# 近世代数课后习题作业 6 参考解答

1.

证明：必要性$\Rightarrow$：设 $\varphi: G\to\overline{G}$ 的满同态，根据群同态基本定理有：$G/Ker\,\varphi\cong\overline{G}$，

则 $|G/Ker\,\varphi|=|\overline{G}|=n$，又根据拉格朗日定理得：$|G/Ker\,\varphi|=\dfrac{|G|}{|Ker\,\varphi|}=\dfrac{m}{|Ker\,\varphi|}$，

即 $m=n\cdot|Ker\,\varphi|$，所以 $n\mid m$。

充分性$\Leftarrow$：设 $G=(a),a^m=e$， $\overline{G}=(b),b^n=\overline{e}$， $\varphi: G\to\overline{G}$，且对 $\forall a^k\in G$，

$\varphi(a^k)=b^k$

1）$\varphi$ 为映射：若 $a^k=a^l$，则 $a^{k-l}=e$，又 $a^m=e$，所以 $m\mid(k-l)$，又 $n\mid m$，所以 $n\mid(k-l)$，而 $b^n=\overline{e}$，所以 $b^{k-l}=\overline{e}$，则 $b^k=b^l$，即 $\varphi(a^k)=\varphi(a^l)$。

2）同态方程：对 $\forall a^k,a^l\in G$， $\varphi(a^k\cdot a^l)=\varphi(a^{k+l})=b^{k+l}=b^kb^l=\varphi(a^k)\varphi(a^l)$。

综上 $G\sim\overline{G}$。

////////////////////////////////////////////////////////////////////////////

2.

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

////////////////////////////////////////////////////////////////////////////

3.

1） $(Z(\sqrt{2}),+)$ 为 Abel 群：

①封闭性：对 $\forall m_1+n_1\sqrt{2},m_2+n_2\sqrt{2}\in Z(\sqrt{2})$，有：

$$(m_1+n_1\sqrt{2})+(m_2+n_2\sqrt{2})=(m_1+m_2)+(n_1+n_2)\sqrt{2}\in Z(\sqrt{2})$$

②结合律：显然。

③单位元： $e=0$。

④逆元：对 $\forall m+n\sqrt{2},\in Z(\sqrt{2})$， $(m+n\sqrt{2})+((-m)+(-n\sqrt{2}))=0\in Z(\sqrt{2})$

⑤交换律：显然。

2） $(Z(\sqrt{2}),*)$ 为半群：

①封闭性：对 $\forall m_1+n_1\sqrt{2},m_2+n_2\sqrt{2}\in Z(\sqrt{2})$，有：

$(m_1+n_1\sqrt{2})*(m_2+n_2\sqrt{2})=(m_1m_2+2n_1n_2)+(m_2n_1+m_1n_2)\sqrt{2}\in Z(\sqrt{2})$

②结合律：显然。

3）分配律：显然。

////////////////////////////////////////////////////////////////////////

4.

证明：$(Z(i),+)$ 为 Abel 群，$(Z(i),*)$ 为半群，且分配律显然成立。

////////////////////////////////////////////////////////////////////////

5.

证明：$Q(\sqrt[3]{2})$ 对乘法不封闭。

假设 $Q(\sqrt[3]{2})$ 对乘法封闭，则由 $\sqrt[3]{2}\in Q(\sqrt[3]{2})\Rightarrow(\sqrt[3]{2})^2\in Q(\sqrt[3]{2})$，设 $(\sqrt[3]{2})^2=a+b\sqrt[3]{2}$，

$\Rightarrow 2=a\sqrt[3]{2}+b(\sqrt[3]{2})^2\Rightarrow 2=a\sqrt[3]{2}+b(a+b\sqrt[3]{2})\Rightarrow 2=ab+(a+b^2)\sqrt[3]{2}$

$\Rightarrow\sqrt[3]{2}=\dfrac{2-ab}{a+b^2}$，而 $\dfrac{2-ab}{a+b^2}$ 为有理数，$\sqrt[3]{2}$ 为无理数，故矛盾。

注：证 $\sqrt[3]{2}$ 为无理数

假设 $\sqrt[3]{2}$ 为有理数，则有：$\sqrt[3]{2}=\dfrac{q}{p}$，$(p,q)=1$。

从而 $q^3=2p^3\Rightarrow p^3\mid q^3\Rightarrow(p^3,q^3)=p^3$，又由 $(p,q)=1$ 可得：

$1=(p,q(p,q))=((p,pq),q^2)=(p,q^2)=\cdots=(p^3,q^3)$，从而 $p^3=1\Rightarrow p=1$，所以

$\sqrt[3]{2}=q$，即 $\sqrt[3]{2}$ 为整数，而 $1<\sqrt[3]{2}<2$，矛盾。

////////////////////////////////////////////////////////////////////////

6.

证明：$(Q(\sqrt[3]{2},\sqrt[3]{4}),+)$ 为 Abel 群，$(Q(\sqrt[3]{2},\sqrt[3]{4})\setminus\{0\},*)$ 为 Abel 群，且分配律显然成立。

////////////////////////////////////////////////////////////////////////

7.

证明：设 $(S,+,\circ)$ 为环，记其唯一的左单位元为 $e_1$，即对 $\forall a\in S$，$e_1a=a$，下证 $ae_1=a$，只须证：$ae_1-a=0$。因为 $(e_1+ae_1-a)a=e_1a+(ae_1)a-aa=a$，所以 $e_1+ae_1-a$ 也为一左单位元，故 $e_1+ae_1-a=e_1$，所以 $ae_1-a=0$，即 $ae_1=a$。

8.

证明：由 $(a-b^{-1})b=ab-1 \Rightarrow a-b^{-1}=(ab-1)b^{-1}$，则 $(a-b^{-1})^{-1}=b(ab-1)^{-1}$。

又 $(a-b^{-1})((a-b^{-1})^{-1}-a^{-1})=1-(1-b^{-1}a^{-1})=b^{-1}a^{-1}$，则：

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

从而 $((a-b^{-1})^{-1}-a^{-1})^{-1}=ab(ab-1)b^{-1}=aba-a$。

////////////////////////////////////////////////////////////////////////

9.

证明：设 $(S,+,\circ)$ 为环，单位元为 1， $\forall a \in S$，且 $a$ 为非零的零因子。下设 $a$ 存在逆元素，记为 $a^{-1}$，则有： $a^{-1}a=1$

由 $a$ 为非零的零因子，则 $\exists b \in S \wedge b \neq 0$，使得 $ab=0$，又由 $a^{-1}a=1 \Rightarrow a^{-1}(ab)=b$ $\Rightarrow b=0$，矛盾。

////////////////////////////////////////////////////////////////////////

10.

证明：设 $(S,+,\circ)$ 为交换环，则 $\forall a,b \in S$， $ab=ba$

1）当 $n=0,1$ 时显然成立。当 $n=2$ 时：

$$(a+b)^2=(a+b)(a+b)=(a+b)a+(a+b)b=a^2+ba+ab+b^2=a^2+2ab+b^2$$ 。

2）假设当 $n=k$ 时成立，即：

$$(a+b)^k=a^k+C_k^1a^{k-1}b+C_k^2a^{k-2}b^2+\cdots+C_k^kb^k$$

则当 $n=k+1$ 时：

$$(a+b)^{k+1}=(a+b)^k(a+b)=(a^k+C_k^1a^{k-1}b+C_k^2a^{k-2}b^2+\cdots+C_k^kb^k)(a+b)$$

$$=a^{k+1}+C_k^1a^kb+C_k^2a^{k-1}b^2+\cdots+C_k^kab^k$$

$$+a^kb+C_k^1a^{k-1}b^2+C_k^2a^{k-2}b^3+\cdots+C_k^kb^{k+1}$$

$$=a^{k+1}+(C_k^1+1)a^kb+(C_k^2+C_k^1)a^{k-1}b^2+\cdots+(C_k^k+C_k^{k-1})ab^k+b^{k+1}$$

$$=a^{k+1}+C_{k+1}^1a^{k+1-1}b+C_{k+1}^2a^{k+1-2}b^2+\cdots+C_{k+1}^kab^k+b^{k+1}$$

（$C_k^{i+1}+C_k^i=C_{k+1}^{i+1}$）

11.

证明：设 $a_l$ 为 $a$ 的左逆元，由 $a_l a = 1 \Rightarrow aa_l aa_l = aa_l$，由于 $R$ 为无零因子环满足消去律，则得：$aa_l = 1$。

////////////////////////////////////////////////////////////////////////////

12.

证明：

1） $a(-b) = -(ab) = -(ba) = (-b)a$

2） $a(-ab) = (-a)(ab) = (-a)(ba) = -(aba) = (-ab)a$

3） $a(b+c) = ab + ac = ba + ca = (b+c)a$

4） $a(a+c) = aa + ac = aa + ca = (a+c)a$

////////////////////////////////////////////////////////////////////////////

13.

证明：设 $(F, +, \circ)$ 为域。

1）由 $|F| = 4$，故 $(F, +)$ 的特征数只能是 1，2，4（关于加法群的阶，根据拉格朗日定理可得），又 $F$ 为域，则其特征数为素数，所以 $F$ 的特征数是 2。

2）由已知可设 $F = \{0, e, a, a^{-1}\}$（因为出了零元素外，剩余 3 元素也构成群），且 $a^2 = a^{-1}$（因为 $F \setminus \{0\}$ 为三阶群，由于阶为素数故 $F \setminus \{0\}$ 为循环群，即 $a^3 = e$）。

① 当 $x = a$ 时，显然有 $a + e = 0 或 a^{-1}$，

若 $a + e = 0 \Rightarrow e + a^{-1} = 0 \Rightarrow a = a^{-1}$，矛盾。

故只能有 $a + e = a^{-1}$，即 $a + e = a^2$，满足方程 $x^2 = x + e$

② 当 $x = a^{-1}$ 时，显然有 $a^{-1} + e = 0 或 a$，

若 $a^{-1} + e = 0 \Rightarrow e + a = 0 \Rightarrow a = a^{-1}$，矛盾。

故只能有 $a^{-1} + e = a \Rightarrow a^{-1} + e = a^{-2} = (a^{-1})^2$，满足方程 $x^2 = x + e$

////////////////////////////////////////////////////////////////////////////

14.

解：不是。如 $p = 6$，则 $[2] \neq [0]$，$[3] \neq [0]$，但 $[2][3] = [6] = [0]$，与域为无零因子环矛盾。

15．设域$F$的特征为有限数$p$，$a$与$b$及$a_i$均在$F$里。证明：

$$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$$

$$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p$$

证明：先证$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$

1）当$n=1$时，由定理知成立。

2）假设当$n=k$时也成立，即$(a\pm b)^{p^k}=a^{p^k}\pm b^{p^k}$

则当$n=k+1$时，$(a\pm b)^{p^{k+1}}=((a\pm b)^{p^k})^p=(a^{p^k}\pm b^{p^k})^p$，又根据已证定理可得：$(a^{p^k}\pm b^{p^k})^p=(a^{p^k})^p\pm(b^{p^k})^p=a^{p^{k+1}}\pm b^{p^{k+1}}$，即$(a\pm b)^{p^{k+1}}=a^{p^{k+1}}\pm b^{p^{k+1}}$。

再证$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p$

$(a_1+a_2+\cdots+a_n)^p=((a_1+a_2+\cdots+a_{n-1})+a_n)^p=(a_1+a_2+\cdots+a_{n-1})^p+a_n^p$

$=(a_1+a_2+\cdots+a_{n-2})^p+a_{n-1}^p+a_n^p=\cdots=a_1^p+a_2^p+\cdots+a_{n-2}^p+a_{n-1}^p+a_n^p$。

//////////////////////////////////////////////////////////////////////////

16.

证明：

1）$E=\{2k\mid k\in Z\}$, 对$\forall 2k_1,2k_2\in E$，$2k_1-2k_2=2(k_1-k_2)\in E$；

又$2k_1\cdot 2k_2=2(2k_1k_2)\in E$，所以$E$是$Z$的一个子环。

2）对$\forall r_1,r_2\in E$，$4r_1-4r_2=4(r_1-r_2)\in N$，$r_1\cdot 4r=4(r_1r)\in N$，故$N$是的$E$理想。

3）$N\neq(4)$，因为$4\in(4)$，但显然$4\notin N$。

//////////////////////////////////////////////////////////////////////////

17.

证明：由 3 与 7 互质，则$k_1,k_2\in Z$，使得$k_1\cdot 3+k_2\cdot 7=1$，即$1\in(3,7)$，而$Z=(1)$，

所以$(3,7)=Z$，同理$(13,10)=Z$

//////////////////////////////////////////////////////////////////////////

18.

证明：

1）对$\forall n_1+h_1,n_2+h_2\in N+H$，$(n_1+h_1)-(n_2+h_2)=(n_1-n_2)+(h_1-h_2)$，

又$(n_1-n_2)\in N,(h_1-h_2)\in H$，所以$(n_1+h_1)-(n_2+h_2)\in N+H$。

2）对 $\forall r \in R$，$n+h \in N+H$，$r(n+h)=rn+rh$，$(n+h)r=nr+hr$，而 $rn \in N, nr \in N$，$rh \in H, hr \in H$，所以 $r(n+h) \in N+H$，$(n+h)r \in N+H$。

综上 $N+H$ 也是 $R$ 的理想。