldots, m$ 都成立。

上述命题中的公式叫做（共轭）**类公式** (conjugacy class formula) 或**类方程** (class equation)。

Rotman, Ch. 3, p. 58 轨道计数

给定一个 G-集合 S，如果 S 和 G 都是有限集，那么我们称 G-集合 S **为有限的**。

定理 (Burnside's Lemma)

如果 S 是一个有限的 G-集合，N 为 S 中 G-轨道的数量，那么

$$N = \frac{1}{|G|} \sum_{x \in G} F(x),$$

其中，对于 $x \in G$，$F(x)$ 是被 x 固定的元素 $s \in S$ 个数，即

$$F(x) = \#\{s \in S : xs = s\}.$$

注：Burnside 引理又称为 "the lemma that is not Burnside's"。William Burnside 在他的书 "Theory of Groups of Finite Order" (1897) 中陈述并证明了该引理，并把它归功于 Frobenius (1887)；然而，甚至早于 Frobenius，Cauchy (1845) 也知道该公式。

为了证明上述定理，我们需要如下引理。

引理 (Rotman, Ex. 3.37, p. 57)

令 S 为一个 G-集合，$s, t \in S$。设 $t = xs$ 对于某个 $x \in G$ 成立，即 t 位于轨道 Gs 上。那么 $G_t = xG_sx^{-1}$；由此得到 $|G_t| = |G_s|$。

证明.

常规，作为习题。 □

证明（Burnside 引理）.

定理公式中的求和项

$$\sum_{x \in G} F(x) = \sum_{s \in S} |G_s|,$$

换而言之，每个 $s \in S$ 都计数了 $|G_s|$ 次，因为稳定子群 G_s 包含了所有固定 s 的 $x \in G$。 □

证明（Burnside 引理，续）.

- 如果 s 和 t 位于同一个轨道，那么上一页的引理表明 $|G_t| = |G_s|$；
- 根据 Lang, Proposition 8.1，轨道 Gs 中元素个数为 $(G : G_s)$，故它们在求和项中一共被计数了 $(G : G_s)|G_s| = |G|$ 次，其中等式来自 Lagrange 定理。
- 每个轨道都在求和中贡献了 $|G|$，因此我们有

$$\sum_{x \in G} F(x) = N|G|.$$

下面阐述 Burnside 引理的一个推论。

定义

如果 G-集合 S 只有一个轨道，则称它为**传递的** (transitive)；换而言之，对于任意 $s, t \in S$，总存在 $x \in G$ 使得 $t = xs$，即 $S = Gs$。

推论

如果 S 是一个传递的有限 G-集合且 $|S| > 1$，那么存在 $x \in G$ 使得相应的置换 $\pi_x \in \mathrm{Perm}(S)$ 没有固定点。

证明.

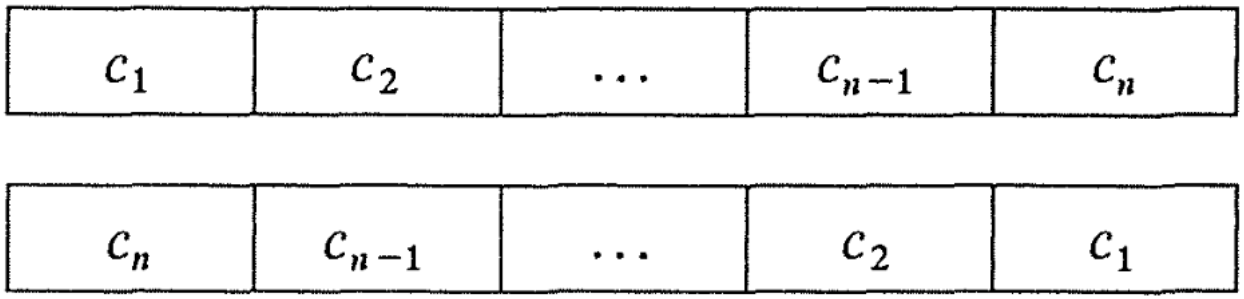
由于 S 是传递的，其轨道数 $N = 1$，故 Burnside 引理给出

$$1 = \frac{1}{|G|} \sum_{x \in G} F(x).$$

现在 $F(e) = |S| > 1$ (等式为何成立 ?)；如果对每个 $x \in G$ 都有 $F(x) > 0$，那么等式右端太大了 (Meaning?)。 □

Burnside 引理在求解一些组合问题时非常有用。例如：用 q 种不同的颜色给有 n 个等宽条带的旗染色，会得到多少面（不同的）条带旗？

- 显然，以下两面旗相同。



令 $\tau \in S_n$ 为置换 $\begin{bmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{bmatrix}$，$\mathscr{C}^n$ 表示所有 n 元组 $\boldsymbol{c} = (c_1, \ldots, c_n)$ 的集合，其中每个 c_i 都可以取 q 个颜色中的任一种。

那么循环群 $G = \langle \tau \rangle$（阶数？）作用于 $\mathscr{C}^n$，其中我们定义

$$\tau \boldsymbol{c} = \tau(c_1, \ldots, c_n) = (c_n, \ldots, c_1).$$

（Ex. 验证该定义足以给出一个群作用。）

由于 $\boldsymbol{c}$ 和 $\tau\boldsymbol{c}$ 给出了相同的旗，故一面旗对应一个 G-轨道，旗的总数等于轨道数 N。

- 根据 Burnside 引理，我们只需要计算 $F(e)$ 和 $F(\tau)$。
- 显然 $F(e) = |\mathscr{C}^n| = q^n$（乘法原理）。
- n 元组 $\boldsymbol{c} = (c_1, \ldots, c_n)$ 被 τ 固定的充要条件是 $\boldsymbol{c}$ 为一个“回文”(palindrome)：$c_1 = c_n$，$c_2 = c_{n-1}$，等等。
- 若 $n = 2k$，则 $\tau = (1\ n)(2\ n-1)\cdots(k\ k+1)$；（置换的轮换分解）若 $n = 2k+1$，则 $\tau = (1\ n)(2\ n-1)\cdots(k\ k+2)$。
- 由此可知 $F(\tau) = q^{\lfloor (n+1)/2 \rfloor}$，其中 $\lfloor x \rfloor$ 为地板函数，即不超过 x 的最大整数。
- 因此，不同旗的数量为

$$N = \frac{1}{2}(q^n + q^{\lfloor (n+1)/2 \rfloor}).$$

上述染色的概念可以被更加精确化。

定义

令 $G \subset S_n$ 为一个子群，其中 S_n 是 $J_n = \{1, \ldots, n\}$ 的对称群，$\mathscr{C}$ 为颜色的集合。若我们对每一个 $\tau \in G$ 定义 $\tau(c_1, \ldots, c_n) = (c_{\tau(1)}, \ldots, c_{\tau(n)})$，则 $\mathscr{C}^n$ 就成为一个 G-集合（Ex. 验证这一点！）。如果 $|\mathscr{C}| = q$，那么 $\mathscr{C}^n$ 的一个轨道叫做 J_n 的一个 (q, G)-染色。

引理 (3.24)

令 $\mathscr{C}$ 为 q 种颜色的集合，$G \subset S_n$ 为子群。若 $\tau \in G$，则 $F(\tau) = q^{t(\tau)}$，其中 $t(\tau)$ 是 τ 的完整分解中包含的轮换个数。

证明.

要求 $\tau \in G$ 的不动点个数 $F(\tau)$，我们写下方程

$$\tau(c_1, \ldots, c_n) = (c_{\tau(1)}, \ldots, c_{\tau(n)}) = (c_1, \ldots, c_n),$$

由此表明对所有 i 有 $c_{\tau(i)} = c_i$，即 $\tau(i)$ 和 i 的颜色相同。 □

证明（续）.

- 进一步，对于任意 k，$\tau^k(i)$ 和 i 的颜色相同 (Why?)；
- 也就是说，位于 J_n 的 $\langle\tau\rangle$-轨道中的所有 i 都有相同的颜色（显然 G 作用于 J_n!)。
- 这构成了 $\boldsymbol{c} = (c_1, \ldots, c_n)$ 为 τ 的不动点的充要条件。

根据 p. 58 习题 3.39，如果 τ 的完整分解为 $\tau = \beta_1 \cdots \beta_{t(\tau)}$ 且 i 出现在 β_j 中，那么 β_j 中出现的所有符号正好是包含 i 的 $\langle\tau\rangle$-轨道。

由于我们有 $t(\tau)$ 个轨道和 q 种颜色，因此共有 $q^{t(\tau)}$ 个 n 元组 $\boldsymbol{c}$ 在 τ 对 $\mathscr{C}^n$ 的作用中被固定。

定义

如果 $\tau \in S_n$ 的完整分解中有 $e_r(\tau) \geq 0$ 个 r-轮换，那么 τ 的**指数** (index) 为（多元单项式）

$$\mathrm{ind}(\tau) = x_1^{e_1(\tau)} x_2^{e_2(\tau)} \cdots x_n^{e_n(\tau)}.$$

若 $G \subset S_n$ 为一个子群，则 G 的**轮换指数** (cycle index) 为（多元）多项式

$$P_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{\tau \in G} \mathrm{ind}(\tau) \in \mathbb{Q}[x_1, \ldots, x_n].$$

例如，考虑所有可能的九条带蓝白双色旗（前面的例子）。

- 此时 $n = 9$，$q = 2$，$G = \langle \tau \rangle \subset S_9$ 为一个子群，其中 $\tau = (1\ 9)(2\ 8)(3\ 7)(4\ 6)(5)$。
- 现在，$\mathrm{ind}(e) = x_1^9$，$\mathrm{ind}(\tau) = x_1 x_2^4$，因此 $G = \langle \tau \rangle = \{e, \tau\}$ 的轮换指数为

$$P_G(x_1, \ldots, x_9) = \frac{1}{2}(x_1^9 + x_1 x_2^4).$$

推论

令 $J_n = \{1, \ldots, n\}$，$G \subset S_n$ 为子群，则 J_n 的 (q, G)-染色个数为 $P_G(q, \ldots, q)$。

证明.

对 G-集合 $\mathscr{C}^n$ 应用 Burnside 引理，我们得到 J_n 的 (q, G)-染色个数为

$$\frac{1}{|G|} \sum_{\tau \in G} F(\tau).$$

根据引理 3.24，上述数字等于

$$\frac{1}{|G|} \sum_{x \in G} q^{t(\tau)},$$

其中 $t(\tau)$ 是 τ 的完整分解中包含的轮换个数。 □

证明（续）.

另一方面，

$$\begin{aligned} P_G(x_1,\ldots,x_n) &= \frac{1}{|G|}\sum_{\tau\in G}\mathrm{ind}(\tau) \\ &= \frac{1}{|G|}\sum_{\tau\in G} x_1^{e_1(\tau)}x_2^{e_2(\tau)}\cdots x_n^{e_n(\tau)}, \end{aligned}$$

所以

$$\begin{aligned} P_G(q,\ldots,q) &= \frac{1}{|G|}\sum_{\tau\in G} q^{e_1(\tau)+e_2(\tau)+\cdots+e_n(\tau)} \\ &= \frac{1}{|G|}\sum_{\tau\in G} q^{t(\tau)}. \end{aligned}$$

进一步阅读：Pólya 在 1937 年把这个技巧又向前推进一步：Burnside 引理能让我们计算九条带蓝白双色旗的数目；一共有 272 条（Ex. 验证！）。那么这些旗中有多少条具有四条蓝色条带和五条白色条带呢？

参考 Rotman, p. 61.

The End