近世代数与数理逻辑作业

wh

2023111xxx

2024-12-14

1　若干基本概念

练习 1 [i]

证明: 以下用数学归纳法证明 n 个确定元素按照任意次序, 任意加括号, 所得到的乘积都等于 $a_1 \circ a_2 \circ \cdots \circ a_n$, 施归纳于 n。

当 n=1,2 时, 由二元代数运算“$\circ$”满足结合律和交换律，结论显然成立。

假设当 n=k-1 时, 结论成立, 往证 n=k 时结论成立。(k>3)

现对于 n 个无次序的元素 $a_{i_1}, a_{i_2}, \cdots, a_{i_n} \in S$, 假设其中 $i_r = n$, 即 $a_{i_r} = a_n$, 则有:

$$
\begin{aligned}
& a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n} \\
= & (ai_1 \circ a_{i_2} \circ \cdots a_{i_{r-1}}) \circ (a_{i_r} \circ (a_{i_{r+1}} \circ \cdots \circ ai_n)) \qquad (\text{结合律, 可任意加括号}) \\
= & (ai_1 \circ a_{i_2} \circ \cdots a_{i_{r-1}}) \circ ((a_{i_{r+1}} \circ \cdots \circ a_{i_n}) \circ a_{i_r}) \qquad (\text{交换律}) \\
= & ((ai_1 \circ a_{i_2} \circ \cdots a_{i_{r-1}}) \circ (a_{i_{r+1}} \circ \cdots \circ a_{i_n})) \circ a_n \qquad (\text{交换律}, a_{i_r} = a_n) \\
= & (ai_1 \circ a_{i_2} \circ \cdots a_{i_{r-1}} \circ a_{i_{r+1}} \circ \cdots \circ a_{i_n}) \circ a_n \\
= & (a_1 \circ a_2 \circ \cdots a_{n-1}) \circ a_n \qquad (\text{由假设得}) \\
= & a_1 \circ a_2 \circ \cdots a_{n-1} \circ a_n
\end{aligned}
$$

综上,n=k 时结论也成立, 归纳推理完毕，命题正确。

[i] 题目为讲义第一讲“若干基本概念”的练习 1

2 半群、幺半群与群

练习 4: 证明有限半群中一定有一个元素 a 使得 $a \circ a = a$。

证明: 取有限半群 G 中的任一元素 a, 令集合 $A = a, a^2, a^3, \cdots, a^{(n+1)}$, 其中 n=|G|.

由抽屉原理可知, 必存在 $a^i = a^j$ 且 i<j, 令 d=j-i,

(1) 若 i<d, 则

$$a^d = a^i \circ a^{d-i} = a^j \circ a^{d-i} = a^{j+d-i} = a^{2d}$$

由此可见,a^d 为 G 中的幂等元素.

(2) 若 i>d, 由 $a^i = a^{i+d} = a^{i+2d} = \cdots$, 故必然存在 $m \in N$, 使 md>i, 则类比 (1), 有

$$a^{md} = a^{mi} \circ a^{md-mi} = a^{m(d+j-i)} = a^{2md}$$

由此可见，a^{md} 为 G 中的幂等元素.

综上, 有限半群 G 中一定存在一个元素 a 使得 $a \circ a = a$,

3 群的简单性质

练习 5: 设 G 为群, 如果 $\forall a \in G, a^2 = e$, 试证:G 为交换群。

证明: 由 G 为群, 则 $\forall a, b \in G$, 有 $ab \in G$, 故 (ab)(ab)=e,

$$\begin{aligned} abab &= e \quad &\text{(结合律, 可任意去括号)} \\ bab &= a \quad &\text{(等号两边同时左乘一个 a)} \\ ab &= ba \quad &\text{(等号两边同时左乘一个 b)} \end{aligned}$$

故群 G 对其运算满足交换律,G 为交换群.

4 子群, 生成子群

练习 4: 找出 3 次对称群中的所有子群。

解: 三次对称群:[ii]

$$S_3 = \{(1),(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}$$

平凡子群:

$$S_3,$$
$$\{(1)\}$$

真子群:

$$\{(1),(1,2)\},$$
$$\{(1),(1,3)\},$$
$$\{(1),(2,3)\},$$
$$A_3{}^{\text{iii}}=\{(1),(1,2,3),(1,3,2)\}$$

[ii] 以下均采用不交轮换的分解式这一表示方式来表示置换

[iii] 该子群为 3 次交代群

5 变换群, 同构

练习 3 [iv]

证明: 要证明 φ 是同构, 只需证以下两个命题成立.

1.φ 是一个双射.

由 $\varphi(x) = \log_p x$, 且 p 为正数, 显然,φ 是一个双射.

2.φ 是同态函数, 即 $\forall a, b \in R_+, \varphi(a \times b) = \varphi(a) + \varphi(b)$.

$$\varphi(a \times b) = \log_p(a \times b) = \log_p a + \log_p b = \varphi(a) + \varphi(b)$$

故 φ 是同态函数.

综上,φ 是同构.

[iv] 题目为讲义第五讲“变换群, 同构”的练习 3

6 循环群

练习 3: 设 G=(a) 为一个 n 阶循环群。证明: 如果 (r,n)=1, 则 $(a^r) = G$。

证明: 由 (r,n)=1,$\exists u, v \in \mathbf{Z}, s.t. un + rv = 1$, 设 e 为 G 的单位元

$$a = a^{un+rv} = (a^n)^u \cdot (a^r)^v = {}^{\mathrm{v}}e \cdot (a^r)^v = (a^r)^v$$

即 $a = (a^r)^v$, 则 G 的生成元 a 可由 a^r 生成, 从而 $(a) \subseteq (a^r)$, 即 $G \subseteq (a^r)$, 又 $(a^r) \subseteq G$, 所以 $(a^r) = G$

[v] 由于 G 是一个 n 阶循环群, 故有 $a^n = e$

7 子群的陪集

练习 2: 设 p 为一个素数, 证明: 在阶为 p^m 的群里一定含有一个 p 阶子群, 其中 $m \geq 1$。

证明: 设 $(G, \circ)$ 为群,$|G| = p^m$, 取 $a \in G(a \neq e)$, 设其阶为 r, 则 r$|p^m$, 由 p 为素数得,$r = p^k, k \geq 1$.

(1) 若 k=1, 则群 G 的一个 p 阶子群为 H=(a).

(2) 若 k>1, 取 $b = a^{p^{k-1}} \in G$, 设 b 的阶为 q, 则 $b^q = e$. 由 $b^p = (a^{p^{k-1}})^p = a^{p^k} = e$, 由元素阶的性质,q|p, 又 $b^q = (a^{p^{k-1}})^q = a^{qp^{k-1}} = e$, 则有 $r|qp^{k-1}$, 即:$p^k|qp^{k-1}$, 从而 p|q.

综上, 由 p|q 且 q|p, 得 p=q. 此时群 G 的一个 p 阶子群为 H=(b).

命题得证。

8 正规子群, 商群

练习 5: 证明两个正规子群的交还是正规子群。

证明: 设 H_1, H_2 为群 G 的两个正规子群, 记 $H = H_1 \cap H_2$. 则对 $\forall a \in G, h \in H$, 由 H_1, H_2 为群 G 的两个正规子群, 可得:$aha^{-1} \in H_1, aha^{-1} \in H_2$, 所以,$aha^{-1} \in H_1 \cap H_2$, 即 $aha^{-1} \in H$, 故 H 是 G 的正规子群.

9 同态基本定理

练习 2: 设 G 为一个循环群,H 为群 G 的子群, 试证:G/H 也为循环群。

证明: 设 G=(a), 由 H 为循环群 (可交换群) 的子群, 故 H 为正规子群. 且 H 为商群 G/H 的单位元, 故对 $\forall bH \in G/H (b \in G), bH = a^k H = (aH)^k$, 因此 G/H=(aH).

10　数理逻辑 1

证明 $\vdash (A \to \neg A) \to \neg A$.

证明:

(1)$A \to (\neg A \to \neg(A \to \neg A))$　定理 3.1.3

(2)$(A \to (\neg A \to \neg(A \to \neg A))) \to ((A \to \neg A) \to (A \to \neg(\neg A \to A)))$　A2

(3)$(A \to \neg A) \to (A \to \neg(\neg A \to A))$　(1)(2)r_{mp}

(4)$(A \to \neg(A \to \neg A)) \to ((A \to \neg A) \to A)$　A3

(5)$(A \to \neg A) \to ((A \to \neg A) \to \neg A)$　(3)(4) 定理 3.1.7r_{mp}

(6)$((A \to \neg A) \to (A \to \neg A)) \to ((A \to \neg A) \to \neg A)$　(5)A2r_{0mp}

(7)$(A \to \neg A) \to (A \to \neg A)$　定理 3.1.1

(8)$(A \to \neg A) \to \neg A$　(6)(7)r_{mp}

11 数理逻辑 2

形式化自然语句“我为且仅为那些部位自己理发的人理发。”

答: 令 x 的论域为全总个体域,

谓词 P(x):x 是理发师,

谓词 Q(x,y):x 为 y 理发.

$$\exists x(P(x) \wedge \forall y(Q(x,y) \leftrightarrow \neg Q(y,y)))$$