近世代数作业七

cycleke

2020 年 11 月 23 日

Contents

1 课后习题

1.1 第一题

证明 不妨设 $G = \{e_1, a, a^2, \ldots, a^{m-1}\}, \bar{G} = \{e_2, b, b^2, \ldots, a^{n-1}\}$。

先证 $\Rightarrow$。若 $G \sim \bar{G}$，不妨设同态为 φ。则 $G/Ker\varphi \cong \bar{G}$，所以 $|G/Ker\varphi| = |\bar{G}| = n$。而 $G/Ker\varphi \leq G$，所以 $|G/Ker\varphi| \bigm| |G|$，即 $n \bigm| m$。

再证 $\Leftarrow$。若 $n \bigm| m$，构造函数 $\varphi : G \to \bar{G}, \forall a^p \in G, 0 \leq p < m, \varphi(a^p) = b^q, p \equiv q(\mathrm{mod}\ n)$。$\forall a^p, a^q \in G, 0 \leq p, q < m, \varphi(a^p \circ a^q) = \varphi(a^{p+q}) = b^s, s \equiv p + q(\mathrm{mod}\ n)$ 又有 $\varphi(a^p) * \varphi(a^q) = b^{s_1} * b^{s_2} = b^{s_1+s_2}$，因为

$$
\begin{gathered}
s_1 \equiv p(\mathrm{mod}\ n) \\
s_2 \equiv q(\mathrm{mod}\ n) \\
s_1 + s_2 \equiv p + q(\mathrm{mod}\ n) \\
\therefore s_1 + s_2 \equiv s(\mathrm{mod}\ n) \\
b^{s_1+s_2} = b^s
\end{gathered}
$$

所以 φ 是一个 G 到 $\bar{G}$ 的同态。由于 $n \bigm| m$，可知 $n \leq m, \forall b^k \in \bar{G}, \varphi(a^k) = b^k$。所以 φ 是一个满射，$G \sim \bar{G}$。

综上所述，命题得证。 □

1.2 第二题

证明 不妨设 $G = \{e, a, a^2, \ldots, a^{n-1}\}, H = \{e, a^k, a^{2k}, \ldots, a^{n-k}\}$。则 $|H| \bigm| |G|$，由第一题结论有 $G \sim H$，设其同态为 $\varphi : G \to \bar{G}, \forall a^p \in G, 0 \leq p < m, \varphi(a^p) = b^q, p \equiv q(\mathrm{mod}\ n)$。则 $Ker\varphi = \{a^{ik}\} = H$，所以 $G \cong G/H$。由于 G 为循环群，所以 G/H 也是循环群。 □

1.3 第三题

1. 构造函数 $\varphi : G \to S_4, \bar{G} = \{\bar{e}, \bar{x}, \bar{y}, \bar{z}\}$，其中

$$
\begin{aligned}
\bar{e} &= \varphi(e) = (1) \\
\bar{x} &= \varphi(x) = (12)(34) \\
\bar{y} &= \varphi(y) = (13)(24) \\
\bar{z} &= \varphi(z) = (14)(23)
\end{aligned}
$$

设 $\bullet$ 为置换的合成，则可以得到表 1

$\bullet$	$\bar{e}$	$\bar{x}$	$\bar{y}$	$\bar{z}$
$\bar{e}$	$\bar{e}$	$\bar{x}$	$\bar{y}$	$\bar{z}$
$\bar{x}$	$\bar{x}$	$\bar{e}$	$\bar{z}$	$\bar{y}$
$\bar{y}$	$\bar{y}$	$\bar{z}$	$\bar{e}$	$\bar{x}$
$\bar{z}$	$\bar{z}$	$\bar{y}$	$\bar{x}$	$\bar{e}$

表 1: $(\bar{G}, \bullet)$ 的乘法表

观察两者的乘法表不难发现，$(G, \circ, e)$ 与 $(\bar{G}, \bullet, \bar{e})$ 同构。

2. 首先证明 $(G_1, *)$ 为一个群。

证明 显然 $*$ 具备封闭性和交换律，且 $\forall x \in G_1, e_1 * x = x, x * x = e_1$，即 e_1 为幺元，每个元素的逆元为其自身，只需证明 $*$ 具有结合律。

$\forall x, y \in G_1$

$$x * (y * e) = x * y = (x * y) * e$$
$$x * (e * y) = x * y = (x * e) * y$$
$$e * (x * y) = x * y = (e * x) * y$$

而 $a * (a * a) = a = (a * a) * a$，所以 $*$ 具有结合律，所以 $(G_1, *, e_1)$ 为一个群。 □

再证明 φ 为一个同态。

证明 通过枚举有表 2 和表 3

p \ q	e	x	y	z
e	e_1	e_1	a	a
x	e_1	e_1	a	a
y	a	a	e_1	e_1
z	a	a	e_1	e_1

表 2: $\varphi(p \circ q)$ 的值

p \ q	e	x	y	z
e	e_1	e_1	a	a
x	e_1	e_1	a	a
y	a	a	e_1	e_1
z	a	a	e_1	e_1

表 3: $\varphi(p) * \varphi(q)$ 的值

所以 $\forall p, q \in G, \varphi(p \circ q) = \varphi(p) * \varphi(q)$，$\varphi$ 为一个 G 到 G_1 的同态。

$$\gamma = \{(e, \{e, x\}), (e, \{e, x\}), (y, \{y, z\}), (z, \{y, z\})\}$$
$$\bar{\varphi} = \{(\{e, x\}, e_1), (\{y, z\}, a)\}$$
$$\varphi = \bar{\varphi} \circ \gamma$$ □

1.4 第四题

证明 显然 $Z(\sqrt{2}) \subset R$，而由于 $(R, +, \times)$ 是一个环，所以若 $(Z(\sqrt{2}), +*)$ 为环，则 $Z(\sqrt{2})$ 为 R 的一个子环，可知我们只需证明 $\forall a, b \in Z(\sqrt{2}), ab, a-b \in Z(\sqrt{2})$。

$\forall a, b \in Z(\sqrt{2}), \exists m_1, m_2, n_1, n_2 \in Z, a = m_1 + n_1\sqrt{2}, b = m_2 + n_2\sqrt{2}$

$$\begin{aligned}
ab &= (m_1 + n_1\sqrt{2}) \times (m_2 + n_2\sqrt{2}) \\
&= (m_1m_2 + 2n_1n_2) + (m_1n_2 + m_2n_1)\sqrt{2} \in Z(\sqrt{2}) \\
a - b &= (m_1 + n_1\sqrt{2}) - (m_2 + n_2\sqrt{2}) \\
&= (m_1 - m_2) + (n_1 - n_2)\sqrt{2} \in Z(\sqrt{2})
\end{aligned}$$

所以 $(Z(\sqrt{2}), +, \times)$ 为一个环。 □

1.5 第五题

证明 先证明 $(Z(i), +)$ 是一个 Abel 群。$\forall a, b, c \in Z(i), \exists m_1, m_2, m_3, n_1, n_2, n_3 \in Z, a = m_1 + n_1 i, b = m_2 + n_2 i, c = m_3 + n_3 i$

$$\begin{aligned}
a + b &= (m_1 + n_1 i) + (m_2 + n_2 i) \\
&= (m_1 + m_2) + (n_1 + n_2)i \in Z(i) \\
b + a &= (m_2 + n_2 i) + (m_1 + n_1 i) \\
&= (m_2 + m_1) + (n_2 + n_1)i \\
&= (m_1 + m_2) + (n_1 + n_2)i \\
&= a + b \\
(a + b) + c &= ((m_1 + n_1 i) + (m_2 + n_2 i)) + (m_3 + n_3 i) \\
&= (m_1 + m_2 + m_3) + (n_1 + n_2 + n_3)i \\
&= (m_1 + n_1 i) + ((m_2 + n_2 i) + (m_3 + n_3 i)) \\
&= a + (b + c) \\
0 + a &= 0 + (m_1 + n_1 i) \\
&= m_1 + n_1 i \\
&= a \\
(-m_1 - n_1 i) + a &= (-m_1 - n_1 i) + (m_1 + n_1 i) \\
&= 0
\end{aligned}$$

所以 $+$ 是 $Z(i)$ 上的二元运算，满足交换律和结合律，且代数系存在幺元，每个元素存在左逆元。所以 $(Z(i), +, 0)$ 是一个 Abel 群。

再证明 $(Z(i), \times)$ 是一个半群。$\forall a, b, c \in Z(i), \exists m_1, m_2, m_3, n_1, n_2, n_3 \in Z, a = m_1 + n_1 i, b = m_2 + n_2 i, c = m_3 + n_3 i$

$$\begin{aligned}
a \times b &= (m_1 + n_1 i) \times (m_2 + n_2 i) \\
&= (m_1m_2 - n_1n_2) + (m_1n_2 + m_2n_1)i \in Z(i) \\
(a \times b) \times c &= ((m_1 + n_1 i) \times (m_2 + n_2 i)) \times (m_3 + n_3 i) \\
&= ((m_1m_2 - n_1n_2) + (m_1n_2 + m_2n_1)i) \times (m_3 + n_3 i) \\
&= (m_1m_2m_3 - m_1n_2n_3 - n_1m_2n_3 - n_1n_2m_3) + (m_1m_2n_3 + m_1n_2m_3 + n_1m_2m_3 - n_1n_2n_3)i
\end{aligned}$$

$$
\begin{aligned}
a\times(b\times c) &= (m_1+n_1 i)\times((m_2+n_2 i)\times(m_3+n_3 i))\\
&= (m_1+n_1 i)\times((m_2m_3-n_2n_3)+(m_2n_3+m_3n_2)i)\\
&= (m_1m_2m_3-m_1n_2n_3-n_1m_2n_3-n_1n_2m_3)+(m_1m_2n_3+m_1n_2m_3+n_1m_2m_3-n_1n_2n_3)i
\end{aligned}
$$

$(a\times b)\times c = a\times(b\times c)$

所以 $\times$ 是 $Z(i)$ 上的二元运算，且满足结合律，所以 $(Z(i),\times)$ 是一个半群。

最后证明 $\times$ 对 $+$ 满足分配律。$\forall a,b,c\in Z(i),\exists m_1,m_2,m_3,n_1,n_2,n_3\in Z, a=m_1+n_1 i, b=m_2+n_2 i, c=m_3+n_3 i$

$$
\begin{aligned}
a\times(b+c) &= (m_1m_2+m_1m_3-n_1n_2-n_1n_3)+(n_1m_2+n_1m_3+m_1n_2+m_1n_3)i\\
&= (m_1m_2-n_1n_2)+(n_1m_2+m_1n_2)i+(m_1m_2-n_1n_3)+(n_1m_3+m_1n_3)i\\
&= a\times b+a\times c\\
(b+c)\times a &= (m_1m_2+m_1m_3-n_1n_2-n_1n_3)+(n_1m_2+n_1m_3+m_1n_2+m_1n_3)i\\
&= b\times a+c\times a
\end{aligned}
$$

综上所述，$(Z(i),+,\times)$ 为一个环。 □

1.6 第六题

证明 取 $(1+\sqrt[3]{2})\in Q(\sqrt[3]{2})$，则 $(1+\sqrt[3]{2})\times(1+\sqrt[3]{2})=1+2\sqrt[3]{2}+2^{\frac{2}{3}}\notin Q(\sqrt[3]{2})$，所以 $\times$ 对 $Q(\sqrt[3]{2})$ 不封闭，$Q(\sqrt[3]{2})$ 对数的通常加法和乘法不构成一个环。 □

1.7 第七题

证明 由于 $(R,+,\times)$ 是一个域，$Q(\sqrt[3]{2},\sqrt[3]{4})\subset R$，$\times$ 具有交换律。所以若可以证明 $Q(\sqrt[3]{2},\sqrt[3]{4})$ 是 R 的一个子体，则命题得证。

显然 $|Q(\sqrt[3]{2},\sqrt[3]{4})|\geq 2$。$\forall x,y\in Q(\sqrt[3]{2},\sqrt[3]{4}),\exists a_1,a_2,b_1,b_2,c_1,c_2\in Q x-y=(a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4})-(a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4})=(a_1-a_2)+(b_1-b_2)\sqrt[3]{2}+(c_1-c_2)\sqrt[3]{4}\in Q(\sqrt[3]{2},\sqrt[3]{4})$，如果 $x\neq 0,y\neq 0$，则 a_1,b_1,c_1 不同时为零，a_2,b_2,c_2 不同时为零。则 $ab^{-1}\in Q(\sqrt[3]{2},\sqrt[3]{4})$。所以 $Q(\sqrt[3]{2},\sqrt[3]{4})$ 是 R 的一个子体。

综上所述，$Q(\sqrt[3]{2},\sqrt[3]{4})$ 是一个域。 □

1.8 第八题

证明 若 e 不是单位元，则 e 不是右单位元，$\exists a\in R, ea=a, ae\neq a$，则 $ae-a+e\neq e$。而 $\forall b\in R,(ae-a+e)b=aeb-ab+b=b$，所以 $ae-a+e$ 也是一个左单位元。这与 e 为唯一左单位元矛盾，所以 e 是单位元。 □

1.9 第九题

证明 由于 a，b，$ab-1$ 有逆元，所以

$$
\begin{aligned}
(a-b^{-1})(b(ab-1)^{-1}) &= ((a-b^{-1})b)(ab-1)^{-1}\\
&= (ab-1)(ab-1)^{-1}\\
&= 1
\end{aligned}
$$

$$\therefore (a-b^{-1})^{-1} = b(ab-1)^{-1}$$

$$\begin{aligned}((a-b^{-1})^{-1}-a^{-1})(aba-a) &= (b(ab-1)^{-1}-a^{-1})(ab-1)a \\ &= (b-a^{-1}(ab-1))a \\ &= ba-ba+1 \\ &= 1\end{aligned}$$

$$\therefore ((a-b^{-1})^{-1}-a^{-1})^{-1} = (aba-a)$$

命题得证。 □

1.10 第十题

证明 不妨设 a 为 R 的一个零因子，则 $\exists b \in R, b \neq 0, ab = 0$。若 a 存在逆元素 a^{-1}，则

$$\begin{aligned}ab &= 0 \\ a^{-1}ab &= 0 \\ b &= 0\end{aligned}$$

产生矛盾，所以 a 不存在逆元。 □

1.11 第十一题

证明 由于 a, b 在交换环中，所以 $ab = ba$，由环的性质有

$$(a+b)^n = \sum_{i=1}^{n} \binom{n}{i} a^i b^{n-i}$$

命题得证。 □

1.12 第十二题

证明 显然 0 无左逆元。对于任一有左逆元的非零元素 a，设其左逆元为 a_l。若 a 无右逆元，则 $aa_l \neq e, a_l a a_l \neq a_l, a_l \neq a_l$，产生矛盾，所以 a 有右逆元，进而有逆元。 □

1.13 第十三题

证明 若 $ab = ba$，则

$$\begin{aligned}a(-b) &= -(ab) \\ &= -(ba) \\ &= (-b)a \\ a(-ab) &= -(aab) \\ &= -(aba) \\ &= (-ab)a\end{aligned}$$

所以 a 与 b，a 与 ab 可交换。

若 a 与 b,c 可交换，即 $ab=ba,ac=ca$，则

$$\begin{aligned} a(b+c) &= ab+ac \\ &= ba+ca \\ &= (b+c)a \\ a(a+c) &= aa+ac \\ &= aa+ca \\ &= (a+c)a \end{aligned}$$

所以 a 与 $b+c$，a 与 $a+c$ 可交换。 □