

5. 群论初步

xiaoga@mailustc.edu.cn

P113

12.

解:

K_4 的所有子群为:

$$\{e\}, \{e, a\}, \{e, b\}, \{e, c\}, \{e, a, b, c\}$$

15.

解:

$$\text{设 } \langle G, * \rangle = \langle a \rangle$$

$$G = \{e, a, a^2, a^3, a^4, a^5\}$$

G 的生成元为 a 或 a^5

$$\text{所有子群为 } \{e\}, \{e, a, a^2, a^3, a^4, a^5\}, \{e, a^2, a^4\}, \{e, a^3\}$$

18.

证明:

$$\text{设 } G = \langle a \rangle$$

存在性:

$$\text{设 } m = n/d,$$

由定理 5.10

a^m 的阶为 d

$$\therefore H = \{(a^m)^n \mid n \in \mathbb{Z}\} \text{ 为 } G \text{ 的 } d \text{ 阶子群。}$$

唯一性:

设除了 $\langle a^m \rangle$ 外, 还存在 G 的 d 阶子群,

则该子群为循环群, 设其为 $\langle a^{m'} \rangle$

$$\therefore n/(n, m') = d, \text{ 即 } (n, m') = n/d$$

$$m' = s \cdot \frac{n}{d}, (s, d) = 1$$

把 $\langle a^m \rangle$ 和 $\langle a^{m'} \rangle$ 展开

$$\langle a^m \rangle = \left\{ a^{1 \cdot \frac{n}{d}}, a^{2 \cdot \frac{n}{d}}, \dots, a^{d \cdot \frac{n}{d}} \right\}$$

$$\langle a^{m'} \rangle = \left\{ a^{1 \cdot \frac{n}{d}}, a^{2 \cdot \frac{n}{d}}, \dots, a^{d \cdot \frac{n}{d}} \right\}$$

$\{1, 2, \dots, d\}$ 为模 d 的完系, $(s, d) = 1$

$\therefore \{1s, 2s, \dots, ds\}$ 也为模 d 的完系

对于 $\langle a^m \rangle$ 和 $\langle a^{m'} \rangle$, 存在双射, 使对应的 $a^i \in \langle a^m \rangle$ 和 $a^j \in \langle a^{m'} \rangle$

$$\text{有 } \frac{i}{n/d} \equiv \frac{j}{n/d} \pmod{d}, \quad i \equiv j \pmod{n}$$

由于 n 为 a 的阶, 则 $a^i = a^j$

$$\therefore \langle a^m \rangle = \langle a^{m'} \rangle$$

即 G 的 d 阶子群唯一。

21.

证明:

设 $H \leq S_n$

则 $\sigma_I \in H$

若 H 中无奇置换, 则 H 全部由偶置换组成。

若 $\exists \sigma_o \in H$, 且 σ_o 为奇置换,

则对 \forall 偶置换 $\sigma \in H$, $\sigma \cdot \sigma_o \in H$ 为奇置换,

对 \forall 奇置换 $\sigma_* \in H$, $\sigma_* \cdot \sigma_o \in H$ 为偶置换。

$\therefore H$ 中奇偶置换各占一半。

24.

解:

与 K_4 同构的 S_n 子群为

$\{\sigma_I, (a, b), (c, d), (a, b)(c, d)\}$, 其中 σ_I 为恒同映射, $a, b, c, d \in N$, a, b, c, d 不等。

25.

证明:

设 $\langle G, * \rangle$ 为无限循环群, 则可设 $G = \langle a \rangle$

且不存在有限的 N , 使 $a^N = e$ 。

任取 G 的一个非 $\{e\}$ 子群 $\langle S, * \rangle$,

G 为循环群,

$\therefore S$ 为循环群, 设 $S = \langle a^i \rangle$

若 S 为有限集

则 $\{(a^i)^1, (a^i)^2, \dots, (a^i)^n, \dots\}$ 中必有相等的两项。

设 $(a^i)^j = (a^i)^k$, 则 $a^{ij} = a^{ik}$

$$\therefore a^{i(k \cdot j)} = e$$

这与不存在有限 N 使得 $a^N = e$ 矛盾。

$\therefore S$ 为无限集， $\langle S, * \rangle$ 为无限循环群。