Lec15 Note of Abstract Algebra

Xuxuayame

日期：2023 年 5 月 5 日

我们回忆，要描述一个群有两种方式，一是如定义一样的集合与运算，这要求我们具体描述出任两个元素运算的结果，这自然很明确，但应用起来未必方便，例如将 G 作用到某个集合上，或打到另外一个群中，你就需要获知每个元素的像。

另一种方式是考虑它的表现，选取它的生成元，发掘它的生成关系，就可以唯一确定这个群。进一步，当我们要从这个群打到另外一个群，使其成为群同态时，我们只需要保证生成元的像也满足相应的生成关系即可。

例 4.5. $D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = (\sigma\tau)^2 = 1 \rangle$。

例 4.6. 考虑 S_n, $|S_n| = n!$，显然 $(12), (23), \cdots, ((n-1)n)$ 是它的一组生成元，我们依次记为 $x_1, x_2, \cdots, x_{n-1}$，那么显然有如下关系：

$$\begin{aligned} x_i^2 &= 1, \\ x_i x_j &= x_j x_i,\ \forall\, |i-j| \geq 2, \\ (x_i x_{i+1})^3 &= 1. \end{aligned}$$

这里第三条也可以替换为 $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$, $1 \leq i \leq n-2$，替换前后的生成关系是等价的。于是 S_n 具有表现：

$$S_n \simeq \left\langle x_1, \cdots, x_{n-1} \;\middle|\; \begin{aligned} & x_i^2 = 1,\ i = 1, \cdots, n-1, \\ & x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1},\ 1 \leq i \leq n-2, \\ & x_i x_j = x_j x_i,\ |i-j| \geq 2. \end{aligned} \right\rangle$$

现在我们证明右边的群确实与 S_n 同构。设右边的群为 G_n，则 $G_n = F\langle x_1, \cdots, x_{n-1} \rangle / \langle R \rangle_N$，且由于 $x_1, \cdots, x_{n-1}$ 都是平方元，我们可以归纳证明，G_n 中任一元素具有以下形式

$$G_n = G_{n-1} \cup x_{n-1} G_{n-1} \cup x_{n-2} x_{n-1} G_{n-1} \cup \cdots \cup x_1 \cdots x_{n-1} G_{n-1}.$$

这里要注意到 G_n 关于 G_{n-1} 的陪集分解的左陪集代表元系最多只有 $1, x_{n-1}, \cdots, x_1 \cdots x_{n-1}$ 这么多，进而恰好有这么多。从而 $|G_n| \leq n|G_{n-1}| \leq \cdots \leq n!$。

而 $G_n \twoheadrightarrow S_n$ 为满射，从而 $G_n \simeq S_n$。

上述处理方式也是处理有限情况的一般思路，对于无限群，思路也是类似的，虽然这个时候我们没法讨论元素的个数。我们可以这么处理：首先我们自然地有满射

$$F\langle S \rangle / \langle R \rangle \twoheadrightarrow G.$$

我们希望找 $W(S)$ 的一个子集 $I \subset W(S)$，使得 I 足够好，一方面存在到 $F\langle S\rangle/\langle R\rangle$ 的满射，另一方面存在到 G 的嵌入，并使得下面的图表交换：

$$\begin{tikzcd} I \arrow[r, two heads] \arrow[rr, bend right, hook] & F\langle S\rangle/\langle R\rangle \arrow[r, tail] & G \end{tikzcd}$$

例如在刚才的例子中，你可以找到 $W\langle x_1, \cdots, x_{n-1}\rangle$ 具有如下形式的一个子集：

$$\left\{ \begin{array}{r|r|c|r|c} 1 & 1 & & & \\ x_{n-1} & x_{n-2} & & 1 & 1 \\ x_{n-2}x_{n-1} & x_{n-3}x_{n-2} & \cdots & x_2 & x_1 \\ \cdots & \cdots & & x_1x_2 & \\ x_1\cdots x_{n-1} & x_1\cdots x_{n-2} & & & \end{array} \right\}$$

这里的符号含义是，字符串被分段，每一段被竖线隔开，并具有相应的选择。例如第一段具有 n 中选择，第二段是 $n-1$ 中选择等等。由于我们前面对 G_n 的归纳证明，从这个集合到 G_n 显然存在满射，而它同时也可以嵌入 S_n。

例 4.7.

$$Q_8 = \langle a, b \mid a^4 = 1,\ a^2 = b^2,\ ba = a^3b\rangle = F\langle a, b\rangle/\langle R\rangle_N.$$

比如 $\{a^ib^j \mid i = 0,1,2,3,\ j = 0,1\} \twoheadrightarrow Q_8$，我们另外构造一个群 G 如下

$$G = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle \le SL_2(\mathbb{C}).$$

这里将两个矩阵分别记为 A, B，那么显然有 $A^4 = I,\ A^2 = B^2,\ BA = A^3B$，于是存在 Q_8 到 G 的满同态，$a \mapsto A,\ b \mapsto B$。而 $|G| = 8$，于是同构。

例 4.8. 考虑 $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$，而 $SL_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \right\rangle$，记两个矩阵为 T, S，那么

$$\begin{aligned} PSL_2(\mathbb{Z}) &\simeq \langle S, T \mid S^2 = (ST)^3 = 1\rangle \\ &\simeq \langle S, X \mid S^2 = X^3 = 1\rangle. \end{aligned}$$

我们记后面的群为 G，那么显然存在满射：

$$I = \{S^aX^{i_1}SX^{i_2}\cdots SX^{i_m}S^b \mid a, b = 0, 1\ m \ge 0,\ i_1, \cdots, i_m = 1, 2\} \twoheadrightarrow G$$

而 G 到 $PSL_2(\mathbb{Z})$ 也有满射，将 $S \mapsto \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$，$X \mapsto \begin{pmatrix} & 1 \\ -1 & -1 \end{pmatrix}$，从而存在 I 到 $PSL_2(\mathbb{Z})$ 的满射，现在我们要说明有单射。你只需注意到 $SX = -\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$，$SX^2 = \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}$，所以你显然不可能得到 I。

例 4.9.

$$\langle x_1, x_2, \cdots, x_n \mid x_i x_j x_i^{-1} x_j^{-1} = 1 \rangle$$

为交换群，称为**自由 Abel 群**。

5 有限生成 Abel 群

定义 5.1. $a, b \in G$，$aba^{-1}b^{-1}$ 称为 a 与 b 的**换位子 (Commutator)**，记作 $[a, b]$。

G 中换位子全体生成的子群称为 G 的**换位子群 (Commutator subgroup)** 或**导子群 (Derived subgroup)**，记为 $[G, G]$ 或 G'，即 $\langle [a, b] \mid a, b \in G \rangle$。

于是显然有

$$ab = ba \Leftrightarrow [a, b] = 1.$$

例 5.1. G 为 Abel 群 $\Leftrightarrow G' = \{1\}$。

$G = S_n,\ n \geq 3$，则 $G' = A_n$。

命题 5.1. *(1)* $G' \triangleleft G$，且 G/G' 为 *Abel* 群。

(2) $\varphi\colon G \to A$ 为 G 到 *Abel* 群 A 的群同态，则 $\mathrm{Ker}\varphi \geq G'$，即有

$$\begin{tikzcd} G \arrow[r] \arrow[rrr, bend right, "\varphi"'] & G/G' \arrow[r, two heads] & G/\ker\varphi \arrow[r, hook] & A \end{tikzcd}$$

证明. 这里证明 (2)。

$\varphi([a, b]) = [\varphi(a), \varphi(b)] = 1 \Rightarrow [a, b] \in \mathrm{Ker}\varphi,\ \forall\, a, b \Rightarrow \mathrm{Ker}\varphi \geq G'$。 □

定义 5.2. S 集合，$\mathbb{Z}(S) = F(S)/F'(S) = \langle S \mid xyx^{-1}y^{-1},\ x, y \in S \rangle$ 称为**由 S 生成的自由 Abel 群**。

$F'(S) = \langle xyx^{-1}y^{-1},\ x, y \in S \rangle_N$ 的原因如下。令 $\langle xyx^{-1}y^{-1},\ x, y \in S \rangle_N = K$，则 $F(S)/K$ 为 Abel 群，那么 $K \geq F'(S)$，而 $K \leq F'(S)$，从而 $K = F'(S)$。