第二章　群

§2.1　基础知识 - 概念与例子

内容提要：半群；群；子群；对称群；几何图形的对称群；多元多项式的对称群.

本节介绍群与子群概念，一些重要例子.

半群概念

2.1.1 定义. 设 M 是一个非空集合，具备：

(G1) M 有一个运算 (常写作乘法);

(G2) 运算满足结合律;

(G3) 存在 $e \in M$ 使得 $ex = x = xe$ 对任 $x \in M$ 成立;

那么称 M 为一个 *幺半群*.

注. (1) 准确的说，幺半群是说的集合 M 及其 *运算结构*; 当说某某是幺半群时，决不是仅仅是一个集合，在没提到运算时是默认了一个运算.

(2) "常写作乘法" 不是说总写作乘法，可以有各种记法；如：也可写加法 "+".

(3) 从结合律可以推出 "广义结合律":

"*对 M 的任意序列 $x_1, x_2, \cdots, x_n$ 以任意两种方式加扩号运算得出的结果相等.*"

(4) (G3) 中的元素 e 是唯一的：若 $e' \in M$ 也满足 (G3), 则由 e' 和 e 都满足 (G3) 得出 $e' = e'e = e$. 运算写作乘法时，常记这唯一元为 1_M, 或更简单的， 1, 称为 *单位元* (运算写作加法时，常记它为 0_G, 或更简单的， 0, 称为 *零元*.)

(5) 幺半群 M 的集合基数 $|M|$ 称为 *幺半群的阶*. $|M| < \infty$ 时称 M 是有限幺办群.

(6) 如果运算还满足交换律，则称 M 是交换幺半群.

例. 非负整数的集合 $\mathbb{Z}^+$ 在加法运算下构成交换幺半群.

例. n 阶复矩阵的集合 $\mathrm{M}_n(\mathbb{C})$ 在乘法运算下构成幺半群. 当 $n > 1$ 时， $\mathrm{M}_n(\mathbb{C})$ 是非交换幺半群.

例. 设 A 是一个集合. A 的自映射 $f : A \to A$ 称为 A 的变换. A 的所有变换的集合记作 $\mathrm{Tran}(A)$. 变换的合成是集合 $\mathrm{Tran}(A)$ 上的运算 (一般把合成写作乘法). 易验证：

$\mathrm{Tran}(A)$ 在合成运算下构成么半群 (恒等变换 id_A 是单位元), 称为集合 X 的 *全变换半群*. 当 $|A|>1$ 时, $\mathrm{Tran}(A)$ 是非交换幺半群.

群的定义

2.1.2 定义. 设 G 是一个幺半群. 如果还满足:

(G4) 对任 $x\in G$ 存在 $x'\in G$ 使得 $xx'=1=x'x$;

那么称 G 为一个 *群*.

注. (1) 对任 $x\in G$, (G4) 中的 x' 是唯一的; 运算写作乘法时, 常记它为 x^{-1}, 称为 x 的 *逆元*; 运算写作加法时, 常记它为 $-x$, 称为 x 的 *负元*.

(2) 如果运算交换, 就称 G 为 *交换群*. 交换群的运算也常记为加法, 若如此, 称为加群.

例. 整数集合 $\mathbb{Z}$ 在加法运算下构成交换群.

例. 可逆 n 阶复矩阵的集合 $\mathrm{GL}_n(\mathbb{C})$ 在乘法运算下构成群. 当 $n>1$ 时, $\mathrm{GL}_n(\mathbb{C})$ 是非交换群. 当 $n=1$ 时, $\mathrm{GL}_1(\mathbb{C})=\mathbb{C}-\{0\}:=\mathbb{C}^\times$ 是交换群.

例. 设 A 是一个集合. A 的所有可逆变换的集合记作 $\mathrm{Sym}(A)$. 由于可逆映射的合成映射仍可逆, 所以合成是集合 $\mathrm{Sym}(A)$ 的运算. 而且, 对任 $\alpha\in\mathrm{Sym}(A)$ 存在 $\alpha'\in\mathrm{Sym}(A)$ 满足 $\alpha\alpha'=\mathrm{id}=\alpha'\alpha$. 所以 $\mathrm{Sym}(A)$ 是一个群. 当 $|A|>2$ 时, $\mathrm{Sym}(A)$ 是非交换群.

子群

2.1.3 定义. 设 G 是一个群. 如果 G 的子集 H 在 G 的运算之下也是一个群则称 H 是 G 的 *子群*, 记作 $H\le G$.

2.1.4 子群的判断. *设 G 是一个群, $H\subset G$.*

(1) 如果 $H\neq\emptyset$ 且对任 $x,y\in H$ 有 $xy^{-1}\in H$, 那么 $H\le G$.

(2) 如果 H 是非空有限集且对任 $x,y\in H$ 有 $xy\in H$, 那么 $H\le G$.

证. (1). 因 $H\neq\emptyset$, 取 $x\in H$; 那么 $1=xx^{-1}\in H$. 于是还有 $x^{-1}=1x^{-1}\in H$. 对任 $x,y\in H$, 因 $y^{-1}\in H$, 就有 $xy=x(y^{-1})^{-1}\in H$. 因此 G 的运算也是 H 的运算 (即 H 在 G 的运算下封闭), 而且 H 也成为群.

(2). 因 $H\neq\emptyset$, 任取定 $x\in H$,

$$H\longrightarrow H,\quad y\longmapsto xy\,,$$

是 H 的变换; 若 $xy_1=xy_2$, 则 $y_1=x^{-1}xy_1=x^{-1}xy_2=y_2$, 所以这是单变换, 因 H 是有限集, 故上述变换为满变换. 那么存在 $e\in H$ 使得 $xe=x$. 于是 $1=x^{-1}x=x^{-1}xe=e\in H$. 仍由上述满变换, 存在 $x'\in H$ 使得 $xx'=1$, 于是 $x^{-1}=x^{-1}xx'=x'\in H$. 那么对任 $y\in H$, 有 $yx^{-1}\in H$. 由 (1), H 是子群. □

例. $\mathrm{SL}_n(\mathbb{C}):=\{\,P\in\mathrm{GL}_n(\mathbb{C})\mid\det P=1\,\}$ 是 $\mathrm{GL}_n(\mathbb{C})$ 的子群.

例. $\mathbb{Z}$ 在整数加法下构成加群. 对任 $m \in \mathbb{Z}$, 子集 $m\mathbb{Z} := \{\, mk \mid k \in \mathbb{Z} \,\}$ 构成子群. 而且, 如果 H 是 $\mathbb{Z}$ 的子群, 则存在唯一非负整数 m 使得 $H = m\mathbb{Z}$.

证. (1). 利用上述判断办法 (1).

(2). 如果 $H = \{0\}$, 只有 $m = 0$ 使得 $H = m\mathbb{Z}$. 否则, 取 H 中的最小正整数 m; 那么, 对正整数 k, 有 $\overbrace{m + \cdots + m}^{k} = km \in H$; 因为 H 是子群, 从 $m \in H$ 得 $-m \in H$, 从而 $(-k)m = k(-m) = \overbrace{(-m) + \cdots + (-m)}^{k} \in H$; 总之, $m\mathbb{Z} \subset H$. 对任 $x \in H$, 做欧氏除法

$$x = qm + r\,, \qquad 0 \le r < m\,;$$

若 $r \neq 0$, 则 $r > 0$ 且 $r = x - qm \in H$, 与 m 是 H 中的最小正整数矛盾; 故只能是 $r = 0$; 所以 $x = mq \in m\mathbb{Z}$. 得 $H \subset m\mathbb{Z}$. 综上, $H = m\mathbb{Z}$. 显然, 使得 $m\mathbb{Z} = m'\mathbb{Z}$ 的正整数 m' 只有 $m' = m$. □

注. (1). $\mathbb{Z}$ 在整数乘法下不构成群, 只是构成么半群.

(2). 虽然 $\{1, -1\} \subset \mathbb{Z}$, $\{1, -1\}$ 在乘法下是群, 但不是加群 $\mathbb{Z}$ 的子群, 可说是乘法么半群 $\mathbb{Z}$ 的子群.

(3). 用 $\mathbb{Z}^+$ 记非负整数的集合, 则 $\mathbb{Z}^+$ 在 $\mathbb{Z}$ 的运算, 即加法, 下封闭, 但 $\mathbb{Z}^+$ 不是 $\mathbb{Z}$ 的子群.

以下简介几类重要的群.

对称群

集合 A 的可逆变换的集合 $\mathrm{Sym}(X) := \{\, f : A \to A \mid f \text{ 可逆} \,\}$, 在变换乘法 (即变换合成) 运算下构成群, 称为 A 的 *对称群*. $\mathrm{Sym}(A)$ 的子群称为 A 的 *变换群*.

如果 A 是有限集, 则 A 的可逆变换称为 *置换*, A 的变换群称为 *置换群*.

设 $A = \{\, 1, 2, \cdots, n \,\}$, 那么记 $S_n := \mathrm{Sym}(A)$, 称为 n *次对称群*. S_n 的元称为 n 次置换; n 次置换 α 可表示为

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}.$$

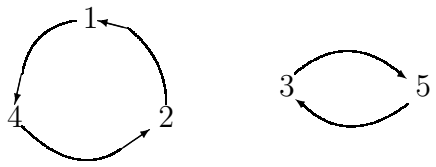
那么第二行显然是 $1, 2, \cdots, n$ 的一个 *排列*, 即一个无重复的序列. 反过来, 只要第二行是 $1, 2, \cdots, n$ 的一个排列, 就给出了一个置换. 如

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$$

是把 1 置换为 4, 把 2 置换为 1, 等等. 故马上可得:

命题. *n 次对称群的阶* $|S_n| = n!$. □

对置换作进一步讨论. 可形象地图示上面的置换 α



用 (142) 表示左边的循环置换圈, 用 (35) 表示右边的循环置换圈. 那么置换 α 可以写成 $\alpha = (142)(35)$.

说明. 如果写 $(142) \in S_n$, 就是表示这样的置换: 映射 1 为 4, 映射 4 为 2, 映射 2 为 1, 其他文字都不变. 这种置换称为循环置换, 简称 *循环*, 或 *轮换循环*. 长度 2 的轮换 (ij) 称为 *对换*. 长度 1 的轮换如 (1), (2) 等表示恒等置换. 下述结论在大学抽象代数中已熟知.

命题. *任意 n 次置换可以惟一地写成彼此无公共文字的循环之积.* □

线性群

实数域 $\mathbb{R}$ 上的向量空间 V 的可逆线性变换的集合

$$\mathrm{GL}(V) := \{\, \alpha : V \to V \mid \alpha \text{ 是可逆线性变换} \,\}$$

在变换乘法 (即变换合成) 运算下构成群, 称为 V 的 *一般线性群*. $\mathrm{GL}(V)$ 的子群称为 V 的 *线性群*.

设 $\mathbb{R}^n = \{\, x = (x_1, \cdots, x_n)^T \mid x_i \in \mathbb{R} \,\}$ 是有限维实向量空间, 则 $\mathbb{R}^n$ 的可逆线性变换可表达为 n 级可逆实矩阵 P,

$$P: \quad \mathbb{R}^n \longrightarrow \mathbb{R}^n, \quad x \longmapsto Px \ .$$

所有 n 级实可逆矩阵的集合记作 $\mathrm{GL}_n(\mathbb{R})$, 在矩阵乘法下构成的群称为实数域上的 n 级 *一般线性群*. 它的任何子群称为 n 级实 *线性群*.

记 $\mathrm{SL}_n(\mathbb{R}) = \{\, P \in \mathrm{GL}_n(\mathbb{R}) \mid \det P = 1 \,\}$, 它是 $\mathrm{GL}_n(\mathbb{R})$ 的子群, 称为实数域上的 n 级 *特殊线性群*.

记 $\mathrm{O}_n(\mathbb{R})$ 为所有 n 级实正交矩阵的集合, 它是 $\mathrm{GL}_n(\mathbb{R})$ 的子群, 称为实数域上的 n 级 *正交群*.

欧氏变换群

考虑欧氏平面 $\mathbb{R}^2 = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \;\middle|\; x_1, x_2 \in \mathbb{R} \right\}$, 内积为

$$\big\langle (x_1, x_2)^T,\ (y_1, y_2)^T \big\rangle = x_1 y_1 + x_2 y_2 \ , \qquad \forall\ (x_1, x_2)^T,\ (y_1, y_2)^T \in \mathbb{R}^2 \ .$$

取 $P \in \mathrm{O}_2(\mathbb{R})$ 是正交矩阵, 任取 $u \in \mathbb{R}^2$ 是向量; 下述变换

$$\alpha_{P,u}: \quad \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad x \longmapsto Px + u$$

称为 欧氏变换; 特别, $\alpha_{P,0}$ 称为 正交变换, $\alpha_{I,u}$ 称为 平移变换. 所有 $\mathbb{R}^2$ 的欧氏变换的集合记作 $\mathrm{E}(\mathbb{R}^2)$. 易验证欧氏变换的合成是欧氏变换:

$$\alpha_{P,u}\alpha_{Q,v}(x) = \alpha_{P,u}(Qx+v) = P(Qx+v)+u = (PQ)x+(Pv+u) = \alpha_{PQ,Pv+u}(x)\ .$$

即

$$\alpha_{P,u}\alpha_{Q,v} = \alpha_{PQ,Pv+u}\ , \qquad \forall\ P,Q\in \mathrm{O}_2(\mathbb{R})\ ,\ u,v\in\mathbb{R}^2\ ;$$

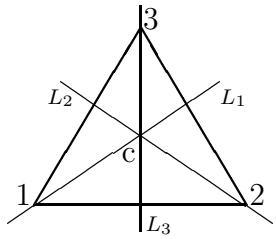
而且 $\mathrm{E}(\mathbb{R}^2)$ 构成群 (习题 4). 称这个群

$$\mathrm{E}(\mathbb{R}^2) = \{\,\alpha_{P,u} \mid P\in \mathrm{O}_2(\mathbb{R}),\ u\in\mathbb{R}^2\,\}$$

为欧氏平面 $\mathbb{R}^2$ 的 欧氏变换群.

几何图形的对称群

考虑欧氏平面上的一个正三角形. 某些欧氏变换可把它变得重合于它自己, 例如绕它的中心旋转 $2\pi/3$. 某些则不能, 例如一个非平凡的平移.



显然, 使此正三角形不变的全体变换的集合 D_3 是三个绕中心 c 的旋转 ρ_0, $\rho_{2\pi/3}$, $\rho_{4\pi/3}$, 旋转角分别是 0, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$, 和三个反射 σ_{L_1}, σ_{L_2}, σ_{L_3}, 反射轴分别是直线 L_1, L_2, L_3; 即:

$$D_3 = \{\,\rho_0,\ \rho_{2\pi/3},\ \rho_{4\pi/3},\ \sigma_{L_1},\ \sigma_{L_2},\ \sigma_{L_3}\,\}.$$

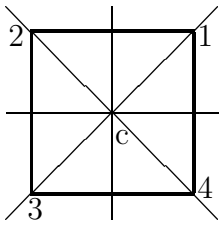
不用计算从几何直观就可看出: 只要 $\alpha,\ \beta\in D_3$ 就有 $\alpha\beta\in D_3$, 因为使此正三角形不变的变换的合成变换显然仍使此正三角形不变; 同理, 使此正三角形不变的变换的逆变换显然仍使此正三角形不变, 等等. 那么易见 D_3 是一个群.

当正三角形重合于它自己时, 它的三个顶点肯定重合于三个顶点; 用 $1,2,3$ 来把它的三个顶点分别标上号, 就可以把使得它变得重合于它自己的变换表达为 3 次置换. 以这种方式就容易看出, 可以把使此正三角形不变的全体变换写成

$$D_3 = \{\,(1),\ (123),\ (132),\ (23),\ (13),\ (12)\,\} = S_3\ ;$$

它就是三次对称群.

再考虑使欧氏平面上的正方形不变的全部欧氏变换,



使此正方形不变的全体变换集合 D_4 是四个绕中心 c 的旋转 ρ_0, $\rho_{\pi/2}$, ρ_π, $\rho_{3\pi/2}$, 和四个反射 σ_{L_1}, σ_{L_2}, σ_{L_3}, σ_{L_4}; 即

$$D_4 = \{\, \rho_0,\ \rho_{\pi/2},\ \rho_\pi,\ \rho_{3\pi/2},\ \sigma_{L_1},\ \sigma_{L_2},\ \sigma_{L_3},\ \sigma_{L_4} \,\}$$

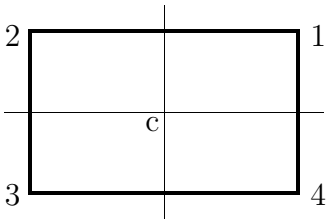
在变换合成运算下它是一个群.

用 $1, 2, 3, 4$ 标记正方形的顶点, 使正方形不变的全部欧氏变换就写为 (例如, 旋转 $\rho_{\pi/2}$ 就对应于 $\binom{1234}{2341} = (1234)$):

$$D_4 = \{\, (1),\ (1234),\ (13)(24),\ (1432),\ (12)(34),\ (14)(23),\ (13),\ (24) \,\}.$$

定义. 对欧氏平面的任何一个几何体, 使它不变的变换的集合在合成运算之下构成一个群, 称为该几何体的 *对称群*.

几何体的对称群刻划了该几何体的对称性质. 可以说这是 "群" 这个概念的直观来源. 为了说明这一点, 考虑边长不等的的长方形, 用 $1, 2, 3, 4$ 给它的顶点标号:



易见, 它的对称群是

$$K_4 = \{\, (1), \quad (13)(24), \quad (12)(34), \quad (14)(23) \,\},$$

显然 K_4 是上述 D_4 的真子集, 但它们的运算是一致的, 单位元也是一样的; 即 K_4 是 D_4 的真子群. 直观来看, 这就说明长方形确实比正方形的 "对称" 少了很多.

代数多项式的对称群

考虑变元集合 $X = \{x_1, x_2, x_3, x_4\}$ 上的任意多项式 $f(X)$, 例如

$$\begin{aligned} f_1(X) &= x_1x_2 + x_3x_4 - x_1x_4 - x_2x_3\ , \\ f_2(X) &= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1\ , \\ f_3(X) &= x_1^2 + x_2^2 + x_3^2 + x_4^2 - 3x_1x_2x_3x_4\ , \end{aligned}$$

等等. 对任 $\alpha \in S_4$, α 可作为 X 的置换：变 x_1 为 $x_{\alpha(1)}$, 变 x_2 为 $x_{\alpha(2)}$ 等等. 则 α 把多项式 $f(X)$ 变为一个多项式，记作 $\alpha f(X)$. 例如，若 $\gamma = (123)$ 而 $f_1(X)$ 如上，则 $\gamma f_1(X) = x_2x_3 + x_1x_4 - x_2x_4 - x_1x_3$. 如果 $\alpha f(X) = f(X)$, 我们就说 α 使 $f(X)$ 不变. 我们找出使 f 不变的所有置换的集合 G_f. 与上述几何例子类似，使多项式 $f(X)$ 不变的变换的合成变换显然还使多项式 $f(X)$ 不变；使多项式 $f(X)$ 不变的变换的逆变换显然还使多项式 $f(X)$ 不变，等等. 所以 G_f 是一个群而且它刻画了多项式 f 的对称性质.

定义. 使多项式 $f(X)$ 不变的 X 的置换构成的群 $G_f := \{\, \alpha \in \mathrm{Sym}(X) \mid \alpha f(X) = f(X) \,\}$ 称为多项式 $f(X)$ 的对称群.

例如，对上面的多项式 $h(X)$, $g(X)$, 很容易得出：

$$\begin{aligned} G_{f_1} &= K_4 = \{\, (1),\ (12)(34),\ (13)(24),\ (14)(23) \,\}; \\ G_{f_2} &= D_4 = \{\, (1),\ (1234),\ (13)(24),\ (1432),\ (12)(34),\ (14)(23),\ (13),\ (24) \,\}; \\ G_{f_3} &= S_4 . \end{aligned}$$

容易看出，上面的多项式 $f_3(X)$ 真正是通常所说的 “对称多项式”; 而多项式 $f_1(X)$ 的 “对称” 就比 $f_2(X)$ 少很多，比 $f_3(X)$ 的 “对称” 就差得更远.

粗想之下，代数例子应比几何例子抽象，但本质上说，它们与上述几何例子真是完全类似. 历史上群的概念实质萌芽于十九世纪初 Galois 研究代数方程的根式解，他的理论后来被称为 Galois 理论.

习题 2.1

1. 举例说明： 2.1.4 的 (2) 中有限性条件不可缺少.

2. 求正 n 边形的对称群.

3. 设 $X = \{\, x_1, x_2, x_3 \,\}$, $f(X) = x_1 - x_2 - x_3$. 求 $f(X)$ 的对称群 G_f.

4. 证明： $\mathrm{E}(\mathbb{R}^2)$ 构成群.

5. 设 $P \in \mathrm{O}_2(\mathbb{R})$. 证明： P 为下述之一：

$$P = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad \text{或} \quad \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

前者给出的正交变换 $\alpha_{P,0}$ 是绕原点角 θ 的旋转 $R(\theta)$, 后者给出的正交变换 $\alpha_{P,0}$ 是以过原点倾角 $\theta/2$ 的直线为轴的反射 $T(\theta/2)$.

6. 设 L_1, L_2 是两条过原点直线，从 L_1 到 L_2 夹角 γ, 设 σ_{L_i}, σ_{L_2} 是以直线 L_i 为轴的反射变换， $i = 1, 2$. 再设 ρ_θ 是绕原点角 θ 的旋转变换. 证明：

(1) $\sigma_{L_2}\,\sigma_{L_1} = \rho_{2\gamma}$.

(2) $\rho_\theta\,\sigma_{L_1} = \sigma_{\rho_{\theta/2}(L_1)}$; $\quad \sigma_{L_1}\,\rho_\theta = \sigma_{\rho_{-\theta/2}(L_1)}$.

7*. 欧氏平面 $\mathbb{R}^2$ 的变换 α 称为 保距变换 如果对任两点 $x, y \in \mathbb{R}^2$, 经 α 变换后 $\alpha(x)$ 到 $\alpha(y)$ 的距离与未变换的 x 到 y 的距离相等： $|\alpha(x) - \alpha(y)| = |x - y|$. 证明：保距变换是欧氏变换.

(**提示**. 直接验证欧氏变换是保距变换. 反过来，设 α 是保距变换.

第 1 步： $\beta = \alpha_{E,u}^{-1}\alpha$ 是保距变换且 $\beta(0) = 0$, 其中 $u = \alpha(0)$.

第 2 步： β 保持向量长度不变： $|\beta(x)| = |\beta(x) - 0| = |x - 0| = |x|$.

第 3 步：利用 $|\beta(x) - \beta(y)| = |x - y|$ 证明 β 保持向量内积不变： $\langle\beta(x), \beta(y)\rangle = \langle x, y\rangle$.

第 4 步：利用上一步结果证明 β 是线性变换，从而 β 是正交变换.

第 5 步： $\beta = \alpha_{P,0}$, $P \in O_2(\mathbb{R}^2)$; 从而 $\alpha = \alpha_{E,u}\beta = \alpha_{P,u}$ 是欧氏变换.)

§2.2 基础知识 - 商群与同态

内容提要: 陪集；正规子群；商群；同态基本定理；子群对应定理.

本节继续介绍大学抽象代数已学习过的陪集，正规子群，商群，同态等基础知识.

设 G 是一个群，运算写作乘法. 对任意非空子集 $S, T \subseteq G$, 定义

$$ST = \{\, st \mid s \in S,\ t \in T \,\}\ .$$

从 G 的元素运算满足结合律易验证子集的上述运算也满足结合律：

$$R(ST) = (RS)T\ , \qquad \forall\ R, S, T \subseteq G\ .$$

简记 $\{a\}S = aS$, $S\{a\} = Sa$.

设 $H \leq G$. 由于 G 不一定是交换群， “同余” 的定义不得不分为两种情况.

定义(左同余和左陪集). 对任 $a, b \in G$, 如果 $a^{-1}b \in H$ 则记 $a \equiv_L b \pmod H$, 称 a 与 b 模 H*左同余*. 易验证这是等价关系，且 a 所在等价类为 $aH = \{\, ah \mid h \in H \,\}$, 称为子群 H 的一个 *左陪集*; 商集记作 $G/H := \{\, aH \mid a \in G \,\}$.

(**验证**. $a^{-1}a = 1 \in H$ 故 $a \equiv_L a \pmod H$. 若 $a \equiv_L b \pmod H$, 即 $a^{-1}b \in H$, 故 $b^{-1}a = (a^{-1}b)^{-1} \in H$, 得 $b \equiv_L a \pmod H$. 若 $a \equiv_L b \pmod H$ 且 $b \equiv_L c \pmod H$, 即 $a^{-1}b \in H$ 且 $b^{-1}c \in H$, 故 $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, 得 $a \equiv_L c \pmod H$. 最后，等价类 $[a] = \{\, b \in G \mid b \equiv_L a \pmod H \,\} = \{\, b \in G \mid a^{-1}b \in H \,\} = \{\, b \in G \mid b \in aH) \,\} = aH$.)

定义(右同余和右陪集). 对任 $a, b \in G$, 如果 $ba^{-1} \in H$ 则记 $a \equiv_R b \pmod H$, 称 a 与 b 模 H*右同余*. 易验证这是等价关系，且 a 所在等价类为 $Ha = \{\, ha \mid h \in H \,\}$, 称为子群 H 的一个 *右陪集*; 商集记作 $H\backslash G := \{\, Ha \mid a \in G \,\}$.

Lagrange 定理.

(1) $|aH| = |H| = |Ha|$;

(2) $|H\backslash G| = |G/H| =: |G : H|$ *(称为 G 对 H 的指数 (index));*

(3) $|G| = |G:H| \cdot |H|$; 特别的，如 G 为有限群，则 $|H| \,\Big|\, |G|$.

证. (1). $H \to aH$, $h \mapsto ah$, 是双射. (其逆映射是 $aH \to H$, $x \mapsto a^{-1}x$; 或直接证明单射.)

(2). $H\backslash G \to G/H$, $Ha \mapsto (Ha)^{-1}$, 是双射.

(3). 由于 G 划分为左同余关系的等价类， aH , 的不交并. □

指数公式. 设 G 是群， $H \le K \le G$. 则 $|G:H| = G:K| \cdot |K:H|$. □

一般来说，不能得到 $aH = Ha$. 如：取 $G = S_3$, $H = \{(1), (12)\}$, $a = (13)$; 则

$$aH = \{(13), (123)\} \neq \{(13), (132)\} = Ha \ .$$

定义. 群 G 的子群 H 称为 正规子群, 记作 $H \trianglelefteq G$, 如果对任 $x \in G$ 有 $xH = Hx$.

注. 按定义， $H \trianglelefteq G$ 就是说 G 的两个等价关系 $\equiv_L \pmod H$ 和 $\equiv_R \pmod H$ 给出的等价类是一样的，也就是说 "模 H 左同余" 与 "模 H 右同余" 是同一个等价关系 (见定理 1.2.4), 我们把它记作 $\equiv \pmod H$. 以下命题给出子群正规的更多等价刻画.

命题. 设 H 是群 G 的子群. 以下三条等价：

(i) $H \trianglelefteq G$.

(ii) $x^{-1}Hx = H$, $\forall\ x \in G$.

(iii) $x^{-1}hx \in H$, $\forall\ h \in H$ $x \in G$.

证. (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii): 显然.

(iii) $\Rightarrow$ (ii): 由 (iii) 得 $x^{-1}Hx \subseteq H$, $\forall\ x \in G$; 两边左乘 x 左乘 x^{-1} 得 $H \subseteq xHx^{-1}$, $\forall\ x \in G$; 令 $y = x^{-1}$, 即 $H \subseteq y^{-1}Hy$, $\forall\ y \in G$. 所以 $x^{-1}Hx = H$, $\forall\ x \in G$. □

设 H 是群 G 的正规子群，即 "模 H 左同余" 和 "模 H 右同余" 是同一个等价关系，记作 $\equiv \pmod H$, 等价类是 $[a] = aH = Ha$; 商集记作 $G/H = \{\, aH \mid a \in G \,\}$.

如果 $a' \equiv a \pmod H$, $b' \equiv b \pmod H$, 即可写 $a' = ah$, $b' = bh'$, 其中 $h, h' \in H$. 那么 $a'b' = ahbh' = ab \cdot b^{-1}hbh'$; 而 $b^{-1}hbh' \in H$, 得 $a'b' \equiv ab \pmod H$. 所以可以利用群 G 的运算通过等价类 (即陪集) 的代表元来定义商集 G/H 的运算如下

$$(aH)(bH) = (ab)H \ , \qquad \forall\ aH,\ bH\ \in\ G/H \ .$$

而且

$$\begin{aligned} \Big((aH)(bH)\Big)(cH) &= ((ab)H)(cH) = ((ab)c)H \\ &= (a(bc))H = (aH)((bc)H = (aH)\Big((bH)(cH)\Big) \ , \end{aligned}$$

即 G/H 的运算满足结合律. 还易验证： $1H = H$ 是 G/H 的单位元， $a^{-1}H$ 是 aH 的逆元. 所以 G/H 是一个群.

定义. 设 G 是群， $H \trianglelefteq G$. 上述群 G/H 称为群 G 模正规子群 H 的 商群.

例. 考虑加群 $\mathbb{Z}$. 设 $m \in \mathbb{Z}$. 易验证 $m\mathbb{Z} \trianglelefteq \mathbb{Z}$ (实际上交换群的任何子群是正规子群), $a \equiv b \pmod{m\mathbb{Z}}$ 就是熟知的模 m 同余关系, $\mathbb{Z}/m\mathbb{Z}$ 就是熟知的模 m 剩余类加群.

例. 易验证: 特殊线性群 $\mathrm{SL}_n(\mathbb{C})$ 是一般线性群 $\mathrm{GL}_n(\mathbb{C})$ 的正规子群. 还易验证: $A \equiv B \pmod{\mathrm{SL}_n(\mathbb{C})}$ 当且仅当 $\det A = \det B$; 陪集 $A \cdot \mathrm{SL}_n(\mathbb{C}) = \{\, B \in \mathrm{GL}_n(\mathbb{C}) \mid \det B = \det A \}$. 所以 $\mathrm{GL}_n(\mathbb{C})/\mathrm{SL}_n(\mathbb{C}) = \mathbb{C}^\times$.

定义. 设 G, G' 是群. 如果映射 $\varphi : G \to G'$ 满足

$$\varphi(ab) = \varphi(a)\varphi(b)\ , \qquad \forall\ a, b \in G\ ,$$

就称 φ 是从群 G 到群 G' 的 同态. 如果同态 φ 是单射 (满射, 双射), 就称 φ 为 单同态(满同态, 同构).

命题. *设 $\varphi : G \to G'$ 是群的同态. 则:*

(1) $\mathrm{Im}(\varphi) \le G'$, *称为 φ 的 象; φ 是满同态当且仅当* $\mathrm{Im}(\varphi) = G'$.

(2) $\mathrm{Ker}(\varphi) := \{\, a \in G \mid \varphi(a) = 1 \,\} \trianglelefteq G$, *称为同态 φ 的 核; φ 是单同态当且仅当* $\mathrm{Ker}(\varphi) = 1$. □

例. $\mathbb{Z} \to \mathbb{Z}_m$, $a \mapsto [a]$, 是满同态, 同态核是 $m\mathbb{Z}$.

例. $\mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$, $a \mapsto \det a$, 是满同态, 同态核是 $\mathrm{SL}_n(\mathbb{C})$

例. 设 $H \trianglelefteq G$, 则 $\rho_H : G \to G/H$, $a \mapsto aH$, 是满同态, 称为 自然同态.

例. 设 $H \le G$, 则包含映射 $H \to G$, $h \mapsto h$, 是单同态.

例. V 是 n 维复向量空间, 取定基底后, 则把可逆线性变换 $\alpha \in \mathrm{GL}(V)$ 映射为其矩阵 $A \in \mathrm{GL}_n(\mathbb{C})$ 是从群 $\mathrm{GL}(V)$ 到群 $\mathrm{GL}_n(\mathbb{C})$ 的同构.

例. 设 $\omega \in \mathbb{C}^\times$ 是一个 m 次单位根. 则 $\mathbb{Z}_m \to \mathbb{C}^\times$, $[a] \to \omega^a$, 是同态. 什么时候这个同态是单同态?

同态基本定理. *设 $\varphi : G \to G'$ 是群同态, 记 $K = \mathrm{Ker}(\varphi)$; 则 $K \trianglelefteq G$, 记 $\rho_K : G \to G/K$ 是自然同态; 那么*

(1) *存在惟一群同态 $\bar\varphi : G/K \to G'$ 使得 $\varphi = \bar\varphi \cdot \rho_K$ (图示为下述 交换图).*

(2) *上述 $\bar\varphi$ 必为单同态; $\bar\varphi$ 为满同态当且仅当 φ 为满同态.*

$$\begin{array}{ccc} G & \xrightarrow{\ \varphi\ } & G' \\ {\scriptstyle \rho_K}\big\downarrow & \nearrow_{\bar\varphi} & \\ G/K & & \end{array}$$

证. 对 $a, b \in G$, 因为 φ 是同态, 故 $\varphi(a) = \varphi(b)$ 当且仅当 $\varphi(a)^{-1}\varphi(b) = 1$ 当且仅当 $\varphi(a^{-1}b) = 1$ 当且仅当 $a^{-1}b \in K$. 所以有结论:

(3) 由 φ 决定的 G 的等价关系 $\sim_\varphi$ *(见 §1.2 映射基本定理)* 就是模 K 同余关系 $\equiv (\mathrm{mod}\ K)$, 等价类 $[a]_{\sim_\varphi}$ 就是 K 的陪集 aK.

那么由映射基本定理, 使得 $\varphi = \bar{\varphi} \circ \rho_K$ 的映射 $\bar{\varphi}$ 存在且惟一, 它定义为 $\bar{\varphi}(aK) = \varphi(a)$ 对所有 $aK \in G/K$; 只需证明这个 $\bar{\varphi}$ 是群同态.

$$\bar{\varphi}(aK \cdot bK) = \bar{\varphi}((ab)K) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(aK) \cdot \bar{\varphi}(bK)\ . \qquad \square$$

同构定理. 设 $H \leq G$, $N \trianglelefteq G$. 那么 $H \cap N \trianglelefteq H$, 且 $H/H \cap N \cong HN/N$.

证. 考虑自然同态 $\rho : G \to G/N$, 限制到 H 得同态

$$\rho|_H : \quad H \longrightarrow G/N\ , \quad h \longmapsto hN\ ;$$

那么它的象为 $\mathrm{Im}(\rho|_H) = HN/N$, 它的核为 $\mathrm{Ker}(\rho|_H) = H \cap N$. 从同态基本定理, 得下述群同构:

$$\overline{(\rho|_H)} : \quad H/H \cap N \xrightarrow{\cong} HN/N\ , \quad h(H \cap N) \longmapsto hN\ .$$

子群对应定理. 设 $\varphi : G \to G'$ 是群的满同态, $K = \mathrm{Ker}(\varphi)$ 是同态核. 那么映射

$$\begin{array}{rccc} \varphi^* : & \{\, H \mid K \subseteq H \leq G \,\} & \longrightarrow & \{\, H' \mid H' \leq G' \,\}\ , \\ & H & \longmapsto & \varphi(H)\ , \end{array}$$

是双射. 而且

(1) 对任 $K \subseteq H_1, H_2 \leq G$ 有: $H_1 \leq H_2 \iff \varphi(H_1) \leq \varphi(H_2)$.

(2) 设 $K \subseteq H \leq G$. 则 $|G : H| = |G' : \varphi(H)|$.

(3) (第一同构定理) 设 $K \subset H \leq G$. 则 $H \trianglelefteq G \iff \varphi(H) \trianglelefteq G$; 此时

$$G/H \xrightarrow{\cong} G'/\varphi(H)\ , \quad aH \longmapsto \varphi(a)\varphi(H)\ .$$

证. 首先指出下述断言正确:

(4) 对任 $T \subseteq G$ 有 $\varphi^{-1}(\varphi(T)) = TK = KT$.

因为: 对任 $tk \in TK$ 其中 $t \in T$ 和 $k \in K$ 有 $\varphi(tk) = \varphi(t)\varphi(k) = \varphi(t) \in \varphi(T)$, 故 $\varphi(tk) \in \varphi^{-1}(\varphi(T))$, 得 $TK \subseteq \varphi^{-1}(\varphi(T))$. 反过来, 对任 $x \in \varphi^{-1}(\varphi(T))$, 有 $t \in T$ 使得 $x \in \varphi^{-1}(\varphi(t))$, 即 $\varphi(x) = \varphi(t)$; 从而 $x \in [t]_{\sim_\varphi} = tK$ (见同态基本定理证明中的结论 (3)); 故 $x \in TK$, 所以 $\varphi^{-1}(\varphi(T)) \subseteq TK$. 总之 $\varphi^{-1}(\varphi(T)) = TK$.

对 $H' \leq G'$, 易验证 $H' \leq G'$ 在 G 中的全原象 $\varphi^{-1}(H')$ 是 G 的子群, 而且因 $1_{G'} \in H'$, 故 $K = \varphi^{-1}(1_{G'}) \subseteq \varphi^{-1}(H')$. 故可以定义映射

$$\begin{array}{rccc} \psi^* : & \{\, H' \mid H' \leq G' \,\} & \longrightarrow & \{\, H \mid K \subseteq H \leq G \,\}\ , \\ & H' & \longmapsto & \varphi^{-1}(H')\ . \end{array}$$

因 φ 是满射，对任 $H' \le G'$ 有 $\varphi(\varphi^{-1}(H')) = H'$. 即 $\psi^*\varphi^* = \mathrm{id}$.

对 $H \le G$, $H \supseteq K$, 由上述结论 (4) 有 $\varphi^{-1}(\varphi(H)) = HK = H$. 也就是 $\varphi^*\psi^* = \mathrm{id}$.

所以 ψ^* 与 φ^* 是互逆的映射，从而 φ^* 是双射.

(1). 显然

(2). 对 $aH \in G/H$, $\varphi(aH) = \{\,\varphi(ah) \mid h \in H\,\} = \{\,\varphi(a)\varphi(h) \mid \varphi(h) \in \varphi(H)\,\} = \varphi(a)\varphi(H)$, 它是 G' 中关于 $\varphi(H)$ 的左陪集. 这就建立了映射：

$$\alpha: \quad G/H \longrightarrow G'/\varphi(H)\,, \qquad aH \longmapsto \varphi(aH) = \varphi(a)\varphi(H)\,.$$

对任 $a'\varphi(H) \in G'/\varphi(H)$, 因 φ 是满射，存在 $a \in G$ 使得 $\varphi(a) = a'$, 那么 $\alpha(aH) = \varphi(a)\varphi(H) = a'\varphi(H)$. 即 α 是满射.

再设 $\alpha(aH) = \alpha(bH)$, 即 $\varphi(a)\varphi(H) = \varphi(b)\varphi(H)$, 则 $\varphi(H) = \varphi(a)^{-1}\varphi(b)\varphi(H) = \varphi(a^{-1}b)\varphi(H)$, 得 $\varphi(a^{-1}b) \in \varphi(H)$, 那么 $a^{-1}b \in \varphi^{-1}(\varphi(H)) = H$, 得 $aH = bH$. 即 α 是单射. 总之 α 是双射.

(3). 设 $H \trianglelefteq G$. 对任 $a' \in G'$ 存在 $a \in G$ 使得 $\varphi(a) = a'$; 那么

$$a'^{-1}\varphi(H)a' = \varphi(a)^{-1}\varphi(H)\varphi(a) = \varphi(a^{-1})\varphi(H)\varphi(a) = \varphi(a^{-1}Ha) = \varphi(H)\,;$$

所以 $\varphi(H) \trianglelefteq G'$.

再设 $\varphi(H) \trianglelefteq G'$. 对任 $a \in G$, 因为 $K = a^{-1}Ka \subseteq a^{-1}Ha$, 所以 $K(a^{-1}Ha) = a^{-1}Ha$; 那么由上面证明的结论 (4), 有

$$\begin{aligned} a^{-1}Ha &= K(a^{-1}Ha) = \varphi^{-1}\Big(\varphi(a^{-1}Ha)\Big) = \varphi^{-1}\Big(\varphi(a^{-1})\varphi(H)\varphi(a)\Big) \\ &= \varphi^{-1}\Big(\varphi(a)^{-1}\varphi(H)\varphi(a)\Big) = \varphi^{-1}\Big(\varphi(H)\Big) = KH = H\,. \end{aligned}$$

得 $H \trianglelefteq G$.

剩下只需指出结论 (2) 的证明中的 α 是群同态. 这可直接验证：

$$\begin{aligned} \alpha\Big((aH)(bH)\Big) &= \alpha\Big((ab)H\Big) = \varphi(ab)\varphi(H) = \Big(\varphi(a)\varphi(b)\Big)\cdot\varphi(H) \\ &= \Big(\varphi(a)\varphi(H)\Big)\Big(\varphi(a)\varphi(H)\Big) = \alpha(aH)\,\alpha(bH)\,. \end{aligned}$$

即 α 是同态. □

习题 2.2

1. 设 $H, K \le G$, 则 $|HK| \cdot |H \cap K| = |H| \cdot |K|$.

2. 设 H 是群 G 的子群, $a \in G$. 则 aHa^{-1} 也是群 G 的子群.

3. 设 H, K 都是群 G 的子群. 则 HK 是子群当且仅当 $HK = KH$.

4. 设 $H \lneq G, a \in G$. 则 $H \cdot aHa^{-1} \neq G$. (**提示**: 否则, 有 $h, h' \in H$ 使得 $a^{-1} = hah'a^{-1}$, 得 $a \in H$, 矛盾.)

5. 设 $H \trianglelefteq G$, $K \leq G$. 则 $HK \leq G$.

6. 设 $H \trianglelefteq G$, $K \trianglelefteq G$. 则 $HK \trianglelefteq G$, $H \cap K \trianglelefteq G$.

7. 设 $H \leq G$ 使得 $|G : H| = 2$. 证明： $H \trianglelefteq G$.

8. 设 $\varphi : G \to H$ 是群同态, 则对任 $a \in G$ 和任整数 $n \in \mathbb{Z}$ 有： $\varphi(a^n) = \varphi(a)^n$.

9. 证明： $\varphi : \mathbb{R} \to \mathbb{C}^\times$, $r \mapsto \exp(2\pi \mathrm{i} r)$, 是群同态, 求 $\mathrm{Im}(\varphi)$ 和 $\mathrm{Ker}(\varphi)$, 并求 $\mathbb{R}/\mathrm{Ker}(\varphi)$.

10. 考虑欧氏平面 $\mathbb{R}^2$ 的欧氏变换群 $E(\mathbb{R}^2) = \{ \alpha_{P,u} \mid P \in O_2(\mathbb{R}), u \in \mathbb{R}^2 \}$. 证明：

(1) $T(\mathbb{R}^2) = \{ \alpha_{I,u} \mid u \in \mathbb{R}^2 \}$ 是 $E(\mathbb{R}^2)$ 的正规子群， $O(\mathbb{R}^2) = \{ \alpha_{P,0} \mid P \in O_2(\mathbb{R}) \}$ 是 $E(\mathbb{R}^2)$ 的子群.

(2) $E(\mathbb{R}^2)/T(\mathbb{R}^2) \cong O(\mathbb{R}^2)$.

11. 设 G 为群, 如 $\varphi : G \to G$ 是同态, 就称为 G 的 自同态. 如 $\varphi : G \to G$ 是同构, 就称为 G 的 自同构. 记 $\mathrm{End}(G) = \{G$ 的自同态$\}$, $\mathrm{Aut}(G) = \{G$ 的自同构$\}$. 则：

(1) 在变换合成运算下， $\mathrm{End}(G)$ 构成幺半群.

(2) 在变换合成运算下， $\mathrm{Aut}(G)$ 构成群.

12. 设 $a \in G$. 则 $\gamma_a : G \to G$, $x \mapsto axa^{-1}$, 是自同构, 称为由 a 决定的 G 的 内自同构. 记 $\mathrm{Inn}(G) = \{G$ 的内自同构$\}$.

(1) 证明： $\gamma : G \to \mathrm{Aut}(G)$, $a \mapsto \gamma_a$, 是群同态; 求 $\mathrm{Im}(\gamma)$ 和 $\mathrm{Ker}(\gamma)$.

(2) 证明： $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. (商群 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ 称为 G 的 外自同构群.)

13. 求 $\mathrm{Aut}(\mathbb{Z})$. (答案 $1 \mapsto \pm 1$)

14. 求 $\mathrm{Aut}(\mathbb{Q})$. (答案 $1 \mapsto q$, $q \in \mathbb{Q}$)

15. 利用子群对应定理找出 $\mathbb{Z}_m$ 的所有子群, 这里 m 是一正整数.

§2.3 循环子群，循环群

内容提要: 群的生成集; 循环子群; 元素的阶; 循环群.

群的生成集

易知：群 G 的任意一些子群的交集仍为子群; 但 G 的子群的并集不一定是子群; 见习题 1.

更一般的, 考虑群 G 的子集 $T \subset G$, 和 $\mathcal{H} = \{ H \leq G \mid H \supseteq T \}$. 则 $\bigcap\limits_{H \in \mathcal{H}} H$ 显然是 G 中包含 T 的最小子群;

2.3.1 定义. 称上述 G 中包含 T 的最小子群 $\bigcap\limits_{H \in \mathcal{H}} H$ 为由 T 生成的子群, 记作 $\langle T \rangle$.

令 $\bar{T} := T \cup T^{-1} = \{\, t^{\varepsilon} \mid t \in T,\ \varepsilon = \pm 1 \,\}$.

令 $\bar{T}^k := \{\, x_1 \cdots x_k \mid x_i \in \bar{T} \,\} = \{\, t_1^{\varepsilon_1} \cdots t_k^{\varepsilon_k} \mid t_i \in T,\ \varepsilon_i = \pm 1 \,\},\ k = 0, 1, 2, \cdots$; 其中约定 $\bar{T}^0 = \{1\}$, 即长度 0 的连乘积表示单位元 1.

因为 $\langle T \rangle \le G$, 故 $\bigcup_{k=0}^{\infty} \bar{T}^k \subseteq \langle T \rangle$. 反过来，对任 $t_1^{\varepsilon_1} \cdots t_k^{\varepsilon_k},\ {t'_1}^{\varepsilon_1} \cdots {t'_{k'}}^{\varepsilon_{k'}} \in \bigcup_{l=0}^{\infty} \bar{T}^l$,

$$(t_1^{\varepsilon_1} \cdots t_k^{\varepsilon_k})({t'_1}^{\varepsilon_1} \cdots {t'_{k'}}^{\varepsilon_{k'}})^{-1} = t_1^{\varepsilon_1} \cdots t_k^{\varepsilon_k}\, {t'_{k'}}^{-\varepsilon_{k'}} \cdots {t'_1}^{-\varepsilon_1} \ \in \ \bigcup_{l=0}^{\infty} \bar{T}^l$$

由 §2.1 的子群判断法知 $\bigcup_{k=0}^{\infty} \bar{T}^k \le G$; 而 $T \subseteq \bigcup_{k=0}^{\infty} \bar{T}^k$; 所以 $\langle\, T \,\rangle \subseteq \bigcup_{k=0}^{\infty} \bar{T}^k$. 得到

2.3.2
$$\begin{aligned} \langle\, T \,\rangle &= \textstyle\bigcup_{k=0}^{\infty} \bar{T}^k = \{\, x_1 \cdots x_k \mid x_i \in \bar{T},\, k \ge 0 \,\} \\ &= \{\, t_1^{\varepsilon_1} \cdots t_k^{\varepsilon_k} \mid t_i \in T,\ \varepsilon_i = \pm 1,\ k \ge 0 \,\}\,. \end{aligned}$$

回顾群的幂运算记号后，可以把上结论写简单一点.

设 G 是群，对 $x \in G$ 和 $n \in \mathbb{Z}$ ，定义：

$$x^n = \begin{cases} \overbrace{x \cdots x}^{n} & \text{若} n > 0\,; \\ 1 & \text{若} n = 0\,; \\ \overbrace{x^{-1} \cdots x^{-1}}^{-n} & \text{若} n < 0\,. \end{cases}$$

则指数律成立 (证明作为练习):

2.3.3
$$\begin{aligned} x^m x^n &= x^{m+n}\,, && \forall\, m,\, n \in \mathbb{Z}\,; \\ (x^m)^n &= x^{mn}\,, && \forall\, m,\, n \in \mathbb{Z}\,; \\ (xy)^n &= x^n y^n\,, && \text{如果 } x, y \in G \text{ 满足 } xy = yx. \end{aligned}$$

注. 如果群 G 是交换群，那么群 G 中的运算也可记作加法 "+", 此时单位元改称零元，并改记作 0, 此时 G 也可称作 *加群*; 那么有相应的加群表达方式：

2.3.3′
$$\begin{aligned} mx + nx &= (m+n)x\,, && \forall\, m,\, n \in \mathbb{Z}\,; \\ n(mx) &= (nm)x\,, && \forall\, m,\, n \in \mathbb{Z}\,; \\ n(x+y) &= nx + ny\,, && \forall\, x,\, y \in G\,. \end{aligned}$$

回到群 G 的子集 T 生成的子群问题，就可以把 2.3.2 改写：

2.3.2′
$$\langle\, T \,\rangle = \{\, t_1^{n_1} \cdots t_k^{n_k} \mid t_i \in T,\ n_i \in \mathbb{Z} - \{0\},\ k \ge 0,\ \text{且} t_i \ne t_{i+1} \,\}\,.$$

与 2.3.2 相比，这里

- $t_i \in T$ 而不是 $\in \bar{T}$, 因为指数 n_i 可以是负的;
- $n_i \ne 0$ 是因为：若 $t_i^0 = 1$ 则它在表达式中是多余的;
- $t_i \ne t_{i+1}$ 是因为若相等它们可以合并写成一个幂.

特别地，若 $T=\{t\}$ 由一个元构成，则记

$$\langle\, t\,\rangle := \langle\, \{t\}\,\rangle = \{\, t^n \mid n\in\mathbb{Z}\,\}\ .$$

称为 G 中由元素 t *生成的循环子群*.

2.3.4 定义. (1). 如果群 G 中存在子集 T 使得 $G=\langle\, T\,\rangle$, 则称 G 由 T 生成，称 T 是 G 的 *生成集*.

(2). 如果存在有限子集 T 使得 $G=\langle\, T\,\rangle$, 则称 G 为 *有限生成的群*.

(3). 如果存在 $a\in G$ 使得 $G=\langle\, a\,\rangle$，则称 G 为 *循环群*，称 a 为循环群 G 的 *循环生成元*.

对生成集合应该有进一步信息：一方面生成集的元素 (称生成元) 可能受某些约束；另一方面一个群的生成集不是唯一的. 这两方面展开来都是大课题，我们只作初步讨论.

本节着重讨论循环群. 从三个观察开始.

对整数及其剩余类加群的三个观察

首先, 看整数剩余类加群 $\mathbb{Z}_m=\{[0],[1],\cdots,[m-1]\}$. 取 $a=[1]$, 则 $\mathbb{Z}_m=\langle\, a\,\rangle$ 由 a 生成，而且 $ma=0$, 这是生成元 a 需要满足的关系. 注意：只要这个关系就全部确定了群 $\mathbb{Z}_m$, 因为 a 的所有倍元 $0a=0$, $1a=a$, $2a$, $\cdots$, $(m-1)a$ 就是 $\mathbb{Z}_m$ 的全部元，到下一个倍元 ma 按照关系 $ma=0$ 就又得到零元 0. 所以我们记

2.3.5
$$\mathbb{Z}_m=\langle\, a\mid ma=0\,\rangle$$

读为：“*加群 $\mathbb{Z}_m$ 由元素 a 按关系 $ma=0$ 生成.*”

更一般地，设 $k\in\mathbb{Z}$, 令 $d=\gcd(k,m)$, 那么

$$n[k]=0 \iff m|nk \iff \frac{m}{d}\,\Big|\, n$$

所以在 $\mathbb{Z}_m$ 中

$$\langle\,[k]\,\rangle=\Big\{\,0=0[k],\ [k],\ \cdots,\ \Big(\frac{m}{d}-1\Big)[k]\,\Big\}\subseteq\mathbb{Z}_m\ .$$

由此马上得

$$\mathbb{Z}_m=\langle\,[k]\,\rangle \quad\Longleftrightarrow\quad \gcd(k,m)=1\ .$$

引用下述数论语言.

定义. 在 $\mathbb{Z}_m$ 中，如果剩余类 $[k]$ 满足 $\gcd(k,m)=1$, 就称 $[k]$ 为 *既约剩余类*. $\mathbb{Z}_m$ 的既约剩余类的集合记作 $\mathbb{Z}_m^\times$. 记 $\varphi(m)=|\mathbb{Z}_m^\times|$, 称 $\varphi(m)$ 为 *欧拉 φ- 函数*.

我们有结论： *m 阶循环群 $\mathbb{Z}_m$ 的循环生成元有 $\varphi(m)$ 个.*

其次, 看整数加群 $\mathbb{Z}$. $\mathbb{Z}$ 也是循环群，因为从例 2.1.5 可以看出：

$$\mathbb{Z} = \langle 1\rangle = 1\mathbb{Z} = \langle -1\rangle = (-1)\mathbb{Z}\ ;$$

即 $\mathbb{Z}$ 是由 $a = 1$ 生成的循环群，也可以由 $b = -1$ 生成；而且 $\mathbb{Z}$ 的其他元不是循环生成元. 但是 $\mathbb{Z}$ 的情况还是有所不同：生成元 $a = 1$ 不满足任何关系，即 $na = 0$ 对任 n 都不成立！这时我们说 a 是 $\mathbb{Z}$ 的 自由生成元, 称 $\mathbb{Z}$ 是一个元 a 生成的 自由群.

第三, $\mathbb{Z}_m$ 与 $\mathbb{Z}$ 的关系. 有满同态 $\rho : \mathbb{Z} \to \mathbb{Z}_m$, $n \mapsto [n]$, 同态核 $\mathrm{Ker}(\rho)$ 是 $\mathbb{Z}$ 的子群 $m\mathbb{Z}$. 我们写作

$$0 \longrightarrow m\mathbb{Z} \longrightarrow \mathbb{Z} \xrightarrow{\ \rho\ } \mathbb{Z}_m \longrightarrow 0$$

这是一个由加群同态构成的序列其特点是：每个节点的 “入同态” 的象等于 ‘出同态” 的核. 称这样的同态序列为加群的 短正合序列.

把这些观察一般化

2.3.6 定义. 设 G 为群， $a \in G$. 如果存在正整数 k 使得 $a^k = 1$, 就称 x 是有限阶元，并称使得 $a^k = 1$ 的最小正整数 m 为元素 a 的 阶, 记作 $\mathrm{ord}(a) = m$.

如果不存在正整数 k 使得 $a^k = 1$, 就称 a 是无限阶元，记作 $\mathrm{ord}(a) = \infty$.

2.3.7 引理. 设 G 为群， $a \in G$.

(1) 如果 $\mathrm{ord}(a) = \infty$, 则对任整数 h, k 有： $a^h = a^k$ 当且仅当 $h = k$. 特别是，对任非零整数 k 有 $\mathrm{ord}(a^k) = \infty$.

(2). 如果 $\mathrm{ord}(a) = m < \infty$, 则对任整数 h, k 有： $a^h = a^k$ 当且仅当 $h \equiv k \pmod m$. 特别是，对任整数 k 有 $\mathrm{ord}(a^k) = \frac{m}{\gcd(k,m)}$.

证. (2). $a^h = a^k$ 当且仅当 $a^{h-k} = 1$; 用欧氏除法， $k - h = mq + r$, $0 \le r < m$; $1 = a^{h-k} = a^{mq+r} = a^{mq}a^r = 1^q a^r = a^r$; 按阶的定义， $a^{h-k} = 1$ 当且仅当 $r = 0$; 当且仅当 $h \equiv k \pmod m$.

$(a^k)^\ell = 1$ 当且仅当 $k\ell \equiv 0 \pmod m$ 当且仅当 $\ell \equiv 0 \pmod{\frac{m}{\gcd(k,m)}}$. □

由上面的引理，得下述定理

2.3.8 定理. 设 $G = \langle a\rangle$ 是循环群.

(1) 如果 $\mathrm{ord}(a) = \infty$, 则 $G = \{\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots\}$ 是 G 的全部互不相同的元素；此时有同构

$$\varphi : \quad \mathbb{Z} \longrightarrow G, \quad k \longmapsto a^k\ .$$

(2) 如果 $\mathrm{ord}(a) = m < \infty$, 则 $G = \{1, a, a^2, \cdots, a^{m-1}\}$ 是 G 的全部互不相同的元素；此时有同构

$$\varphi : \quad \mathbb{Z}_m \longrightarrow G, \quad [k] \longmapsto a^k\ .$$

证. $\varphi\colon \mathbb{Z}\to G,\ k\mapsto a^k$, 是群的满同态.

(1). 由 2.3.7(1), φ 也是单的，故为同构.

(2). 由 2.3.7(2), $G=\{1,\ a,\ a^2,\ \cdots,\ a^{m-1}\}$ 是 G 的全部互不相同的元素，从而 φ 也是单的，故为同构. □

2.3.9 推论. **(1)** *设 G 是群，$a\in G$. 则 $|\langle a\rangle|=\mathrm{ord}(a)$; 特别是 $\mathrm{ord}(a)\Big||G|$.*

(2) *设 $G=\langle a\rangle$ 是 m 阶循环群. 则 $G=\langle a^k\rangle \iff [k]\in\mathbb{Z}_m^\times$.* □

注. 也就是说，无限阶循环群 $G=\langle a\rangle$ 有 2 个元可以是循环生成元：$a,\ a^{-1}$. 而 m 阶循环群中有 $\varphi(m)$ 个元素的阶是 m, 它们也只有它们中的任一个可以是循环生成元.

2.3.10 定理. *设 $G=\langle a\rangle$ 是 m 阶循环群，设 $m=dq$. 则*

(1) *$\langle a^q\rangle$ 是 G 的阶为 d 的子群.*

(2) *如果 $H\le G$ 且 $|H|\Big|d$, 则 $H\subseteq\langle a^q\rangle$; 特别的，$\langle a^q\rangle$ 是 G 的惟一的阶为 d 的子群.*

证. (1). 由引理 2.3.7, $\mathrm{ord}(a^q)=d$.

(2). 任取 $x\in H$, 由上推论，$\mathrm{ord}(x)\Big|d$, 故 $x^d=1$. 因为 $G=\langle a\rangle$, 可写 $x=a^k$, 就有 $a^{kd}=1$. 那么 $m|kd$, 即 $qd|kd$, 从而 $q|k$; 写 $k=qh$, 则 $a^k=(a^q)^h\in\langle a^q\rangle$. 得 $H\subseteq\langle a^q\rangle$. □

利用循环群的知识证明一个数论公式：

2.3.11. $\sum_{d|m}\varphi(d)=m$.

证. 设 $G=\langle a\rangle$ 是 m 阶循环群. 对任 $d|m$, 令 G 中阶为 d 的元素个数为 $\psi_G(d)$. 则

$$\sum_{d|m}\psi_G(d)=m$$

由上述引理，G 有惟一一个 d 阶子群，它是循环子群. 任何 d 阶元在这个子群中. 再由推论 2.3.9, 这个循环子群中的 d 阶元有 $\varphi(d)$ 个，所以 $\psi_G(d)=\varphi(d)$. 代入上式就得所求证等式. □

2.3.12 定理. *设有限群 G 阶为 m. 若对任 $d|m$, G 至多有 d 个元 x 满足 $x^d=1$, 则 G 是循环群.*

证. 对任 $d|m$ 设 G 中阶为 d 元素个数为 $\psi_G(d)$. 若 $\psi_G(d)>0$, 则 G 有 d 阶元 a, 它生成 d 阶循环子群 $\langle a\rangle$, 其中的 d 个元素 x 均满足 $x^d=1$; 由假设，G 的 d 阶元都只能在子群 $\langle a\rangle$ 中. 而 $\langle a\rangle$ 中的 d 阶元共有 $\varphi(d)$ 个，故 $\psi_G(d)=\varphi(d)$. 这就是说 $\psi_G(d)=0$ 或 $\psi_G(d)=\varphi(d)$. 但是 $\sum_{d|m}\psi_G(d)=m$; 但又有 $\sum_{d|m}\varphi(d)=m$; 所以只能是对任 $d|m$ 有 $\psi_G(d)=\varphi(d)$. 取 $d=m$, 就有 $\psi_G(m)=\varphi(m)>0$. 因此 G 有 m 阶元素. □

推论. *数域的乘法群的有限子群必为循环群.* □

习题 2.3

1. 证明：

(1). 群 G 的任意一些子群的交集仍为子群.

(2). 群 G 的子群的并集不一定是子群.

2. 设 G 是群， $a, b \in G$ 是有限阶元且 $\mathrm{ord}(a) = m$, $\mathrm{ord}(b) = n$.

(1). 设 $ab = ba$. 证明 $\mathrm{ord}(ab) \,\Big|\, \frac{mn}{\gcd(m,n)}$; 举例说明不一定有 $\mathrm{ord}(ab) = \frac{mn}{\gcd(m,n)}$.

(2). 设 $ab = ba$ 且 $\gcd(m, n) = 1$, 证明 $\mathrm{ord}(ab) = mn$.

(3). 试举出这样的例子： $ab \neq ba$, $\mathrm{ord}(ab) = \infty$.

3. 设 G 是群， $a \in G$ 是有限阶元且 $|a| = mn$, $\gcd(m, n) = 1$. 证明：

(1). 存在 $b, c \in G$ 满足 $bc = cb$, $|b| = m$, $|c| = n$, $a = bc$.

(2). 如果 $b', c' \in G$ 也满足 $b'c' = c'b'$, $|b'| = m$, $|c'| = n$, $a = b'c'$, 那么 $b' = b$, $c' = c$.

4. 设 G 是群. 记 $Z(G) = \{\, z \in G \mid xz = zx\,,\ \forall\, x \in G \,\}$, 称为 G 的中心. 证明：

(1). $Z(G) \trianglelefteq G$.

(2). 如果 G 不是交换群，那么商群 $G/Z(G)$ 不是循环群.

5. 习题 2.1.5 中，旋转 $R(\theta)$ 为有限阶元当且仅当旋转角 θ 是周角 2π 的有理倍数.

§2.4 生成和关系

内容提要: 二面体群的生成和关系；二个元素生成的群，自由群；多个元素生成的群.

上节讲到一个元素按关系生成的群： $\langle\, a \mid a^n = 1 \,\rangle$, 它是 n 阶循环群，见 2.3.5.

本节介绍一般的生成和关系. 以两个元素按一些关系生成一个群为例，说明主要思想和主要结论.

二面体群 D_n 的生成和关系

看 $\mathbb{R}^2$ 的欧氏变换群的一个例子：正 n 边形的自同构群 — $2n$ 阶的 二面体群:

2.4.1
$$D_n = \left\{\, \rho_0,\ \rho_{\frac{2\pi}{n}},\ \cdots,\ \rho_{\frac{2(n-1)\pi}{n}},\ \sigma_0,\ \sigma_{\frac{\pi}{n}},\ \cdots,\ \sigma_{\frac{(n-1)\pi}{n}} \right\},$$

其中 ρ_θ 表示绕原点旋转 θ 角的旋转， σ_η 表示沿过原点倾角 η 的直线的反射. 那么：

- ρ_θ 对应矩阵 $R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$; 使用 §2.1 中欧氏变换的记号，就是

$$\rho_\theta = \alpha_{R(\theta),\,0}\ .$$

- σ_η 对应矩阵

$$T(\eta) = \begin{pmatrix} \cos\eta & -\sin\eta \\ \sin\eta & \cos\eta \end{pmatrix} \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \begin{pmatrix} \cos\eta & -\sin\eta \\ \sin\eta & \cos\eta \end{pmatrix}^{-1} = \begin{pmatrix} \cos 2\eta & \sin 2\eta \\ \sin 2\eta & -\cos 2\eta \end{pmatrix},$$

就是

$$\sigma_\eta = \alpha_{T(\eta),\,0}\ .$$

显然

$$\rho_{\theta_1}\rho_{\theta_2} = \rho_{\theta_1+\theta_2}\ , \quad \text{特别,} \quad \rho_\theta^k = \rho_{k\theta}\ .$$

而且易计算:

- $\rho_\theta\sigma_\eta$, 对应矩阵

$$\begin{aligned} R(\theta)T(\eta) &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos 2\eta & \sin 2\eta \\ \sin 2\eta & -\cos 2\eta \end{pmatrix} \\ &= \begin{pmatrix} \cos(2\eta+\theta) & \sin(2\eta+\theta) \\ \sin(2\eta+\theta) & -\cos(2\eta+\theta) \end{pmatrix} \\ &= \begin{pmatrix} \cos 2(\eta+\frac{\theta}{2}) & \sin 2(\eta+\frac{\theta}{2}) \\ \sin 2(\eta+\frac{\theta}{2}) & -\cos 2(\eta+\frac{\theta}{2}) \end{pmatrix} \\ &= T(2(\eta+\tfrac{\theta}{2}))\ , \end{aligned}$$

即

$$\rho_\theta\sigma_\eta = \sigma_{\eta+\frac{\theta}{2}}\ .$$

- $\sigma_\eta\rho_\theta$, 对应矩阵

$$\begin{aligned} T(\eta)R(\theta) &= \begin{pmatrix} \cos 2\eta & \sin 2\eta \\ \sin 2\eta & -\cos 2\eta \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \\ &= \begin{pmatrix} \cos(2\eta-\theta) & \sin(2\eta-\theta) \\ \sin(2\eta-\theta) & -\cos(2\eta-\theta) \end{pmatrix} \\ &= \begin{pmatrix} \cos 2(\eta-\frac{\theta}{2}) & \sin 2(\eta-\frac{\theta}{2}) \\ \sin 2(\eta-\frac{\theta}{2}) & -\cos 2(\eta-\frac{\theta}{2}) \end{pmatrix} \\ &= T(2(\eta-\tfrac{\theta}{2}))\ , \end{aligned}$$

即

$$\sigma_\eta\rho_\theta = \sigma_{\eta-\frac{\theta}{2}}\ .$$

- $\sigma_{\eta_1}\sigma_{\eta_2}$ 对应矩阵

$$\begin{aligned} T(\eta_1)T(\eta_2) &= \begin{pmatrix} \cos 2\eta_1 & \sin 2\eta_1 \\ \sin 2\eta_1 & -\cos 2\eta_1 \end{pmatrix}\begin{pmatrix} \cos 2\eta_2 & \sin 2\eta_2 \\ \sin 2\eta_2 & -\cos 2\eta_2 \end{pmatrix} \\ &= \begin{pmatrix} \cos 2(\eta_1-\eta_2) & -\sin 2(\eta_1-\eta_2) \\ \sin 2(\eta_1-\eta_2) & \cos 2(\eta_1-\eta_2) \end{pmatrix} \\ &= R(2(\eta_1-\eta_2))\ , \end{aligned}$$

即

$$\sigma_{\eta_1}\sigma_{\eta_2} = \rho_{2(\eta_1-\eta_2)}\ .$$

小结以上公式如下：

2.4.2
$$\begin{cases} \rho_{\theta_1}\rho_{\theta_2}=\rho_{\theta_1+\theta_2}\ , \quad \text{特别,}\quad \rho_\theta^k=\rho_{k\theta}\ . \\ \rho_\theta\sigma_\eta=\sigma_{\eta+\frac{\theta}{2}}\ ; \qquad \sigma_\eta\rho_\theta=\sigma_{\eta-\frac{\theta}{2}}\ . \\ \sigma_{\eta_1}\sigma_{\eta_2}=\rho_{2(\eta_1-\eta_2)}\ . \end{cases}$$

利用这些公式，对二面体群 D_n, 见 2.4.1, 易知：

$$\rho_{\frac{2\pi}{n}}^i=\rho_{\frac{2i\pi}{n}}\ , \qquad i=0,1,\cdots,n-1\ ;$$

$$\rho_{\frac{2\pi}{n}}^i\sigma_0=\sigma_{\frac{i\pi}{n}}\ , \qquad i=0,1,\cdots,n-1\ ;$$

所以

$$\rho_{\frac{2\pi}{n}}^i\sigma_0^j\ , \qquad i=0,1,\cdots,n-1\ ,\ j=0,1\ ;$$

恰是 D_n 的全部 $2n$ 个元素.

另一方面，还易验证： $\rho_{\frac{2\pi}{n}}$ 和 σ_0 满足：

$$\rho_{\frac{2\pi}{n}}^n=1=\sigma_0^2\,, \qquad \sigma_0\rho_{\frac{2\pi}{n}}\sigma_0^{-1}=\rho_{\frac{2\pi}{n}}^{-1}\ ;$$

从这三个关系式，对 $\rho_{\frac{2\pi}{n}}$, σ_0 的任何表达式 $\cdots\ \sigma_0\,\rho_{\frac{2\pi}{n}}^i\ \cdots$ 可以变形

$$\cdots\ \sigma_0\,\rho_{\frac{2\pi}{n}}^i\ \cdots\ =\ \cdots\ \sigma_0\,\rho_{\frac{2\pi}{n}}^i\,\sigma_0^{-1}\sigma_0\ \cdots\ =\ \cdots\ \rho_{\frac{2\pi}{n}}^{-i}\,\sigma_0\ \cdots$$

反复使用这种变形，可以把 $\rho_{\frac{2\pi}{n}}$, σ_0 的任何表达式中的 σ_0 全部移至尾部，简化为表达式 $\rho_{\frac{2\pi}{n}}^i\sigma_0^j$. 因此我们说：

“群 D_n 可以由元素 $\rho_{\frac{2\pi}{n}}$, σ_0 通过关系 $\rho_{\frac{2\pi}{n}}^n=1=\sigma_0^2$, $\sigma_0\rho_{\frac{2\pi}{n}}\sigma_0^{-1}=\rho_\theta^{-1}$ 生成.”

用以下表达式表示这句话：

$$D_n=\left\langle\ \rho_{\frac{2\pi}{n}},\ \sigma_0\ \middle|\ \rho_{\frac{2\pi}{n}}^n=1=\sigma_0^2,\ \sigma_0\rho_{\frac{2\pi}{n}}\sigma_0^{-1}=\rho_{\frac{2\pi}{n}}^{-1}\ \right\rangle\ .$$

更简单地，可以把关系写成生成元的表达式，如 $\rho_{\frac{2\pi}{n}}^n$ 等等放在尖括号内右部，表示这些表达式等于 1; 即写成

2.4.3
$$D_n=\left\langle\ \rho_{\frac{2\pi}{n}}\ ,\ \sigma_0\ \middle|\ \rho_{\frac{2\pi}{n}}^n\ ,\ \sigma_0^2\ ,\ \sigma_0\rho_{\frac{2\pi}{n}}\sigma_0^{-1}\rho_{\frac{2\pi}{n}}\ \right\rangle\ .$$

其中 $\rho_{\frac{2\pi}{n}}$, σ_0 称为 D_n 的两个 生成元, $\rho_{\frac{2\pi}{n}}^n$, σ_0^2 , $\sigma_0\rho_{\frac{2\pi}{n}}\sigma_0^{-1}\rho_{\frac{2\pi}{n}}$ 称为 D_n 的三个 生成关系.

由两个元素生成的群

如果群 G 由两个元 a,b 生成，那么由 2.3.2′ 知

$$G=\{\,a^{i_1}b^{j_1}a^{i_2}b^{j_2}\cdots a^{i_k}b^{j_k}\mid i_\ell,j_\ell\in\mathbb{Z},\ k\geq 0\}\ , \tag{T}$$

表达式 $a^{i_1}b^{j_1}a^{i_2}b^{j_2}\cdots a^{i_k}b^{j_k}$ 中除 i_1, j_k 外其他 i_ℓ, j_ℓ 非零 ($i_1=0$ 是说表达式以 b^{j_1} 开头, $j_k=0$ 是说表达式以 a^{i_k} 结尾). $k=0$ 时是空表达式, 表示单位元 1. 为方便, 我们称这样的表达式为 "非交换洛朗单项表达式", "洛朗 (Laurent)" 是说单项式中幂指数容许负整数, "非交换" 是说 a, b 不交换, 例如 $ab^{-1}a^2$ 与 a^3b^{-1} 是不同表达式. 换言之, 除了相邻同底幂合并外, 不可交换顺序去合并同底幂. 如 aa^2b^{-1} 与 a^3b^{-1} 是同一表达式, 但 $ab^{-1}a^2$ 与 a^3b^{-1} 是不同表达式.

但是在一个群 G 中, 不同的非交换洛朗单项表达式可能是同一个元素, 例如 D_n 中: 为简单, 记 $a:=\rho_{\frac{2\pi}{n}}$, $b:=\sigma_0$; 则

"bab^{-1} 与 a^{-1} 是不同表达式, 但在 D_n 中是同一个元素."

前面我们已经看到, 这等价于说:

"$bab^{-1}a$ 与空表达式 1 是不同表达式, 但在 D_n 中是同一个元素."

一般地,两个元 a, b 生成的群 G 中某些非空非交换洛朗单项表达式 $a^{i_1}b^{j_1}a^{i_2}b^{j_2}\cdots a^{i_k}b^{j_k}$ 可能为 1, 即生成元可能受到某些关系式约束.

2.4.4 定义. 符号如上. 如果任何非空非交换洛朗单项表达式 $a^{i_1}b^{j_1}a^{i_2}b^{j_2}\cdots a^{i_k}b^{j_k}\neq 1$, 就称群 G 是由 a,b 自由生成的 *自由群*.

引理. 记号如上. 以下两条等价:

(i) G 是 a, b 自由生成的自由群, 即 a, b 的任何非空单项表达式不等于 1.

(ii) 两个单项表达式相等 $a^{i_1}b^{j_1}\cdots a^{i_k}b^{j_k}=a^{i'_1}b^{j'_1}\cdots a^{i'_{k'}}b^{j'_{k'}}$ 当且仅当 $k=k'$ 且 $i_\ell=i'_\ell$, $j_\ell=j'_\ell$, $\forall\ \ell=1,\cdots,k$.

证. (ii) $\Rightarrow$ (i). 显然, 因为: 如果表达式 $a^{i_1}b^{j_1}\cdots a^{i_k}b^{j_k}=1$, 则由 (ii), 必须是 $k=0$, 即 $a^{i_1}b^{j_1}\cdots a^{i_k}b^{j_k}$ 只能是空表达式.

(i) $\Rightarrow$ (ii). 显然只需证明必要性. 设

$$a^{i_1}b^{j_1}a^{i_2}b^{j_2}\cdots a^{i_k}b^{j_k}=a^{i'_1}b^{j'_1}a^{i'_2}b^{j'_2}\cdots a^{i'_{k'}}b^{j'_{k'}}\ .$$

两边左乘 $b^{-j_k}a^{-i_k}\cdots b^{-j_2}a^{-i_2}b^{-j_1}a^{-i_1}$ 得

$$1=b^{-j_k}a^{-i_k}\cdots b^{-j_2}a^{-i_2}b^{-j_1}\underline{a^{-i_1}\,a^{i'_1}}\,b^{j'_1}a^{i'_2}b^{j'_2}\cdots a^{i'_{k'}}b^{j'_{k'}}\ .$$

由条件 (i), 等式右端必须是空表达式;因此下划线的两个同底幂合并必须是零次幂 $a^{-i_1}a^{i'_1}=a^{i_1+i'_1}=a^0=1$, 即 $i_1=i'_1$. 带入上式得

$$\begin{aligned}1&=b^{-j_k}a^{-i_k}\cdots b^{-j_2}a^{-i_2}b^{-j_1}\,1\,b^{j'_1}a^{i'_2}b^{j'_2}\cdots a^{i'_{k'}}b^{j'_{k'}}\\&=b^{-j_k}a^{-i_k}\cdots b^{-j_2}a^{-i_2}\underline{b^{-j_1}\,b^{j'_1}}\,a^{i'_2}b^{j'_2}\cdots a^{i'_{k'}}b^{j'_{k'}}\ .\end{aligned}$$

同上推理, 必须是 $j_1=j'_1$, $b^{-j_1}\,b^{j'_1}=b^0=1$. 得

$$1=b^{-j_k}a^{-i_k}\cdots b^{-j_2}\underline{a^{-i_2}\,a^{i'_2}}\,b^{j'_2}\cdots a^{i'_{k'}}b^{j'_{k'}}\ .$$

依此类推，最后得 $k=k'$ 且 $i_\ell=i'_\ell$, $j_\ell=j'_\ell$, $\forall\ \ell=1,\cdots,k$. □

两个元素生成的自由群存在. 一方面可以在具体群中找到这样的群；另一方面我们可以形式地构造这样的群. 现在我们就来形式地构造两个元素生成的自由群.

令 $X=\{x,\ y\}$. 表达式

2.4.4 $$x^{i_1}y^{j_1}x^{i_2}y^{j_2}\cdots x^{i_k}y^{j_k}\ ,\qquad i_1,\cdots,i_k,j_1,\cdots,j_k\in\mathbb{Z}\ ,$$

其中除 i_1, j_k 外其他指数均不为零 ($i_1=0$ 是说 $x^{i_1}=1$ 应被删去即以 y^{j_1} 开头；同样, $j_k=0$ 是说以 x^{i_k} 结尾), 称为不定元 x, y 的 **非交换洛朗单项式**. $k=0$ 时称为空单项式, 记作 1. 不定元 x, y 的非交换洛朗单项式可记作 $f(x,y)$, 也称为 X 上的 **非交换洛朗单项式**, 记作 $f(X)$. 两个非交换洛朗单项式相等 $x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}=x^{i'_1}y^{j'_1}\cdots x^{i'_{k'}}y^{j'_{k'}}$ 是说 $k=k'$ 且 $i_\ell=i'_\ell$, $j_\ell=j'_\ell$, $\forall\ \ell=1,\cdots,k$.

令 $F(X)=\{X$ 上的非交换洛朗单项式$\}$ 是所有 X 上的非交换洛朗单项式的集合. 在 $F(X)$ 上定义乘法为非交换洛朗单项式的乘积，即 $x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}$ 与 $x^{i'_1}y^{j'_1}\cdots x^{i'_{k'}}y^{j'_{k'}}$ 的乘积就是把它们连接起来

$$x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}\ x^{i'_1}y^{j'_1}\cdots x^{i'_{k'}}y^{j'_{k'}}$$

但这不一定是非交换洛朗单项式，因为，第一：可能有相邻的幂是同底的幂需要合并：如果左式的尾部与右式的首部字母相同，就把该同底的幂合并：如 $j_k\neq0$ 且 $i'_1=0$ 即左式尾部是 y^{j_k}, 右式首部是 $y^{j'_1}$, 合并为 $y^{j_k+j'_1}$, 得：

$$x^{i_1}y^{j_1}x^{i_2}y^{j_2}\cdots x^{i_k}y^{j_k+j'_1}x^{i'_2}y^{j'_2}\cdots x^{i'_k}y^{j'_k}\ ;$$

又如 $j_k=0$ 且 $i'_1\neq0$ 即左式尾部是 x^{i_k}, 右字首部是 $x^{i'_1}$, 合并为 $x^{i_k+i'_1}$, 得：

$$x^{i_1}y^{j_1}x^{i_2}y^{j_2}\cdots x^{i_k+i'_1}y^{j'_1}x^{i'_2}y^{j'_2}\cdots x^{i'_k}y^{j'_k}\ .$$

第二：合并后可能产生零次幂需要删去. 总之，对连接得的序列按两个规则操作：

- 相邻同底幂合并 (但是不能交换顺序去合并同底幂);
- 删去零次幂.

直至得到一个非交换洛朗单项式.

例如：

$$(xy^{-1}x^2)(x^3y)=xy^{-1}x^2\,x^3y^{-1}=xy^{-1}x^5y\ .$$

$$(xy^{-1}x^{-3})(x^3yx)=xy^{-1}x^{-3}\,x^3yx=xy^{-1}x^0yx=xy^{-1}yx=xy^0x=xx=x^2.$$

$$\begin{aligned}(xy^{-1}x^{-3})(x^3yx^{-1}) &= xy^{-1}x^{-3}\,x^3yx^{-1}=xy^{-1}x^0yx^{-1}=xy^{-1}yx^{-1}=xy^0x^{-1}\\ &= xx^{-1}=x^0=1.\end{aligned}$$

现在易验证 $F(X)$ 是一个群. 验证结合律：对 $F(X)$ 的任三个元

$$f(X)=x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}\ ,\quad f'(X)=x^{i'_1}y^{j'_1}\cdots x^{i'_{k'}}y^{j'_{k'}}\ ,\quad f''(X)=x^{i''_1}y^{j''_1}\cdots x^{i''_{k''}}y^{j''_{k''}}\ ;$$

乘积 $\Big(f(X)f'(X)\Big)f''(X)$ 与 $f(X)\Big(f'(X)f''(X)\Big)$ 都是对下述序列

$$x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}\ x^{i'_1}y^{j'_1}\cdots x^{i'_{k'}}y^{j'_{k'}}\ x^{i''_1}y^{j''_1}\cdots x^{i''_{k''}}y^{j''_{k''}}$$

按 “相邻同底幂合并” 和 “删去零次幂” 两个规则操作得的非交换洛朗单项式. 所以乘积 $\Big(f(X)f'(X)\Big)f''(X)=f(X)\Big(f'(X)f''(X)\Big)$. 空单项式 1 是单位元. 最后，按两个规则马上可得，$y^{-j_k}x^{-i_k}\cdots y^{-j_1}x^{-i_1}$ 是 $x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}$ 的逆元.

按构造，$F(X)$ 由 $x,\,y$ 两个元素生成；而且，任何非空的非交换洛朗单项式都不是空单项式 1. 所以得到结论：

2.4.5 结论. *上面构造的群 $F(X)$ 是集合 $X=\{x,y\}$ 生成的自由群.* □

注. 如果仅考虑非交换单项式，即不容许负整数幂，那么得到集合

$$X^*=\{\,x,y\text{ 的非交换单项式}\,\}\ ;$$

可同样定义连接运算，而且，因为没有负幂所以两个单项式连接后只需合并相邻同底幂就得到非交换单项式. 这样得到的 X^* 是幺半群，称为 $X=\{x,y\}$ 上的自由幺半群.

回到自由群 $F(X)$. 它的元素是非交换洛朗单项式 $f(x,y)=x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}$；那么对任一其他的群 G 的任意元 $a,b\in G$, 可以赋值，即代入 a,b 计算 $f(a,b)\in G$. 例如 $f(x,y)=x^{-2}yx$, 则 $f(a,b)=a^{-2}ba$. 因此得映射

$$\tau:\quad F(X)\longrightarrow G\,,\quad x^{i_1}y^{j_1}x^{i_2}y^{j_2}\cdots x^{i_k}y^{j_k}\longmapsto a^{i_1}b^{j_1}a^{i_2}b^{j_2}\cdots a^{i_k}b^{j_k}\ ;$$

容易验证这是群同态；而且 $\tau(x)=a$, $\tau(y)=b$. 换言之

2.4.6 结论. *从 $F(X)$ 的自由生成集 $X=\{x,y\}$ 到群 G 的任何映射 $x\mapsto a$, $y\mapsto b$, 唯一地扩张成为群同态 $\tau:F(X)\to G$.*

把这结论应用于 2.4.3 中的二面体群 D_n, $x\mapsto\rho_{\frac{2\pi}{n}}$, $y\mapsto\sigma_0$, 就唯一地扩张成为群同态 (为简单，记 $\frac{2\pi}{n}=:\theta$):

$$\tau:\quad F(X)\longrightarrow D_n\,,\quad x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}\longmapsto\rho_\theta^{i_1}\sigma_0^{j_1}\cdots\rho_\theta^{i_k}\sigma_0^{j_k}\ ;$$

而 D_n 由 ρ_θ,σ_0 生成，所以 τ 是满同态. 再按照 2.4.3 中的关系，有：

$$\begin{aligned}\tau(x^n)&=\tau(x)^n=\rho_\theta^n=1\ ;\\ \tau(y^2)&=\tau(y)^2=\sigma_0^2=1\ ;\\ \tau(yxy^{-1}x)&=\tau(y)\tau(x)\tau(y)^{-1}\tau(x)=\sigma_0\rho_\theta\sigma_0^{-1}\rho_\theta=1\ ;\end{aligned}$$

即： x^n, y^2, $yxy^{-1}x$ 都在 $\mathrm{Ker}(\tau)$ 中. 而且只要这三个关系就可确定 D_n, 所以 $\mathrm{Ker}(\tau)$ 是包含这三个非交换洛朗单项式的 $F(X)$ 的最小正规子群.

定义. 群 G 的子集 S*生成* 的正规子群是指所有包含 S 的 G 的正规子群之交，它是 G 的包含 S 的正规子群中最小的一个.

使用这个术语，上述 $\mathrm{Ker}(\tau)$ 是 $F(X)$ 的由 $\{x^n,\ y^2,\ yxy^{-1}x\}$ 生成的正规子群.

如同 §2.3, 我们把上面陈述的事情表达为一个短正合序列：

2.4.7
$$1 \longrightarrow \mathrm{Ker}(\tau) \longrightarrow F(X) \xrightarrow{\tau} D_n \longrightarrow 1\ .$$

进一步，设 H 是一个群，把 D_n 的生成元 ρ_θ, σ_0 分别对应于元素 $h, k \in H$, 即 $\rho_\theta \mapsto h$, $\sigma_0 \mapsto k$, 如果这能扩张成为群同态 $\varphi : D_n \to H$, 那么 φ 肯定把关系映射为 1:

$$h^n = \varphi(\rho_\theta)^n = \varphi(\rho_\theta^n) = \varphi(1) = 1\ ;$$

$$k^2 = \varphi(\sigma_0)^2 = \varphi(\sigma_0^2) = \varphi(1) = 1\ ;$$

$$khk^{-1}h = \varphi(\sigma_0)\varphi(\rho_\theta)\varphi(\sigma_0)^{-1}\varphi(\rho_\theta) = \varphi(\sigma_0\rho_\theta\sigma_0^{-1}\rho_\theta) = 1\ ;$$

反过来，如果 $h, k \in H$ 满足 D_n 的生成元的同样的关系，即

$$h^n = k^2 = khk^{-1}h = 1\ ,$$

那么 $\rho_\theta \mapsto h$, $\sigma_0 \mapsto k$ 唯一地扩张成为群同态：

$$D_n \longrightarrow H\ , \quad \rho_\theta^i\sigma_0^j \longmapsto h^i k^j\ .$$

(**证明**: 映射分解定理.)

2.4.8 结论. *设 H 是群， $h, k \in H$. 则 $\rho_\theta \mapsto h$, $\sigma_0 \mapsto k$, 可以扩张为群同态的充要条件是 h, k 也满足 3.4.3 中同样的关系： $h^n = 1$, $k^2 = 1$, $khk^{-1} = h$.* □

一般情形概述

对多个元生成的群，从 2.4.4 到 2.4.8 的过程都可以同样完成；主要结论如下.

2.4.9 定义. 设群 G 由元素 $a_1, \cdots, a_n$ 生成，则

$$G = \left\{ b_1^{i_1} b_2^{i_2} \cdots b_k^{i_k} \;\middle|\; \text{每 } b_t \in \{a, \cdots, a_n\},\ \text{每 } i_t \in \mathbb{Z} - \{0\},\ k \geq 0 \right\}$$

其中 $b_t \neq b_{t+1}$, $t = 1, \cdots k-1$, 是 $a_1, \cdots, a_n$ 的非交换洛朗单项表达式的集合. 如果任何非空的非交换洛朗单项表达式 $b_1^{i_1} b_2^{i_2} \cdots b_k^{i_k} \neq 1$, 则称 G 是由自由元 $a_1, \cdots, a_n$ 生成的 *自由群*.

设集合 $X = \{x_1, \cdots, x_n\}$,

2.4.10. 令 $F(X)$ 是 X 上的所有非交换洛朗单项式的集合

$$F(X) = \{\, y_1^{i_1} \cdots y_k^{i_k} \mid y_1, \cdots, y_k \in X,\ i_1, \cdots, i_k \in \mathbb{Z} - \{0\},\ k \geq 0 \,\}$$

其中 $y_t \neq y_{t+1},\ t = 1, \cdots k-1$; 在连接运算 (遵从规则 "相邻同底幂合并","删去零次幂") 下它是一个群, 称为 X 生成的自由群.

注意: 非交换洛朗单项式可记作 $f(x_1, \cdots, x_n) = y_1^{i_1} \cdots y_k^{i_k}$, 其中 $y_1, \cdots, y_k \in X$, $i_1, \cdots, i_k \in \mathbb{Z} - \{0\}$, 且 $y_t \neq y_{t+1},\ t = 1, \cdots k-1$.

2.4.11. 如果 G 是群, $a_1, \cdots, a_n \in G$ 是任意元, 那么 $x_i \mapsto a_i,\ i = 1, \cdots, n,$ 可以唯一地扩张成群同态

$$\tau_{a_1, \cdots, a_n} : \quad F(X) \longrightarrow G, \quad f(x_1, \cdots, x_n) \longmapsto f(a_1, \cdots, a_n)\ .$$

2.4.12. 如果 G 可由 n 个元 $a_1, \cdots, a_n$ 生成, 那么 $x_i \mapsto a_i,\ i = 1, \cdots, n,$ 可以扩张成群的满同态 $\tau : F(X) \to G,$ 有短正合序列:

$$1 \longrightarrow \mathrm{Ker}(\tau) \longrightarrow F(X) \xrightarrow{\tau} G \longrightarrow 1\ ;$$

如果同态核 $\mathrm{Ker}(\tau)$ 是由 $r_1, \cdots, r_m \in F(X)$ 正规生成的正规子群, 注意每 $r_j = r_j(x_1, \cdots, x_n)$ 都是关于 $x_1, \cdots, x_n$ 的非交换洛朗单项式, 那么把 r_j 中的 x_i 换为 a_i, 就得到 G 的生成关系; 即

$$G = \langle\, a_1, \cdots, a_n \mid r_1(a_1, \cdots, a_n),\ \cdots,\ r_m(a_1, \cdots, a_n) \,\rangle$$

2.4.13(Van Dyck 定理). 设 G 如上 *2.4.12*; 设 H 是群, $h_1, \cdots, h_n \in H,$ 那么映射

$$a_i \mapsto h_i\ , \qquad i = 1, \cdots, n\ ,$$

可以扩张为群同态 $f : G \to H$ 当且仅当群 H 的元素 $h_1, \cdots, h_n$ 也满足关系 $r_1, \cdots, r_m,$ 即

$$r_j(h_1, \cdots, h_n) = 1\ , \qquad j = 1, \cdots, m\ .$$

习题 2.4

1. 设 G 是一个群, $S \subseteq G$. 举例说明 S 生成的子群, 与 S 生成的正规子群一般是不相同的. 进一步证明 S 生成的正规子群是 $\bigcup\limits_{g \in G} gSg^{-1}$ 生成的子群.

2. 设群 G 由子集 $T \subseteq G$ 生成: $G = \langle T \rangle$. 设 H 是群. 设 $\varphi : G \to H$ 和 $\psi : G \to H$ 都是群同态. 证明: $\varphi = \psi$ 当且仅当 $\varphi(t) = \psi(t),\ \forall\ t \in T$.

3. 设 $G = \langle\, a \mid a^n \,\rangle$ 是 n 阶循环群. 设 H 是群, $b \in H$. 证明: $a \mapsto b$ 能扩张为群同态 $G \to H,\ a^k \mapsto b^k$, 当且仅当 $\mathrm{ord}(b) \mid n$.

4. 试求从 $\mathbb{Z}_n$ 到 $\mathbb{Z}_m$ 的所有群同态.

5. (1). $\mathrm{GL}_n(\mathbb{C})$ 由初等矩阵的集合 $\mathcal{E}$ 生成.

(2). $\mathrm{SL}_n(\mathbb{C})$ 由消法初等矩阵的集合 $\mathcal{D}$ 生成.

提示: 由线性代数，任一可逆矩阵可写成初等矩阵之积；任一行列式等于 1 的可逆矩阵可写成消法初等矩阵之积.

6. 设 $\alpha_{P,0} \in \mathrm{E}(\mathbb{R}^2)$, 其中 $P \in \mathrm{O}_2(\mathbb{R})$ 且 $P \neq I$. 证明：

(1). 如果 P 没有实根，则 $\alpha_{P,0}$ 是绕原点的旋转.

(2). 如果 P 有实根，则 $\alpha_{P,0}$ 是一个反射，或是中心对称.

7. 设 $\alpha \in \mathrm{E}(\mathbb{R}^2)$ 是欧氏平面 $\mathbb{R}^2$ 的欧氏变换. 如果 $x \in \mathbb{R}^2$ 满足 $\alpha(x) = x$ 就称 x 是 α 的 *不动点*. 证明：

(1). 如果 α 没有不动点，则 α 是一个平移.

(2). 如果 α 恰有一个不动点，则 α 是绕该不动点的一个旋转.

(3). 如果 α 的不动点恰构成一条直线，则 α 是关于该直线的反射.

(4). 除了上述三种情形外， α 必为恒等变换.

8. 求出平面欧氏变换群 $\mathrm{E}(\mathbb{R}^2)$ 的所有有限子群.

提示: 如果 G 是 $E(\mathbb{R}^2)$ 的有限子群. 任取 $x \in \mathbb{R}^2$, 则 $x_0 = \frac{1}{|G|}\sum\limits_{\alpha\in G}\alpha(x)$ 使得 $\alpha(x_0) = x_0, \forall\ \alpha \in G$. 以 x_0 为原点重建坐标系. 那么 $\alpha_{P,u} \in G$ 都使原点不动，故 G 不含平移，即 $u = 0$. G 只含旋转、反射. 分两种情形.

(a). G 只含旋转. 把旋转角都表示为非负的. 令 $1 \neq \rho_\theta \in G$ 是旋转角 θ 最小的旋转. 对任 $\rho_\zeta \in G$, 令 $\zeta = m\theta + \delta$, 其中 $0 \leq \delta < \theta$; 那么 $\rho_\theta^{-m} = \rho_{-m\theta}$ 是旋转角为 $-m\theta$ 的旋转，故 $\rho_\delta = \rho_\theta^{-m}\rho_\zeta \in G$; 由对 θ 的假设，得 $\delta = 0$, 即 $\zeta = m\theta$ ，从而 $\rho_\zeta = \rho_\theta^m$. 故 G 是循环群.

(b). G 含反射 σ. 由上段证明， G 的所有旋转构成循环子群 $\langle\rho_\theta\rangle$. 对任 $\tau \in G$ 是反射， $\tau\sigma$ 是旋转 (见 2.4.2), 即 $\tau\sigma \in \langle\rho_\theta\rangle$; 所以 $\tau = \rho_\theta^i\sigma$. 所以 G 是由旋转 ρ_θ 和反射 σ 生成的二面体群.

§2.5 置换群

内容提要: 共轭计算；共轭类；对换分解；奇偶性；生成集；交错群.

命题. 设 A 与 B 是两个基数相等的有限集合. 设 $f : A \to B$ 是双射. 则映射

$$\tilde{f}: \quad \mathrm{Sym}(A) \xrightarrow{\cong} \mathrm{Sym}(B), \quad \alpha \longmapsto f \cdot \alpha \cdot f^{-1}$$

是群同构并使得

$$(f \cdot \alpha)(a) = \tilde{f}(\alpha) \cdot f(a)\ , \quad \forall\ \alpha \in \mathrm{Sym}(A)\ \forall\ a \in A\ .$$

证. 按照 $\tilde{f}$ 的定义可以容易地直接验证它是群同态. 再从 f 的逆映射 $f^{-1} : B \to A$ 也可诱导

$$\tilde{f^{-1}}: \quad \mathrm{Sym}(B) \xrightarrow{\cong} \mathrm{Sym}(A), \quad \beta \longmapsto f^{-1} \cdot \beta \cdot f$$

那么显然容易验证 $\tilde{f}$ 与 $\tilde{f^{-1}}$ 正好互为逆映射. 所以 $\tilde{f}$ 是群同构. 验证最后的等式：$f\cdot\alpha = f\cdot\alpha\cdot f^{-1}\cdot f = \tilde{f}(\alpha)\cdot f$. 从下面的交换图更容易理解这个等式.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle f\alpha f^{-1}=\tilde{f}} \\ X & \xrightarrow[f]{} & Y \end{array}$$ □

本命题说明：考虑置换群时，集合中的元素是什么并不重要.

因此以下讨论 S_n 和 n 次置换. 在 §2.1 中我们已陈述了下述结论.

2.5.1 命题. **(1)**. *n 次对称群的阶 $|S_n| = n!$.*

(2). *任二个彼此无公共文字的循环置换相乘可交换.*

(3). *任一置换在不记乘积顺序的意义下可以唯一底写成彼此无公共文字的循环置换之积使得每个文字恰出现一次，称为置换的 循环分解.* □

把 n 次置换 α 的循环分解

$$\alpha = (a_{11}a_{12}\cdots a_{1i})(a_{21}a_{22}\cdots a_{2j})\cdots(a_{r1}a_{r2}\cdots a_{rk})$$

中的括号去掉，就是 $1, 2, \cdots, n$ 的一个排列. 如 $(264)(13)(5)$, 去掉括号就是 264135

反之，对 $1, 2, \cdots, n$ 的任一个排列加上括号就可以是一个 n 次置换的循环分解.

2.5.2 引理. *设 $\alpha = (a_{11}a_{12}\cdots a_{1i})(a_{21}a_{22}\cdots a_{2j})\cdots(a_{r1}a_{r2}\cdots a_{rk})$ 是 n 次置换 α 的循环分解, $\gamma\in S_n$. 则 α 的共轭元 $\gamma\alpha\gamma^{-1}$ 的循环分解如下*

$$\gamma\alpha\gamma^{-1} = \Big(\gamma(a_{11})\gamma(a_{12})\cdots\gamma(a_{1i})\Big)\Big(\gamma(a_{21})\gamma(a_{22})\cdots\gamma(a_{2j})\Big)\cdots\Big(\gamma(a_{r1})\gamma(a_{r2})\cdots\gamma(a_{ak})\Big)\ .$$

证. $a_{11}, \cdots, a_{1i}, \cdots, a_{r1}, \cdots, a_{rk}$ 是 $1, 2, \cdots, n$ 的一个排列，所以

$$\gamma(a_{11}), \cdots, \gamma(a_{1i}), \cdots, \gamma(a_{r1}), \cdots, \gamma(a_{rk})$$

也是 $1, 2, \cdots, n$ 的一个排列，因而引理的等式右端是一个循环置换分解. 那么只要证明

$$\gamma\alpha\gamma^{-1}(\gamma(a_{11})) = \gamma(a_{12})\,,\quad \gamma\alpha\gamma^{-1}(\gamma(a_{12})) = \gamma(a_{13})\,,\quad \cdots$$

即可；而这些式子是显然成立的. □

2.5.3 定义. 设 n 次置换 α 的循环分解中长度 ℓ 的循环有 $\lambda_\ell(\alpha)$ ，则 λ_ℓ 是置换 α 的非负整函数，称为置换的第 ℓ 个 *型函数*; 在 α 确定时，简记为 λ_ℓ. 序列 $(\lambda_1,\ \lambda_2,\ \cdots,\ \lambda_n)$ 称为该 n 次置换 α 的 *型*; 型有时也形式地记作 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$.

一个 n 次置换 α 的型显然满足 $\lambda_1+2\lambda_2+\cdots+n\lambda_n = n$; 反过来, 关于变元 $x_1, x_2, \cdots, x_n$ 的方程 $x_1 + 2x_2 + \cdots + nx_n = n$ 的任何非负整数解 $(\lambda_1,\ \lambda_2,\ \cdots,\ \lambda_n)$ 是某些 n 次置换的型.

例如： n=5; 置换 $(124)(35)$ 的型是 $(0,1,1,0,0)$, 它是 $x_1+2x_2+3x_3+4x_4+5x_5=5$ 的非负整数解. 显然 $(1,0,0,1,0)$ 也是这个方程的非负整数解，而它是 5 次置换 $(1435)=(2)(1435)$ 的型.

2.5.4 命题. *对称群 S_n 中两置换 α 与 β 共轭当且仅当 α 与 β 的型相同，即 $\lambda_\ell(\alpha)=\lambda_\ell(\beta)$ ， $\forall\ \ell=1,\cdots,n$.*

证. 若 $\gamma\alpha\gamma^{-1}=\beta$, 由引理 2.5.2, 它们的型相同. 反之设它们的型相同，那么可以把它们的循环分解按循环长度排列使得对应的循环的长度相等：

$$\begin{aligned}\alpha &= (a_{11}a_{12}\cdots a_{1i})(a_{21}a_{22}\cdots a_{2j})\cdots(a_{r1}a_{r2}\cdots a_{rk})\ ,\\ \beta &= (b_{11}\,b_{12}\cdots b_{1i})(b_{21}\,b_{22}\cdots b_{2j})\cdots(b_{r1}\,b_{r2}\cdots b_{rk})\ ;\end{aligned}$$

那么 $a_{11}\,a_{12}\cdots a_{1i}\ \cdots\ a_{r1}\,a_{r2}\cdots a_{rk}$ 与 $b_{11}\,b_{12}\cdots b_{1i}\ \cdots\ b_{r1}\,b_{r2}\cdots b_{rk}$ 都是 $1,\,2,\,\cdots,\,n$ 的排列，所以

$$\gamma=\begin{pmatrix} a_{11}\ a_{12}\ \cdots\ a_{1i}\ a_{21}\ a_{22}\ \cdots\ a_{2j}\ \cdots\ a_{r1}\ a_{r2}\ \cdots\ a_{rk}\\ b_{11}\ \ b_{12}\ \cdots\ b_{1i}\ \ b_{21}\ b_{22}\ \cdots\ b_{2j}\ \ \cdots\ \ b_{r1}\ b_{r2}\ \ \cdots\ \ b_{rk}\end{pmatrix}$$

是一个 n 次置换；仍由引理 2.5.2, 就得 $\gamma\alpha\gamma^{-1}=\beta$. □

用图表示型的方法. 整数 n 的一个 划分 *(partition)* 是指整数序列 $\alpha=(a_1,a_2,\cdots,a_\ell)$ 满足 $a_1\ge a_2\ge\cdots\ge a_\ell>0$ 和 $a_1+a_2+\cdots+a_\ell=n$; 划分图示为：

□ □ ⋯ ⋯ □ a_1 个
□ □ ⋯ □ a_2 个
⋯ ⋯ ⋯
□ ⋯ □ a_ℓ 个

称为 *杨图 (Young tableau).*

例如 $n=5$ 的划分共有 7 个，因而 S_5 共有 7 个共轭类；杨图及相应共轭类代表元列如下表：

杨图	□ □ □ □ □	□ □ □ □ □	□ □ □ □ □
共轭类 代表元	$(1)(2)(3)(4)(5)$ $=(1)$	$(12)(3)(4)(5)$ $=(12)$	$(12)(34)(5)$ $=(12)(34)$

□ □ □ □ □	□ □ □ □ □	□ □ □ □ □	□ □ □ □ □
(123)(4)(5) = (123)	(123)(45)	(1234)(5) = (1234)	(12345)

2.5.5 Cauchy 公式. 型为 $(\lambda_1,\ \lambda_2,\ \cdots,\ \lambda_n)$ 的 n 次置换的个数等于

$$\frac{n!}{\lambda_1!\,\lambda_2!\,\cdots\,\lambda_n!\cdot 1^{\lambda_1}\,2^{\lambda_2}\,\cdots\,n^{\lambda_n}}$$

证. 考虑填空模型

$$\overbrace{(*)\ \cdots\ (*)}^{\lambda_1}\ \overbrace{(**)\ \cdots\ (**)}^{\lambda_2}\ \cdots\ .$$

把 $1,\,2,\,\cdots,\,n$ 填入各 $*$ 位置处, 共有 $n!$ 种填法; 这样就给出了全部型为 $(\lambda_1,\ \lambda_2,\ \cdots,\ \lambda_n)$ 的 n 次置换. 但同一个 n 次置换在此过程中重复得出多次：前 λ_1 个括号的任意排列得出同一个置换, 这种重复有 $\lambda_1!$ 次; 类似地, λ_2 个 $(**)$ 型括号给出 $\lambda_2!$ 次重复; 等等. 又, 同一个 k- 循环可以有 k 种不同写法 (循环中任一文字可以放在首位) , 而 k- 循环有 λ_k 个, 就得到 k^{λ_k} 个重复; 这里 $k=1,2,\cdots,n$. 综合起来, 同一个 n 次置换在上述填空过程中重复得出的次数是 $\lambda_1!\,\lambda_2!\,\cdots\,\lambda_n!\cdot 1^{\lambda_1}\,2^{\lambda_2}\,\cdots\,n^{\lambda_n}$. 这样就得到了 Cauchy 公式. □

例. S_3 中型为 $(1,1,0)$ (对应划分是 $(2,1)$) 的置换有 $3!/(1!2!3!1^1 2^1 3^0)=3$ 个; 即 $(12),\ (13),\ (23)$.

注意到一个简单的事实, 任意 ℓ- 循环可以写成 2- 循环也就是对换之积:

2.5.6 $$(a_1\,a_2\,\cdots,a_\ell)=(a_1\,a_\ell)\,\cdots\,(a_1\,a_3)\,(a_1\,a_2)\ ;$$

对换个数 $\ell-1$ 是循环长度减 1. 那么任意置换 α 就可以写成对换之积. 而且有一种写法的对换因子个数 $T(\alpha)$ 是 α 的循环分解中各循环长度减 1 之和, 即

2.5.7 $$T(\alpha)=\sum_{\ell=1}^{n}(\ell-1)\lambda_\ell(\alpha)=\sum_{\ell=1}^{n}\Big(1-\lambda_\ell(\alpha)\Big)\ .$$

但把置换写成对换之积的写法肯定不是唯一的; 比如, 即使一个对换就还可以写成三个对换之积的形式:

2.5.8 $$(ij)=(1\,i)\,(1\,j)\,(1\,i)\ .$$

我们有下述结论.

2.5.9 置换的对换分解定理. 任意 n 次置换 α 可以写成有限个对换的乘积，其对换因子的个数 $\equiv T(\alpha) \pmod 2$.

证 令 $X=\{x_1, x_2 \cdots, x_n\}$ 是 n 个变元的集合；考虑 X 上的多项式

$$f(X)=\prod_{1\le i<j\le n}(x_i-x_j)\ ;$$

即任一对互异的脚标 $i<j$ 恰对应于一个因式. 由 §2.1 最后的例子知，对任 $\alpha\in S_n$, 按对变元脚标的置换它使 $f(X)$ 变成多项式

$$\alpha f(X)=\prod_{1\le i<j\le n}(x_{\alpha(i)}-x_{\alpha(j)})\ .$$

由于 $\alpha(1),\alpha(2),\cdots,\alpha(n)$ 是 $1,2,\cdots,n$ 的排列， $\alpha f(X)$ 与 $f(X)$ 的因子一一对应：

- 若 $\alpha(i)<\alpha(j)$, 则 $x_{\alpha(i)}-x_{\alpha(j)}$ 既是 $\alpha f(X)$ 的因子也是 $f(X)$ 的因子.
- 若 $\alpha(i)>\alpha(j)$, 则 $x_{\alpha(i)}-x_{\alpha(j)}$ 是 $\alpha f(X)$ 的因子，但 $x_{\alpha(j)}-x_{\alpha(i)}=-(x_{\alpha(i)}-x_{\alpha(j)})$ 是 $f(X)$ 的因子.

所以

$$\alpha f(X)=(-1)^{R(\alpha)}f(X)\ ; \tag{R}$$

其中 $R(\alpha)$ 是排列 $\alpha(1),\alpha(2),\cdots,\alpha(n)$ 的 *逆序数*:

$$R(\alpha)=\Big|\{\,(i,j)\mid 1\le i<j\le n,\ \alpha(i)>\alpha(j)\,\}\Big|\ .$$

下面按 α 的对换分解来确定符号 $(-1)^{R(\alpha)}$. 分别情形由易至难来做.

首先设 $\alpha=(k,\,k+1)$ 是相邻对换. 显然 α 仅仅使 x_k-x_{k+1} 变成 $x_{k+1}-x_k=-(x_k-x_{k+1})$, 而不改变 $f(X)$ 的其他因式的符号，即 $\alpha f(X)=-f(X)$.

再设 $\alpha=(i\,j)$, $i<j-1$, 是不相邻的对换，则可分解为 $2(j-i-1)+1$ 个，即奇数个相邻对换之积：

$$\begin{aligned}(i\,j)\ \ =\ \ &\overbrace{(j-1,\,j)\,(j-2,\,j-1)\cdots(i+1,\,i+2)}^{j-i-1}\cdot(i,\,i+1)\cdot\\ &(i+1,\,i+2)\cdots(j-2,\,j-1)\,(j-1,\,j)\end{aligned} \tag{T}$$

所以 $\alpha f(X)=-f(X)$. 即对任对换 α 恒有 $\alpha f(X)=-f(X)$.

一般情形：把置换 α 写成 $\alpha=\tau_1\cdots\tau_{k-1}\tau_k$ 每个 τ_i 是对换，则

$$\alpha f(X)=\tau_1\cdots\tau_{k-1}\tau_k f(X)=-\tau_1\cdots\tau_{k-1}f(X)=\cdots=(-1)^k f(X)\ .$$

对照前面的等式 (R), 得 $(-1)^k=(-1)^{R(\alpha)}$.

但是由 (2.5.7) 我们已经知道有一种写法 $\alpha = \tau'_1 \cdots \tau'_{T(\alpha)}$; 所以 $\alpha f(X) = (-1)^{T(\alpha)} f(X)$. 故得 $(-1)^k = (-1)^{T(\alpha)}$; 即是 $k \equiv T(\alpha) \pmod 2$. □

推论. $T(\alpha) \equiv R(\alpha) \pmod 2$, 其中 $R(\alpha)$ 是 α 的逆序数. □

2.5.10 定义. 置换 α 称为 偶置换 如果 α 可写成偶数个对换之积; 否则称 α 为 奇置换.

从定理 2.5.9 马上可以得到下述推论, 注意其中 $\{\pm 1\}$ 在乘法之下构成 2 阶群.

2.5.11 推论. 映射 $\sigma: \ S_n \to \{\pm 1\}$, $\sigma(\alpha) = \begin{cases} 1 & \text{若 } \alpha \text{ 是偶置换} \\ -1 & \text{若 } \alpha \text{ 是奇置换} \end{cases}$, 是群同态, 特别地, S_n 中所有偶置换的集合 A_n 是 S_n 的正规子群, 称为 n 次交错群; 且 $|S_n : A_n| = 2$. □

即有正合序列:

$$1 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\sigma} \{\pm 1\} \longrightarrow 1$$

回头看 (2.5.6) 和 (2.5.8):

$$(ij) = (1j)(1i)(1j)$$

$$(i_1\, i_2,\ \cdots,\ i_{\ell-1}\, i_\ell) = (i_1 i_\ell)(i_1 i_{\ell-1}) \cdots (i_1 i_3)(i_1 i_2)\ ;$$

马上知道定理 2.5.9 的另一显然推论是:

2.5.12 推论. S_n, $n \geq 2$, 由 $n-1$ 个元素 $\alpha_i = (1, i+1)$, $i = 1, 2, \cdots, n-1$ 生成, 满足下述关系:

$$\begin{aligned} &\alpha_i^2 = 1\,, && i = 1, \cdots, n-1\,; \\ &(\alpha_i \alpha_j)^3 = 1\,, && 0 < i \neq j < n\,; \\ &(\alpha_i \alpha_j \alpha_k \alpha_j)^2 = 1\,, && i, j, k \text{ 彼此不等}\,. \end{aligned}$$ □

2.5.13 定理. 设 $n \geq 2$. 由 $x_1,\ x_2,\ \cdots,\ x_{n-1}$ 按下列关系生成的群同构于 S_n:

$$\begin{aligned} &x_i^2 = 1\,, && i = 1, \cdots, n-1\,; \\ &(x_i x_j)^3 = 1\,, && 0 < i \neq j < n\,; \\ &(x_i x_j x_k x_j)^2 = 1\,, && i, j, k \text{ 彼此不等}\,. \end{aligned} \tag{RL}$$

证. $n = 2$ 时显然正确, 此时 $\langle x_1 \mid x_1^2 = 1 \rangle \cong S_2$ 是 2 阶循环群. 对 n 归纳. 设 G 是由 $x_1,\ x_2,\ \cdots,\ x_{n-1}$ 按关系 (RL) 生成的群. 考虑对应:

$$x_i \longmapsto (1,\, i+1)\,, \qquad i = 1, \cdots, n-2\,,$$

对应到 S_n 中的元素满足关系 (RL), 由 Van Dyck 定理 2.4.15, 该对应诱导群同态

$$\tau: \quad G \longrightarrow S_n\,, \quad x_i \longmapsto (1,\, i+1)\,;$$

S_n 的生成元在同态象中，所以是满同态. 特别有 $|G| \geq n!$.

设 H 是 G 的子群, 由 $x_1, \cdots, x_{n-2}$ 生成. 由归纳假设，τ 诱导同构 $H \cong S_{n-1} \leq S_n$. 特别有，$|H| = (n-1)!$.

考虑 G 中 H 的左陪集

$$H\,,\ x_{n-1}H\,,\ x_{n-2}x_{n-1}H\,,\ x_{n-3}x_{n-1}H\,,\ \cdots\,,\ x_2x_{n-1}H\,,\ x_1x_{n-1}H\,; \tag{C}$$

我们来证明：任 x_i 与上述任一陪集之积仍为上列陪集之一. 显然

$$x_iH = \begin{cases} H\,, & \text{若 } i < n-1\,, \\ x_{n-1}H\,, & \text{若 } i = n-1. \end{cases}$$

$$x_ix_{n-1}H = \begin{cases} x_ix_{n-1}H\,, & \text{若 } i < n-1\,, \\ H\,, & \text{若 } i = n-1. \end{cases}$$

再看 $x_ix_jx_{n-1}H$ 其中 $j < n-1$. 若 $i = j$, 则 $x_ix_j = 1$ 从而 $x_ix_jx_{n-1}H = x_{n-1}H$.

若 $i = n-1$, 由于 $(x_{n-1}x_j)^3 = 1$, 故

$$x_{n-1}x_jx_{n-1}x_j = (x_{n-1}x_j)^2 = (x_{n-1}x_j)^{-1} = x_j^{-1}x_{n-1}^{-1} = x_jx_{n-1}$$

而 $H = x_jH$, 所以

$$x_{n-1}x_jx_{n-1}H = x_{n-1}x_jx_{n-1}x_jH = x_jx_{n-1}H\ .$$

最后设 $i \neq j$ 且 $i \neq n-1$, 那么 $(x_ix_jx_{n-1}x_j)^2 = 1$, 故

$$x_ix_jx_{n-1}x_j = (x_ix_jx_{n-1}x_j)^{-1} = x_jx_{n-1}x_jx_i\ ;$$

所以

$$x_ix_jx_{n-1}H = x_ix_jx_{n-1}x_jH = x_jx_{n-1}x_jx_iH = x_jx_{n-1}H$$

由于 G 的任意元是一些 x_i 之积，可以断言 (C) 是全部 H 的左陪集. 那么 $|G:H| \leq n$, 从而 $|G| \leq (n-1)!n = n!$.

于是 $|G| = n!$, 从而满同态 $\tau : G \to S_n$ 是同构. □

2.5.14 定义. 如果群 $G \neq 1$, G 只有两个正规子群 1 和 G, 则称 G 为 *单群*.

2.5.15 定理. *交错群 A_n, $n \geq 5$, 是非交换单群.*

证. 设 $1 \neq H \trianglelefteq A_n$; 我们证明 $H = A_n$. 为此先指出：只要能证明 H 中有一个 3- 循环 (3- 轮换) 就行了；这是因为若 $(i_1\,i_2\,i_3) \in H$, 则对任 3- 循环 $(j_1\,j_2\,j_3) \in A_n$, 由引理 2.5.2, 有

$$\begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix} (i_1\ \ i_2\ \ i_3) \begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix}^{-1} = (j_1\ \ j_2\ \ j_3)\,,$$

所以在 $\begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix}$ 是偶置换时就可断言 $(j_1\, j_2\, j_3) \in H$; 若 $\begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix}$ 是奇置换, 因为 $n \geq 5$, 可取 $k, \ell \notin \{j_1, j_2, j_3\}$, 那么 $(k\,\ell)\begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix}$ 是偶置换而

$$(k\ \ \ell)\begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix}(i_1\ \ i_2\ \ i_3)\begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix}^{-1}(k\ \ \ell)^{-1} = (j_1\ \ j_2\ \ j_3)\,,$$

仍得 $(j_1\, j_2\, j_3) \in H$. 总之可断言 H 包含所有 3- 循环. 但是 A_n 由 3- 循环生成 (习题 11), 因此 $H = A_n$.

下面用反证法证明 H 中有一个 3- 循环. 设 H 不含 3- 循环.

如果 H 有一个元的循环分解含大于 3 的循环: $\alpha = (i_1\, i_2\, i_3\, i_4\ \cdots\ i_\ell)\cdots$, 其中可能 $\ell = 4$; 因 $(i_1\, i_2\, i_3) \in A_n$, 故 H 含下述元素 (以下计算参看引理 2.5.2):

$$\beta := (i_1\, i_2\, i_3)\,\alpha\,(i_1\, i_2\, i_3)^{-1} = (i_2\, i_3\, i_1\, i_4\ \cdots\ i_\ell)\cdots$$

那么 H 含元素 (注意 $(i_2\, i_3\, i_1\, i_4\ \cdots\ i_\ell)^{-1} = (i_\ell\ \cdots\ i_4\, i_1\, i_3\, i_2)$)

$$\alpha\beta^{-1} = (i_1\, i_2\, i_3\, i_4\ \cdots\ i_\ell)\cdots\,(i_2\, i_3\, i_1\, i_4\ \cdots\ i_\ell)^{-1}\cdots = (i_1\, i_4\, i_2) \in H\ .$$

与假设 "H 不含 3- 循环" 相矛盾. 所以 H 的任一元的循环分解只含 2- 循环 3- 循环.

如果 H 有元恰含一个 3- 循环, 即有元 $\alpha = (i_1\, i_2\, i_3)(a_1\, a_2)\cdots$; 则 H 含有下述 3- 循环

$$\alpha^2 = (i_1\, i_2\, i_3)^2(a_1\, a_2)^2\cdots = (i_1\, i_3\, i_2) \in H\ ,$$

与 H 不含 3- 循环相矛盾.

如果 H 有一个元至少含 2 个 3- 循环, 即有元 $\alpha = (i_1\, i_2\, i_3)(j_1\, j_2\, j_3)\cdots$, 则

$$\beta = (j_1\, j_2\, i_3)\,\alpha\,(j_1\, j_2\, i_3)^{-1} = (i_1\, i_2\, j_1)(j_2\, i_3\, j_3)\cdots\ \in H\ ,$$

$$\alpha\beta = (i_1\, i_3\, j_1\, i_2\, j_2)\cdots \in H\ ;$$

这与上面已论述的 "H 的元的循环分解只含 2- 循环 3- 循环" 相矛盾.

所以 H 的元的循环分解只能含 2- 循环 (当然是偶数个).

如果 H 有元素其循环分解恰含两个 2- 循环 $\alpha = (i_1\, i_2)(j_1\, j_2)$, 因为 $n \geq 5$, 所以存在 $k \notin \{i_1, i_2, j_1, j_2\}$; 那么

$$\beta = (i_1\, k\, i_2)\,\alpha\,(i_1\, k\, i_2)^{-1} = (k\, i_1)(j_1\, j_2) \in H\ ,$$

$$\alpha\beta = (i_1\, i_2)(j_1\, j_2)\ (k\, i_1)(j_1\, j_2) = (i_1\, k\, i_2) \in H\ ;$$

仍然与 H 不含 3- 循环相矛盾.

最后，H 有元素 α 其循环分解由至少四个 2- 循环构成：$\alpha = (i_1\ i_2)(j_1\ j_2)(k_1\ k_2)\cdots$; 则

$$\beta = (i_2\ j_1)(j_2\ k_1)\,\alpha\,((i_2\ j_1)(j_2\ k_1))^{-1} = (i_1\ j_1)(i_2\ k_1)(j_2\ k_2)(l_1\ l_2)\cdots \in H\ ,$$

$$\alpha\beta = (i_1\ j_2\ k_1)(j_1\ i_2\ k_2) \in H\ .$$

这与 H 的元的轮换分解只含 2- 轮换相矛盾. □

习题 2.5

1. 证明：

(1). ℓ- 循环置换的阶为 ℓ.

(2). 设 α 和 β 是两个无公共文字的循环置换. 证明：$|\alpha\beta| = |\alpha|\cdot|\beta|\Big/(|\alpha|,\ |\beta|)$.

(3). 任一置换 α 的阶是它的循环分解中各循环的长度的最小公倍数.

2. 证明：

(1). 如果 n 次置换 α 的型是 $(\lambda_1, \lambda_2, \cdots, \lambda_n)$, 则 $\lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = n$.

(2). 如果 $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ 是关于变元 $(x_1, x_2, \cdots, x_n)$ 的方程 $x_1 + 2x_2 + \cdots + nx_n = n$ 的非负整数解，则存在 n 次置换 α 它的型是 $(\lambda_1, \lambda_2, \cdots, \lambda_n)$.

3. 求 S_6 有多少个共轭类，写出各共轭类的代表元.

4. 设 n 是自然数. 证明：

$$\sum_{(\lambda_1,\lambda_2,\cdots,\lambda_n)} \frac{1}{\lambda_1!\,\lambda_2!\,\cdots\,\lambda_n!\cdot 1^{\lambda_1}\,2^{\lambda_2}\,\cdots\,n^{\lambda_n}} = 1\ ;$$

其中 $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ 跑遍方程 $x_1 + 2x_2 + \cdots + nx_n = n$ 的非负整数解.

5. 偶置换与偶置换之积为偶置换；奇置换与奇置换之积为偶置换；奇置换与偶置换之积为奇置换.

6. (1). 对任置换 α, 平方 α^2 是偶置换.

(2). 奇阶的置换必为偶置换.

7. 设 G 是一个 n 次置换群，即 $G \le S_n$. 证明：如果 G 有奇置换，则奇置换的个数与偶置换的个数相等.

8. 证明：S_n, $n \ge 2$, 由 $n-1$ 个元素 $\beta_1 = (1\,2)$, $\beta_2 = (2\,3)$, $\cdots$, $\beta_{n-1} = (n-1,\ n)$ 生成，满足下述关系：

$$\begin{aligned}
&\beta_i^2 = 1\,, && i = 1, \cdots, n-1\,;\\
&(\beta_i\beta_{i+1})^3 = 1\,, && i = 1, \cdots, n-2\,;\\
&\beta_i\beta_j = \beta_j\beta_i\,, && 1 \le i, j < n\ ,\ \ |i-j| > 1\ .
\end{aligned}$$

9. 由 $x_1,\ x_2,\ \cdots,\ x_{n-1}$ 按下列关系生成的群同构于 S_n:

$$\begin{aligned} &x_i^2 = 1\,, && i = 1, \cdots, n-1\,;\\ &(x_i x_{i+1})^3 = 1\,, && i = 1, \cdots, n-2\,;\\ &x_i x_j = \beta_j \beta_i\,, && 1 \le i, j < n\ ,\ \ |i-j| > 1\ . \end{aligned}$$

(**提示**: 仿照定理 1.5.13 的证明, 但 (C) 中取下述陪集:
$H\,,\ x_{n-1}H\,,\ x_{n-2}x_{n-1}H\,,\ x_{n-3}x_{n-2}x_{n-1}H\,,\ \cdots\,,\ x_2\cdots x_{n-2}x_{n-1}H\,,\ x_1x_2\cdots x_{n-2}x_{n-1}H$.)

10. 证明: S_n 可以由 2 个元素生成.

(**提示**: (12), $(23\cdots n)$ 可生成.)

11. 证明: A_n, $n \ge 3$, 可以由子集 $\{(1\,2\,3),\ (1\,2\,4),\ \cdots,\ (1\,2\,n)\}$ 生成.

(**提示**: $(1i)(12) = (12i)$, $(12)(1j) = (12j)^2$, $(1i)(1j) = (1i)(12)(12)(1j) = (12i)(12j)^2$.)

12. 如果 G 是交换单群, 则 G 是素数阶循环群.

§2.6 群在集合上的作用

内容提要: 概念和例子; 可迁作用和左平移作用; 轨道长; 轨道计数; 本原可迁性.

2.6.1 定义. 设 A 是集合, G 是群. 如果有一个映射

$$G \times A \longrightarrow A, \quad (g, a) \longmapsto ga, \qquad (\text{为简便, 记 } (g,a) \text{ 的像为 } ga)$$

满足两条:

(A1). $1_G a = a,\ \forall\ a \in A$;

(A2). $(gg')a = g(g'a),\ \forall\ g, g' \in G\ \forall\ a \in A$;

就说群 G *(左)* 作用 在集合 A 上, 也称 A 为 G- 集.

注. 类似定义方式在线性代数中已出现过. 例如域 $\mathbb{C}$ 上的抽象向量空间 V 定义为一个加群 V 和一个映射 (称为纯量积) $\mathbb{C} \times V \to V$, $(c, v) \mapsto cv$, 满足四个条件:

$$c(v+v') = cv + cv'; \qquad (c+c')v = cv + c'v; \qquad (cc')v = c(c'v); \qquad 1v = v.$$

2.6.2 命题. 设 A 是集合, G 是群. 以下两条等价:

(i). 群 G 作用在集合 A 上: $G \times A \longrightarrow A$, $(g, a) \mapsto ga$;

(ii). 有一个群同态 $\sigma : G \to \mathrm{Sym}(A)$.

证. (i) $\Rightarrow$ (ii). 从映射 $G \times A \to A$, $(g, a) \mapsto ga$, 任 $g \in G$ 对应 A 的一个变换 $\sigma(g) : A \to A$, $a \mapsto ga$; 即 $\sigma(g)(a) = ga$. 由条件 (A1) 知单位元 1_G 对应恒等变换 $\sigma(1_G) = \mathrm{id}_A$. 再由 (A2) 得:

$$\sigma(gg')(a) = (gg')a = g(g'a) = \sigma(g)(\sigma(g')(a)) = (\sigma(g)\sigma(g'))(a)\ ;$$

即 $\sigma(gg') = \sigma(g)\sigma(g')$, $\forall\ g, g' \in G$. 特别是, $\sigma(g)\sigma(g^{-1}) = \sigma(gg^{-1}) = \sigma(1_G) = \mathrm{id}_A$; 同样有, $\sigma(g^{-1})\sigma(g) = \mathrm{id}_A$; 所以 $\sigma(g) \in \mathrm{Sym}(A)$ 是可逆变换. 这样就得到一个映射 $\sigma : G \longrightarrow \mathrm{Sym}(A)$,

$g \mapsto \sigma(g)$; 而且这个映射满足： $\sigma(gg') = \sigma(g)\sigma(g')$, $\forall\ g, g' \in G$; 即，这个映射是群同态. 得到 (ii).

(ii) $\Rightarrow$ (i). 设 $\sigma : G \to \mathrm{Sym}(A)$, $g \mapsto \sigma(g)$, 是群同态. 作映射 $G \times A \longrightarrow A$, $(g, a) \mapsto \sigma(g)(a)$, 即令 $ga = \sigma(g)(a)$. 那么

$$(gg')a = \sigma(gg')(a) = (\sigma(g)\sigma(g'))a = \sigma(g)(\sigma(g')(a)) = g(g'a)\ ;$$

即 (A2) 成立. 而 $\sigma(1_G) = \mathrm{id}_A$, (A1) 显然成立. 得 (i). □

注. (1). 以上证明同时指明了群作用的两种表达形式互相转化的具体方式.

(2). 从群 G 到集合 A 的对称群 $\mathrm{Sym}(A)$ 的一个群同态 $\sigma : G \to \mathrm{Sym}(A)$, 称为群 G 在集合 A 上的一个 *变换表示*, 在 A 是有限集时也称为 *置换表示*. 群同态的核 $\mathrm{Ker}(\sigma)$ 称为该变换表示的 *核*. 如果 $\mathrm{Ker}(\sigma) = 1$ 则称该变换表示是 *忠实的 (faithful)*.

(3). 由命题，群 G 在集合 A 上的一个作用就是群 G 在集合 A 上的一个变换表示 $\sigma : G \to \mathrm{Sym}(A)$, 变换表示的核 $\mathrm{Ker}(\sigma)$ 也称为该作用的 *核*, 如果变换表示 σ 是忠实的则也称该作用是 *忠实的 (faithful)*.

例. 如果 $G \leq \mathrm{Sym}(A)$, 即 G 是集合 A 的变换群 (置换群，若 A 是有限集) ，则包含同态 $G \to \mathrm{Sym}(A)$ 给出 G 在 A 的作用，这时 G 的元就是 A 的双射变换 (A 的置换若 A 是有限集). 所以，群作用是变换群 (置换群) 的推广；而忠实作用就可等同于变换群 (置换群) 的作用.

因此，关于群作用的结论对变换群 (置换群) 都成立. 反过来，对变换群 (置换群) 成立的结论，用到群作用时则需要根据作用的核的情况作适当修正.

例. 设 G 是群. 那么群 G 以下述方式忠实作用在集合 G 上：

$$G \times G \ \longrightarrow\ G\ ,\quad (g, a)\ \longmapsto\ ga\ ;$$

这里 $G \times G$ 的后一 G 以及箭头右边的 G 都只是作为集合，最后的 ga 则是群中的运算. 这个作用称为群 G 在 G 上的左平移作用. 它对应的变换表示记作 $\lambda : G \to \mathrm{Sym}(G)$, $g \mapsto \lambda_g$, (即 λ_g 是集合 G 的变换 $\lambda_g : G \to G$, $a \mapsto ga$), 称为群 G 的 (左) 凯莱表示 ((left) Cayley representation).

证. 显然 $1a = a$, $\forall\ a \in G$. 对 $g, g' \in G$ 和 $a \in A$, 群 G 的运算满足结合律，即 $(gg')a = a(g'a)$. 按定义 $(g, a) \mapsto ga$ 是群 G 在集合 G 上的作用. 又，如果 $g \in G$ 使得 $ga = a$, $\forall\ a \in G$, 取 $a = 1$ 就得 $g = 1$. 所以这个作用的核 $= 1$. 即这是忠实作用. □

例. 对任 $g \in G$ 令 $\sigma(g) = \mathrm{id}_A$, 即作用的核是 G, 则这个作用称为 *平凡作用*.

2.6.3 定义. (1). 设群 G 作用在集合 A 上. 如果 A 的子集 $B \subseteq A$ 满足

$$gb \in B\ ,\qquad \forall\ b \in B\ ,\ g \in G\ ,$$

就称 B 是 A 的 G- *稳定子集*, 也称 G- 不变子集.

(2). 对 G- 稳定子集 B, 按照定义，从群 G 在 A 上的作用可以得出 G 在集合 B 上的作用：

$$G \times B \longrightarrow B\ , \quad (g,b) \longmapsto gb\ .$$

称为群 G 在稳定子集 B 上的 限制作用.

2.6.4 例. 设群 G 作用在集合 A 上. 令 $\mathcal{P}(A) = \{\, B \mid B \text{ 是 } A \text{ 的子集} \,\}$ 是 A 的 幂集. 那么对任 $g \in G$, $B \in \mathcal{P}(A)$, 有 $gB := \{\, gb \mid b \in B \,\} \in \mathcal{P}(A)$. 以这种方式，群 G 作用在集合 $\mathcal{P}(A)$ 上：

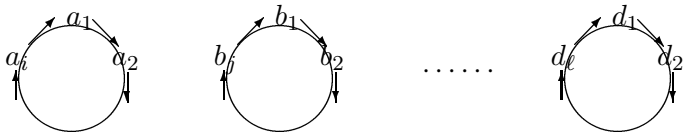
$$G \times \mathcal{P}(A) \longrightarrow \mathcal{P}(A)\ , \quad (g,B) \longmapsto gB\ ;$$

把 A 的基数为 k 的子集称为 k- 子集. 以 $\mathcal{P}_k(A)$ 表示 A 的所有 k- 子集的集合. 显然，$g \in G$ 把 k- 子集变为 k- 子集, 所以 $\mathcal{P}_k(A)$ 是 G- 稳定子集. 所以群 G 可以限制作用在 $\mathcal{P}_k(A)$ 上. 特别的， G 在 $\mathcal{P}_1(A)$ 上的作用就是 G 在 A 上的作用.

回顾置换的轮换分解：设 n 次置换

$$\alpha = (a_1 a_2 \cdots a_i)(b_1 b_2 \cdots b_j) \cdots (d_1 d_2 \cdots d_\ell)\ . \tag{CD}$$

从群作用的角度来看，α 生成的子群 $\langle \alpha \rangle$ 可以把文字 a_1 变成任一 a_t; 但不能变为任一 b_t , 不能变为任一 d_t 等等.



这种直观图形可以作为下述概念的原始模型.

2.6.5 定义. 设群 G 作用在集合 A 上.

(1). 在 A 上定义关系：对任 $a, a' \in A$, 如果存在 $g \in G$ 使得 $ga = a'$, 就称 a 被 G- 迁移到 a', 记作 $a \sim_G a'$.

易验证则 G- 迁移关系 "$\sim_G$" 是 A 上的等价关系： 自反性显然成立；若 $ga = a'$, 则 $g^{-1}a' = a$, 此即对称性；若 $g_1 a = a'$, $g_2 a' = a''$, 则 $g_2 g_1(a) = a''$; 传递性成立.

(2). 称 G- 集 A 中关于 G- 迁移关系 "$\sim_G$" 的等价类为 G- 轨道 , 简称 轨道. 点 $a \in A$ 所在的轨道 (即 a 所在的等价类) 记作如果 A 的 G- 轨道只有一个，就说 G 在 A 上的作用是 可迁的.

注. (1). G 在集合 A 上可迁作用就是对任 $a, a' \in A$ 存在 $g \in G$ 使得 $ga = a'$.

(2). 如果 G 在集合 A 的作用不可迁，则 A 划分为各轨道 A_i 的不交并. 按可迁关系 $\sim_G$ 的定义，对任 $a_i \in A_i$ 有 $A_i = \{\, ga_i \mid g \in G \,\} =: Ga_i$.

(3). 对每个轨道 A_i, 对任 $a_i \in A_i$ 和 $g \in G$ 有： $ga_i \sim_G a_i$, 所以 $ga_i \in A_i$. 所以轨道 A_i 是 G- 稳定子集. 那么 G 可以限制作用在 A_i 上： $G \times A_i$, $(g, a_i) \mapsto ga_i$. 而且 G 作用在轨道 A_i 上是可迁的：因为对任 $a_i, a_i' \in A_i$, 按等价类定义， $a_i \sim_G a_i'$, 有 $g \in G$ 使得 $ga_i = a_i'$.

(4). 当 A 是有限集时，设 $A_1, \cdots, A_m$ 是所有轨道，它们就构成集合 A 的一个划分，即有不交并 $A = \bigcup_{i=1}^{m} A_i$. 那么轨道的长度 $|A_i|$（即轨道 A_i 中元素个数）就满足

$$|A| \;=\; \sum_{i=1}^{m} |A_i| \,. \tag{OL}$$

称为 *轨道长方程*. 这样一个看起来简单的公式，有时很有用. 将有计算公式计算每轨道的长度 $|A_i|$.

例. 上面 (CD) 中 α 生成的子群 $\langle\alpha\rangle$ 的轨道就是

$$\Omega_1 = \{a_1, a_1, \cdots, a_i\}, \quad \Omega_2 = \{b_1, b_2, \cdots, b_j\}, \quad \cdots, \quad \Omega_\ell = \{d_1, d_2, \cdots, d_\ell\}.$$

2.6.6 例. 设 H 是群 G 的子群，令 $\mathcal{L} = G/H = \{\, sH \mid s \in G \,\}$ 是左陪集的集合. 那么 $G \times \mathcal{L} \longrightarrow \mathcal{L}$, $(g, sH) \longmapsto gsH$, 是 G 在 $\mathcal{L}$ 上的可迁作用，称为群 G 在子群 H 的左陪集集合 G/H 上的 *左平移作用*.

证. $1(sH) = sH$. $(g_1g_2)(sH) = g_1(g_2(sH))$. 即 G 作用在 $\mathcal{L}$ 上.
对任 $sH, s'H \in \mathcal{L}$, $(s's^{-1})(sH) = s'H$. 即 G 作用是可迁的，见上注解 (1). □

以下看每个轨道的形态.

首先，如果群 G 作用在两个集合 A, A' 上，如何比较这两个作用？什么情况下能说这两个作用实质上相同？

定义. 设 G 是群， A, A' 是两个集合，设有两个同态 $\sigma : G \to \mathrm{Sym}(A)$, 和 $\sigma' : G \to \mathrm{Sym}(A')$. 如果存在双射 $f : A \to A'$ 使得

$$f\,\sigma(g)(a) = \sigma'(g) f(a) \,, \qquad \forall\ a \in A \quad g \in G \,,$$

我们就说 G 在 A 的作用 σ 与 G 在 A' 的作用 σ' 等价. 按 G- 作用的另一记法，就是

$$f(ga) = g(f(a)) \,, \qquad \forall\ a \in A \quad g \in G \,.$$

图示如下

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & A' \\ {\scriptstyle \sigma(g)}\downarrow & & \downarrow{\scriptstyle \sigma'(g)} \\ A & \xrightarrow[\ f\ ]{} & A' \end{array} \qquad \forall\ g \in G \,.$$

2.6.7 定理. *设群 G 可迁地作用在集合 A 上， $a_0 \in A$. 记 $G_{a_0} = \{\, g \in G \mid ga_0 = a_0 \,\}$. 则 $G_{a_0} \le G$; 而 G 在 G_{a_0} 的左陪集集合 G/G_{a_0} 上的左平移作用与 G 在集合 A 上的作用等价. 特别有， $|A| = |G : G_{a_0}|$.*

注. G_{a_0} 称为 a_0 的 *稳定子群*.

证. 显然 $1_G \in G_{a_0}$. 设 $g, h \in G_{a_0}$ ；则 $ha_0 = a_0$ 从而 $h^{-1}a_0 = a_0$ ，那么 $h^{-1}ga_0 = a_0$; 得 $h^{-1}g \in G_{a_0}$. 于是 G_{a_0} 是子群.

对左陪集 $sG_{a_0} \in G/G_{a_0}$ ，令 $f(sG_{x_0}) = sa_0 \in A$ 与之对应；若 $s' \in sG_{a_0}$, 则有 $t \in G_{a_0}$ 使得 $s' = st$, 那么 $s'a_0 = sta_0 = s(ta_0) = sa_0$. 这样从子群 G_{a_0} 的左陪集的集合 G/G_{a_0} 到 A 我们就作出了一个合理定义的映射

$$f : G/G_{a_0} \longrightarrow A\,, \quad sG_{a_0} \longmapsto sa_0\ .$$

这显然是满射. 如果 $sG_{a_0} \in G/G_{a_0}$ 与 $s'G_{a_0} \in G/G_{a_0}$ 使得 $f(sG_{a_0}) = f(s'G_{a_0})$, 就是 $sa_0 = s'a_0$, 则 $s^{-1}s'a_0 = a_0$, 从而 $s^{-1}s' \in G_{a_0}$, 也就是 $sG_{a_0} = s'G_{a_0}$ 是同一陪集. 故上述映射 f 是单射. 因此 f 是双射.

最后，对 $g \in G$, $sG_{a_0} \in G/G_{a_0}$, 有

$$f(g(sG_{a_0})) = f(gsG_{a_0}) = gsa_0 = g(sa_0) = g(f(sG_{a_0}))\ ;$$

所以 f 是 G- 集 G/G_{x_0} 到 G- 集 A 的等价. □

推论. *设群 G 作用在集合 A 上，设 A_i 是一个 G- 轨道， $a_i \in A_i$. 则*

(1). $A_i = Ga_i := \{\, ga_i \mid g \in G \,\}$;

(2). (轨道长公式). $|A_i| = |G : G_{a_i}|$. □

2.6.8 例. (1). 设 G 是群. 则群 G 以下述方式作用于集合 G:

$$G \times G \longrightarrow G, \quad (g, a) \longmapsto gag^{-1}\ ;$$

称为 G 在 G 上的 *共轭作用*. G- 共轭作用的轨道称为 G 的元素的 *共轭类*. 元素 $a \in G$ 在共轭作用下的稳定子群记作 $C_G(a) = \{\, g \in G \mid gag^{-1} = a \,\}$, 称为 a 在 G 中的 *中心化子*. a 所在的共轭类长度 $=|G : C_G(a)|$. 特别的， a 所在共轭类长度 1 当且仅当 $a \in Z(G)$(群的中心).

群 G 划分为共轭类的不交并集，长度 1 的共轭类就是中心元；记 $Z = Z(G)$ 是 G 的中心，令 C_1, C_2, $\cdots$, C_ℓ 为 G 的全部长度大于 1 的共轭类，则轨道长方程 (OL) 用在这里就是

$$|G| = |Z| + |C_1| + \cdots + |C_\ell|\ . \tag{CE}$$

称为群 G 的 *类方程*.

S_3 划分为 3 个共轭类：$\{(1)\}$, $\{(123),\ (132)\}$, $\{(12,\ (23),\ (13))\}$. 类方程就是 $6 = 1{+}2{+}3$.

(2). 令 $\mathcal{H} = \{\, H \mid H \leq G \,\}$ 为 G 的所有子群的集合, 则 G 也以共轭方式作用在 $\mathcal{H}$ 上, 这是因为，如果 $H \leq G$, 则 $gHg^{-1} \leq G$ 也是子群，称为 H 的 *共轭子群*. 子群 H 在共轭作用下的稳定子群记作 $N_G(H) = \{\, t \in G \mid tHt^{-1} = h \,\}$, 也称为 H 在 G 中的 *正规化子*. H 的共轭子群个数等于 $|G : N_G(H)|$. 那么 H 是正规子群当且仅当 $N_G(H) = G$, 当且仅当 H 的共轭子群只有 H 自己.

关于群作用时轨道的个数计数则有：

2.6.9Burnside 轨道计数公式. *设有限群 G 作用在有限集 A 上. 对 $g \in G$ 令 $A^g := \{\, a \in A \mid ga = a \,\}$ (称为 g 在 A 上的 不动点集). 则 A 的 G- 轨道的个数 m 为*

$$m \ = \ \frac{1}{|G|} \sum_{g \in G} |A^g|\ .$$

证. 考虑集合 $\mathcal{S} = \{\,(g,a) \mid g \in G,\ a \in A,\ ga = a\,\}$ 的计数. 有两种途径来计算 $|\mathcal{S}|$. 一方面，对任一个固定的 $g \in G$ ，按照 A^g 的定义这种偶对 (g,a) 的个数是 $|A^g|$ ；所以

$$|\mathcal{S}| = \sum_{g\in G} |A^g| \,. \tag{$*$}$$

另一方面，对任一个固定的 $a \in A$ ，按照 G_a 的定义这种偶对 (g,a) 的个数是 $|G_a|$; 所以

$$|\mathcal{S}| = \sum_{a\in A} |G_a| \,.$$

将 A 划分为轨道的不交并 $A = A_1 \cup A_2 \cup \cdots \cup A_m$. 对同一轨道的 $a_i \in A_i$ 根据轨道长公式 $|G_{a_i}| = |G|/|A_i|$. 因而

$$|\mathcal{S}| = \sum_{i=1}^{m}\sum_{a\in A_i} |G|/|A_i| = |G|\sum_{i=1}^{m}\sum_{a\in A_i} 1/|A_i| = |G|\sum_{i=1}^{m} |A_i|/|A_i| = |G|\cdot m$$

把此式与式 $(*)$ 相比较，就得到所要求证的公式. □

注. 容易看出 $|A^g|$ 就是 g 对应的置换 $\sigma(g) \in \mathrm{Sym}(A)$ 的型 (其中 $n = |A|$)

$$(\lambda_1(\sigma(g)),\ \lambda_2(\sigma(g)),\ \cdots,\ \lambda_n(\sigma(g)))$$

中的第一个型函数 $\lambda_1(\sigma(g))$ 值；参看定义 2.5.3.

下面介绍可迁作用的本原性.

前面已谈到：如果群 G 作用在集合 A 上，那么群 G 作用在幂集 $\mathcal{P}(A)$ 上. 而 A 的划分 $\mathcal{T}$ 是幂集 $\mathcal{P}(A)$ 的满足一定条件的子集，任 $g \in G$ 把 $\mathcal{T}$ 变为 $g\mathcal{T} := \{\,gT \mid T \in \mathcal{T}\,\} \subseteq \mathcal{P}(A)$; 其中 $gT = \{\,gt \mid t \in T\,\} \subseteq A$.

引理. *设群 G 作用在集合 A 上. 则对 A 的任划分 $\mathcal{T}$ 和任 $g \in G$, 有： $g\mathcal{T}$ 也是 A 的一个划分.*

证. 对任 $T \in \mathcal{T}$, $T \neq \emptyset$, 所以 $gT = \{gt \mid t \in T\} \neq \emptyset$. 任 $a \in A$ 有 $a' \in A$ 使得 $a = ga'$; 对 a' 存在 $T \in \mathcal{T}$ 使得 $a' \in T$; 那么 $a = ga' \in gT$. 最后，设 $T, T' \in \mathcal{T}$, 如果 $gT \cap gT' \neq \emptyset$, 有 $a \in gT \cap gT'$, 故有 $t \in T$, $t' \in T'$ 使得 $gt = a = gt'$; 那么 $t = g^{-1}(gt) = g^{-1}(gt') = t'$; 所以 $T \cap T' \neq \emptyset$; 而 $\mathcal{T}$ 是划分，故 $T = T'$. 从而 $gT = gT'$. □

定义. 设群 G 作用在集合 A 上. 称 A 的划分 $\mathcal{T}$ 是 G- **稳定** 的划分如果 $g\mathcal{T} = \mathcal{T}, \forall\, g \in G$.

2.6.10 引理. *设群 G 作用在集合 A 上，设 $\mathcal{T}$ 是 A 的 G- 稳定的划分. 那么：*

(1). *G 作用在 $\mathcal{T}$ 上： $G \times \mathcal{T} \longrightarrow \mathcal{T}$, $(g,\ T) \longmapsto gT$.*

(2). *对 $a \in A$, 如果 $T \in \mathcal{T}$ 使 $a \in T$, 则 $G_a \subseteq G_T$, 其中 $G_a = \{\,g \in G \mid ga = a\}$ 是 a 在 G 中的稳定子群，而 $G_T = \{\,g \in G \mid gT = T\}$ 是 T 在 G 中的稳定子群.*

(3). *如果 G 在 A 上的作用是可迁的, 那么 G 在 $\mathcal{T}$ 上的作用是可迁的, 且对任 $T, T' \in \mathcal{T}$ 有 $|T| = |T'|$.*

证. 作为习题 9. □

显然，离散划分 $\mathfrak{T}_0 = \{\,\{a\} \mid a \in A\,\}$, 和全集划分 $\mathfrak{T}_1 = \{A\}$, 都是 G- 稳定的. 这两个划分称为平凡划分.

2.6.11 定义. 设 G 可迁地作用在集合 A 上, $|A| > 1$. 如果除了两个平凡划分以外没有 G- 稳定的划分，就称 G 本原地 可迁作用在集合 A 上.

注意：群 G 的子群 H 称为 极大子群 如果 $H \neq G$ 且只要 $H \leq K \leq G$ 就或者 $K = H$ 或者 $K = G$.

2.6.12 定理. *设 G 可迁地作用在集合 A 上, $a \in A$. 那么 G 是本原可迁的当且仅当 a 的稳定子群 G_a 是 G 的极大子群.*

证. 充分性. 设 G_a 是极大子群. 设 $\mathfrak{T}$ 是 G- 稳定的划分. 存在 $T \in \mathfrak{T}$ 使得 $a \in T$. 如果 $T = A$ 则 $\mathfrak{T}$ 是全集划分. 下设 $T \neq A$. 那么划分 $\mathfrak{T}$ 至少含两个 A 的子集，即 $|\mathfrak{T}| > 1$. 由于 G 稳定 $\mathfrak{T}$, 由引理 2.6.10, G 可迁作用在 $\mathfrak{T}$ 上，且 $G_a \leq G_T \leq G$. 由轨道长公式 (定理 2.6.7 的推论), $|G : G_T| = |\mathfrak{T}| > 1$, 故 $G_T \neq G$. 但 G_a 是极大子群，所以 $G_T = G_a$. 若存在 $b \in T - \{a\}$, 由可迁性，存在 $g \in G$ 使 $ga = b$; 那么 $b \in T \cap gT$, $T \cap gT \neq \emptyset$, 所以 $gT = T$, $g \in G_T = G_a$, 于是 $b = ga = a$, 这与 $b \in T - \{a\}$ 相矛盾. 所以 $T = \{a\}$; 因为每个 $T' \in \mathfrak{T}$ 满足 $|T'| = |T| = 1$, 所以 $\mathfrak{T}$ 是离散划分.

必要性. 设 A 只有平凡划分是 G- 稳定的划分. 设 $G_a \subseteq H \leq G$, 我们证明 $H = G$ 或 $= G_a$. 注意

$$G/G_a \longrightarrow A\,, \quad gG_a \longmapsto ga\,, \tag{†}$$

是双射；令 $T = \{\,ha \mid h \in H\,\} \subseteq A$, 则

$$H/G_a \longrightarrow T\,, \quad hG_a \longmapsto ha\,, \tag{‡}$$

是双射. 对 H 的任一左陪集 gH, 它可划分为 G_a 的左陪集：

$$gH/G_a := \{\,ghG_a \mid hG_a \in H/G_a\,\}\,, \qquad ghG_a = gh'G_a \iff hG_a = h'G_a\,;$$

那么有双射：

$$gH/G_a \longrightarrow gT\,, \quad ghG_a \longmapsto gha\,.$$

所以

$$\mathfrak{T} = \{\,gT \mid g \text{ 跑遍 } G/H \text{ 的一个代表系}\,\}$$

构成 A 的一个划分且为 G- 稳定的划分.

那么 $\mathfrak{T}$ 或者是离散划分或者是全集划分. 如果 $\mathfrak{T}$ 是离散划分, 则 $T = \{a\}$, 从双射 (‡) 得 $H = G_a$. 否则 $\mathfrak{T}$ 是全集划分，则 $T = A$, 从双射 (†) 和 (‡) 得 $H/G_a = G/G_a$, 即 $H = G$. 总之 G_a 是极大子群. □

习题 2.6

1. 设 G 是群, A 是集合. 如果映射 $\tau : G \to \mathrm{Tran}(A)$ 满足：

(a1). $\tau(gg') = \tau(g)\tau(g')$, $\forall\ g, g' \in G$;

(a2). $\tau(1_G) = \mathrm{id}_A$;

则 τ 是群 G 在集合 A 上的一个作用.

2. (1) 设 $\alpha \in S_n$ 为 n- 循环, 则 $\langle\alpha\rangle$ 在 $\{1, 2, \cdots, n\}$ 上可迁. 特别是, S_n 在 $\{1, 2, \cdots, n\}$ 上是可迁作用.

(2) $n > 2$ 时 A_n 在 $\{1, 2, \cdots, n\}$ 上是可迁作用.

3. (1). 设 $\rho_\theta \in E(\mathbb{R}^2)$, $\theta \neq 2k\pi$, 为欧氏平面 $\mathbb{R}^2$ 的一个非平凡旋转, 则 $\langle\rho_\theta\rangle$ 在 $\mathbb{R}^2$ 上的一个轨道在一个圆圈上.

(2). 设 $\alpha_{0,u} \in E(\mathbb{R}^2)$, $u \neq 0$, 为欧氏平面 $\mathbb{R}^2$ 的一个非平凡平移, 则 $\langle\alpha_{0,u}\rangle$ 在 $\mathbb{R}^2$ 上的一个轨道在一条以 u 为方向向量的直线上.

4. 设群 G 可迁地作用在集合 A 上. 问: G 在 A 的幂集 $\mathcal{P}(A)$ 上的作用是否也可迁?

5. 设群 G 既作用在集合 A 上也作用在集合 B 上. 对任意 $g \in G$ 和任意 $(a, b) \in A \times B$, 令 $g(a, b) = (ga,\ gb)$. 证明: 群 G 作用在集合 $A \times B$ 上. 如果 G 在集合 A 和集合 B 上的作用都是可迁的, 群 G 在 $A \times B$ 上的作用可迁吗? 考虑 $A = B$ 的情况.

6. 设群 G 作用在集合 A 上, 对 $a \in A$, 记 G_a 是 a 的稳定子群. 设 $g \in G$. 证明: $gG_ag^{-1} = G_{ga}$.

7. 设 G 为有限群, 取集合 $A = G$, 令 $H \leq G$. 证明:

(1). H 以下述方式作用于 A: 对 $h \in H$ 和 $a \in A\ (= G)$, $h(a) = ha$;

(2). 对 $a \in A$, a 所在的 H- 轨道正好是 H 的右陪集 Ha;

(3). 用轨道长公式证明 $|Ha| = |H|$.

8. 设 G 为有限群, $H \lneqq G$. 证明 $\bigcup_{g\in G} gHg^{-1} \neq G$. 本结论对无限群对吗?

9. 证明引理 2.6.10.

§2.7 Sylow 定理

内容提要: p- 子群计数; *Sylow* 定理.

始终设 p 是一个素数. 设有限群 G 作用在有限集 A 上.

一个简单但有用的事实是: A 的轨道分为两类: 一类是长度被 p 整除的轨道, 一类是长度与 p 互素的轨道; 设 A' 是后一类轨道的并集; 那么

2.7.1
$$|A'| \equiv |A| \pmod{p}\ .$$

记 $A^G = \{\, a \in A \mid ga = a\ ,\ \forall\ g \in G\,\}$, 称为 A 中 G 的不动点集合. 那么 A^G 就是 A 中的独点轨道 (长度 1 的轨道) 的并集.

定义. 有限群 P 称为 p- 群如果 $|P| = p^n$ 是 p 之幂.

由 Lagrange 定理, p- 群的任何子群是 p- 群, p- 群的任何子群的指数是 p 之幂.

2.7.2 引理. 设 p- 群 P 作用于有限集 A. 则

$$|A^P| \equiv |A| \pmod{p} .$$

证. 由定理 2.6.7, A 的轨道 A_i 长 $|A_i| = |P : P_{a_i}|$, 其中 $a_i \in A_i$, 但 $p \nmid |P : P_{a_i}|$ 当且仅当 $|P : P_{a_i}| = 1$ 当且仅当 $a_i \in A^P$. 由 2.7.1, 得本引理. □

2.7.3 推论. 非平凡 p- 群有非平凡中心.

证. 考虑 p- 群 P 在集合 P 上的共轭作用, 则中心

$$Z(P) = \{ z \in P \mid uz = zu, \ \forall\, u \in P \} \{ z \in P \mid uzu^{-1} = z, \ \forall\, u \in P \} = P^P .$$

故

$$|Z(P)| = |P^P| \equiv |P| \equiv 0 \pmod{p} .$$

但 $|Z(P)| \geq 1$, 所以 $|Z(P)| > 1$. □

2.7.4 Sylow 定理 I. 设有限群 G 的阶 $|G| = mp^n$, $p \nmid m$. 如果 $0 \leq k \leq n$, 则 G 中存在子群 Q 使得 $|Q| = p^k$, 且 G 的这种 p- 子群的个数 $\equiv 1 \pmod{p}$.

证. 设 $\mathcal{A} = \{ A \subset G \mid |A| = p^k \}$. 让 G 左平移地作用在 $\mathcal{A}$ 上:

$$G \times \mathcal{A} \longrightarrow \mathcal{A}, \quad (g, \ A) \longmapsto gA = \{ ga \mid a \in A \} .$$

把 $\mathcal{A}$ 的任 G- 轨道 Ω 长写为 $|\Omega| = ap^b$ 其中 $p \nmid a$; 那么 $\mathcal{A}$ 的 G- 轨道 Ω 分为两种:

- 一种是使得 $b \leq n - k$ 的; 令 $\mathcal{A}'$ 是 $\mathcal{A}$ 中这种轨道之并集.
- 另一种使得 $b > n - k$ 的; 令 $\mathcal{A}''$ 是 $\mathcal{A}$ 中此种轨道之并集.

对任 G- 轨道 $\Omega'' \subseteq \mathcal{A}''$, 都有 $p^{n-k+1} \,\Big|\, |\Omega''|$; 所以 $p^{n-k+1} \,\Big|\, |\mathcal{A}''|$. 而 $|\mathcal{A}| = |\mathcal{A}'| + |\mathcal{A}''|$, 故有

$$|\mathcal{A}'| \equiv |\mathcal{A}| = \binom{p^n m}{p^k} \pmod{p^{n-k+1}} . \tag{S1}$$

再看 $\mathcal{A}'$ 中的 G- 轨道 Ω'. 设 $A' \in \Omega'$. 如果 $1 \notin A'$, 任取 $a \in A'$, 则 $a^{-1}A' \in \Omega'$, 而 $1 = a^{-1}a \in a^{-1}A'$. 所以总有 $A' \in \Omega'$ 使得 $1 \in A'$.

因此以下设 $A' \in \Omega'$ 使得 $1 \in A'$. 设 $Q = G_{A'} := \{ u \in G \mid uA' = A' \}$ 是 A' 在 G 中的稳定子群. 由轨道长公式, $|G : Q| = |\Omega'| = ap^b$, 其中 a 与 p 互素而 $b \leq n - k$; 但 $|G : Q| \cdot |Q| = |G| = p^n m$, 因此

$$p^k \,\Big|\, |Q| . \tag{S2}$$

按稳定子群的定义, 对任 $u \in Q$ 有 $uA' = A'$, 故 $u = u1 \in A'$; 得 $Q \subseteq A'$. 那么 $|Q| \leq |A'| = p^k$. 结合 (S2) 式, 得

$$|Q| = p^k = |A'| ;$$

从而 Q 是阶为 p^k 的子群, 且 $Q = A' \in \Omega'$. 按轨道的定义知

$$\Omega' = \{ gQ \mid g \in G \} ;$$

这正好是 p- 子群 Q 的所有左陪集的集合，特别 $|\Omega'| = |G : Q| = mp^{n-k}$.

反过来，如果 $Q \leq G$ 使得 $|Q| = p^k$, 那么 $Q \in \mathcal{A}$, 而且按 G- 作用轨道的定义， Q 的所有左陪集的集合 $\Omega' = \{\, gQ \mid g \in G \,\}$ 正好是一个轨道其长度 $|\Omega'| = |G : Q| = mp^{n-k}$, 从而 $\Omega' \subseteq \mathcal{A}'$.

总结上述， $\mathcal{A}'$ 正好就是所有阶为 p^k 的子群的所有左陪集为成员的集合，而且一个阶为 p^k 的子群的左陪集的集合恰好是 $\mathcal{A}'$ 中的一个 G- 轨道，其长度为 mp^{n-k}. 设 G 的阶为 p^k 的子群个数为 $r_k(G)$, 则得

$$|\mathcal{A}'| = r_k(G)\, mp^{n-k} \ .$$

结合 (S1), 得

$$r_k(G)\, mp^{n-k} \equiv \binom{p^n m}{p^k} \qquad (\mathrm{mod}\ p^{n-k+1}) \ .$$

因为 $p \nmid m$, 故 m 在 $\mathbb{Z}_{p^{n-k+1}}$ 中可逆，即有整数 ℓ 使得 $\ell m \equiv 1 \pmod{p^{n-k+1}}$. 所以

$$r_k(G)\, p^{n-k} \equiv \ell \binom{p^n m}{p^k} \qquad (\mathrm{mod}\ p^{n-k+1}) \ . \tag{$S3$}$$

把组合数写成如下形式

$$\begin{aligned} \binom{p^n m}{p^k} &= \frac{p^n m(p^n m - 1)(p^n m - 2) \cdots \Big(p^n m - (p^k - 1)\Big)}{1 \cdot 2 \cdots (p^k - 1) p^k} \\ &= \frac{p^{n-k} m}{1} \cdot \frac{p^n m - 1}{1}\, \frac{p^n m - 2}{2} \ \cdots\ \frac{p^n m - (p^k - 1)}{p^k - 1} \end{aligned}$$

这样便于分析这个整数的因子分解中 p 的幂次. 考虑 $p^n m - t$ 与 t, 因为 $t < p^k$, t 中的 p 的幂次 $< k$, 因此 t 中的 p 的幂次与 $p^n m - t$ 中的 p 的幂次相等. 由此断言 $\binom{p^n m}{p^k}$ 的因子分解中 p 的幂次等于 $n - k$; 那么 $p^{n-k} \,\Big|\, \binom{p^n m}{p^k}$. 从 (S3) 就得

$$r_k(G) \equiv \ell \binom{p^n m}{p^k} \Big/ p^{n-k} \qquad (\mathrm{mod}\ p) \ . \tag{$S4$}$$

此式对任意阶为 mp^n 的群成立. 那么对阶为 mp^n 的循环群 C 成立, 而循环群 C 的 $r_k(C) = 1$, 见定理 2.3.10; 所以

$$\ell \binom{p^n m}{p^k} \Big/ p^{n-k} \equiv r_k(C) = 1 \qquad (\mathrm{mod}\ p) \ .$$

那么从 (S4) 得：对任意为 $p^n m$ 的群 G 有

$$r_k(G) \equiv \ell \binom{p^n m}{p^k} \Big/ p^{n-k} \equiv 1 \qquad (\mathrm{mod}\ p) \ .$$

2.7.5 Sylow 定理. *设有限群 G 的阶 $|G| = p^n m$, $p \nmid m$.*

(1) G 中存在子群 P 使得 $|P| = p^n$, 这种子群称为 G 的 *Sylow* p- *子群*; 且 G 的 Sylow p- 子群的个数 $\equiv 1 \pmod{p}$.

(2) G 的任意两个 Sylow p- 子群在 G 中彼此共轭.

(3) G 的任一 p- 子群包含在至少一个 Sylow p- 子群之中.

证. (1) 是定理 2.7.4 的特别情形.

对 (2) 与 (3) 一起证明. 取 P 为 G 的 Sylow p- 子群. 设 Q 是 G 的一个 p- 子群. 令

$$\mathcal{P} = \{\, gPg^{-1} \mid g \in G \,\}$$

是 P 的共轭子群的集合. 注意, 在 G 的共轭作用之下, P 的稳定子群就是 P 的正规化子 $N_G(P)$; 则由轨道长公式得

$$|\mathcal{P}| = |G : N_G(P)| \ . \tag{S5}$$

因为 $P \subseteq N_G(P)$, 所以 $|P| \,\Big|\, |N_G(P)|$, 因而 $p \nmid |\mathcal{P}|$. 让 Q 共轭作用在集合 $\mathcal{P}$ 上, 记 $\mathcal{P}^Q$ 是 Q-不动成员的集合, 即

$$\mathcal{P}^Q = \{\, gPg^{-1} \in \mathcal{P} \mid ugPg^{-1}u^{-1} = gPg^{-1} \ , \ \forall\, u \in Q \,\} \ .$$

那么由引理 2.7.2,

$$|\mathcal{P}^Q| \equiv |\mathcal{P}| \ \not\equiv \ 0 \qquad (\mathrm{mod}\ p) \ .$$

因此存在 $P_1 = gPg^{-1} \in \mathcal{P}^Q$, 使得

$$uP_1u^{-1} = P_1 \ , \qquad \forall\, u \in Q \ ;$$

因而 $QP_1 = P_1Q$, 于是 QP_1 是子群, 该子群的阶

$$|QP_1| = \frac{|Q||P_1|}{|Q \cap P_1|} = |P_1| \cdot \frac{|Q|}{|Q \cap P_1|} \ .$$

由 Lagrange 定理, $|QP_1| \,\Big|\, p^n m$; 但是 $|P_1| = p^n$; 所以只能是

$$\frac{|Q|}{|Q \cap P_1|} = 1 \ ;$$

那么 $Q \cap P_1 = Q$, 即

$$Q \subset P_1 = gPg^{-1} \ .$$

也就是说, 对 G 的 p- 子群 Q 存在 $g \in G$ 使得 $Q \subseteq gPg^{-1}$. 把此结论用到 Sylow p- 子群 Q 上, 就得结论 (2). 把此结论用到任意 p- 子群上就得结论 (3). □

在定理证明过程中, (S5) 已证得下述结论:

推论. *设 G 同上 2.7.5, 设 P 是有限群 G 的一个 Sylow p- 子群. 则 G 的 Sylow p- 子群的个数 $r(G) = |G : N_G(P)|$, 从而 $r(G) \,|\, m$.* □

例. 如果 G 是一个阶为 10 的群, 即 $|G| = 10$, 那么 G 的 5-Sylow 子群正规, 且下列之一成立:

(1). $G \cong \mathbb{Z}_{10}$.

(2). $G \cong D_5$.

证. 令 r 是 Sylow 5- 子群的个数. 注意 $|G:P|=2$ 其中 P 是一个 Sylow 5- 子群, 由 2.7.5(1) 和 2.7.6, r 满足:

$$\begin{cases} r \equiv 1 \pmod 5 \ ; \\ r \mid 2 \ . \end{cases}$$

满足这两个条件的正整数只有 $r=1$. 所以 G 只有惟一一个 Sylow 5- 子群 P. 对任 $g \in G$, 因为 gPg^{-1} 也是 Sylow 5- 子群, 故 $gPg^{-1}=P$. 即 $P \trianglelefteq G$.

因为 $|P|=5$ 是素数, P 是循环群, 即 $P=\langle a\rangle$, $\mathrm{ord}(a)=5$. 取 $Q=\langle b\rangle$ 是一个 Sylow 2- 子群. 由于 P 是正规子群, $bPb^{-1}=P$; 从而 $bab^{-1}=a^n$. 那么

$$a=b^2ab^{-2}=b(bab^{-1})b^{-1}=ba^nb^{-1}=(bab^{-1})^n=(a^n)^n=a^{n^2} \ ;$$

所以

$$n^2 \equiv 1 \pmod 5 \ .$$

因此

$$n \equiv \pm 1 \pmod 5 \ .$$

如果 $n \equiv 1 \pmod 5$, 则 $bab^{-1}=a$, 即 $ba=ab$, 那么 $\mathrm{ord}(ab)=5\cdot 2=10$. 所以 $G=\langle ab\rangle$ 是 10 阶循环群, $G \cong \mathbb{Z}_{10}$.

如果 $n \equiv -1 \pmod 5$, 则 $bab^{-1}=a^{-1}$; 所以

$$G=\langle\, a,\ b \mid a^5=1,\ b^2=1,\ bab^{-1}=a^{-1}\,\rangle \cong D_5 \ . \qquad \square$$

习题 2.7

1. 利用引理 2.7.2 证明: 若 $p \,\Big|\, |G|$, 则 G 有 p 阶元.

(**提示**: 考虑集合 $\{\,(g_1,g_2,\cdots,g_p) \mid g_i \in G,\ \ g_1\cdots g_p=1\,\}$, p- 阶群 $\langle(12\cdots p)\rangle$ 按位置置换作用于该集合.)

2. 设 G 为有限群, p 为素数, $|G|=p^am$ 其中 $p \nmid m$; 设 $0 \le b \le k \le a$, 并设 $Q \trianglelefteq G$, $|Q|=p^b$. 证明: G 的包含 Q 的阶为 p^k 的子群的个数 $\equiv 1 \pmod p$.

3. 设 G 是一个 6 阶群. 证明: 或者 $G \cong \mathbb{Z}_6$ (6 阶循环群), 或者 $G \cong S_3$ (3 次对称群).

4. 设群 G 的阶 $|G| \le 20$, 则 G 不是单群.

5. 若群 P 的阶 $|P|=p^2$ 是一个素数的平方, 则 P 是交换群.