# 第二周作业参考解答及补充

## 作业

**1.** (习题 1.4.1)

设 $\varphi: G \to G'$ 是群同态, 试证明:

(1) $\ker(\varphi) \coloneqq \{g \in G \mid \varphi(g) = e'\}$ ($e' \in G'$ 表示的单位元) 是 $G$ 的子群 (称为群同态 $\varphi$ 的核);

(2)

$$\varphi(G) = \{\varphi(g) \mid \forall g \in G\} \subset G'$$

是 $G'$ 的子群 (称为群同态 $\varphi$ 的像).

*proof*

教材命题 1.4.1 的 (1)(5) 直接使用.

(1) $e \in \ker(\varphi)$ 非空, 直接验证

$$\begin{aligned} &\forall a, b \in \ker(\varphi),\ \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e'e' = e' \\ &\implies ab^{-1} \in \ker(\varphi). \end{aligned}$$

(2) $e' \in \varphi(G)$ 非空, 直接验证

$$\begin{aligned} &\forall x, y \in \varphi(G),\ \exists a, b \in G,\ x = \varphi(a), y = \varphi(b) \\ &\implies xy^{-1} = \varphi(a)(\varphi(b))^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(G). \end{aligned}$$

**2.** (习题 1.4.3)

设 $R \xrightarrow{\varphi} R'$ 是环同态, 证明集合 $ker(\varphi) = \{x \in R \mid \varphi(x) = 0_{R'}\}$ 满足:

(1) $\ker(\varphi)$ 是 $(R, +)$ 的子群;

(2) $\forall a \in \ker(\varphi), x \in R$ 有 $ax \in \ker(\varphi)$, $xa \in \ker(\varphi)$. ($\ker(\varphi)$ 称为环同态 $\varphi$ 的核.)

*proof*

(1) 即习题 1.4.1(1);

(2) 直接验证

$$\forall a \in \ker(\varphi),\ x \in R,\ \varphi(xa) = \varphi(x)\varphi(a) = \varphi(x)0_{R'} = 0_{R'}$$

另一半同理.

**3.** (习题 1.4.5)

证明实数的加法群 $(\mathbb{R}, +)$ 和正实数的乘法群 $(\mathbb{R}_{>0}, \cdot)$ 同构.

*proof*

注意到 $f:\mathbb{R}\to\mathbb{R}_{>0}$, $x\mapsto e^x$ 是同构. $f^{-1}(x)=\ln x$.
注: 事实上, 由 $f(x+y)=f(x)f(y)$ 可以先直接推出 $f(x)=a^x$, $a=f(1)$, $x\in\mathbb{Q}$, 再根据连续性延拓到 $\mathbb{R}$ 上.

**4.** (习题 1.4.6)

证明有理数的加法群 $(\mathbb{Q},+)$ 和正有理数的乘法群 $(\mathbb{Q}_{>0},\cdot)$ 不同构.

*proof*

反证, 假设存在同构 $f:\mathbb{Q}\to\mathbb{Q}_{>0}$, 则设 $2=f(a)=f(\frac{a}{2}+\frac{a}{2})=f(\frac{a}{2})\cdot f(\frac{a}{2})=f(\frac{a}{2})^2$ 矛盾.

**5.** (习题 1.4.9)

设 $K,L$ 是两个域, 如果 $L$ 是 $K$ 的子域, 则 $K$ 称为 $L$ 的扩域, $K\supset L$ 称为域扩张, 试证明:

(1) 域的加法和乘法使得 $K$ 是一个 $L$-向量空间 ($[K:L]=\dim_L(K)$ 称为域扩张 $K\supset L$ 的次数);

(2) 如果 $K\supset\mathbb{R}$ 是一个二次扩张 (即 $[K:\mathbb{R}]=2$), 则 $K$ 必同构于复数域 $\mathbb{C}$.

*proof*

(1) $(K,+)$ 是一个 Abel 群, 这一点无需再说明. 乘法在这里可能有些歧义, 此处是要验证乘法限制在 $L\times K$ 上, 即

$$\cdot: L\times K\to K,\quad (l,k)\mapsto lk$$

是数乘. 即要验证

$$(l_1l_2)k=l_1(l_2k),$$
$$(l_1+l_2)k=l_1k+l_2k,$$
$$l(k_1+k_2)=lk_1+lk_2,$$
$$1k=k=k1.$$

这些都由域的定义得到.

这也说明若同态 $K_1\to K_2$ 保持 $L(K_1,K_2$ 为 $L$ 的两个扩域), 则一定是 $L$-线性映射.

事实上, 若有环同态 $R\xrightarrow{\varphi}S$, 则 $S$ 上自动有一个 $R$-模结构

$$R\times S\to S,\quad (r,s)\mapsto\varphi(r)s$$

这道题对应的同态其实就是包含 (inclusion)$L\overset{i}{\hookrightarrow}K$.

(2) 由 (1), 扩域 $\mathbb{C}/\mathbb{R}$ 的自同构一定是 $\mathbb{R}$-线性的. 设同构 $f:\mathbb{C}\to\mathbb{C}$, 则有 $f(x+yi)=x+yf(i)$, $x,y\in\mathbb{R}$, 且保持乘法, 可得 $f(i)=\pm i$. 也就是说 $\mathbb{C}/\mathbb{R}$ 的自同构都只有恒等映射和共轭, 即 $\mathrm{Gal}(\mathbb{C}/\mathbb{R})=\mathbb{Z}/2\mathbb{Z}$.

由线性代数的结论, 可以直接得到 $K$ 和 $\mathbb{C}$ 是作为线性空间同构, 但这是不够的, 只有上述两个线性映射是域同构, 需要做基变换转为恒等或共轭才能保持乘法. 事实上只要存在一个基变换就能变回恒等映射, 恒等映射总是同构, 但前提是承载集合 (underlying set) 要一样. 比如 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 作为 $\mathbb{Q}$-线性空间也是同构的, 但他们之间没有域同态.

可取 $K$ 的一组基为 $1, \alpha$, 其中 $\alpha \in \mathbb{C} \setminus \mathbb{R}$. 不可避免地要考虑 $\alpha^2$ 的结果, 由于 $1, \alpha$ 是基, 因此 $\alpha^2$ 可以被线性表出, 即 $\alpha^2 = x + y\alpha$. 由于 $\alpha \notin \mathbb{R}$, 有 $y^2 + 4x < 0$, 解二次方程得到 $\alpha = \dfrac{y \pm i\sqrt{|y^2+4x|}}{2}$. 故映射

$$f : K \to \mathbb{C}, u + v\alpha \mapsto u + v\frac{y \pm i\sqrt{|y^2+4x|}}{2}$$

是域同构.

注意 $K$ 是域, 也就是说 $K$ 的乘法是已知的, 无法把 $K$ 先看作 $\mathbb{R}$-线性空间然后重定义向量的乘法, 这在逻辑上是不对的.

**6.** (习题 1.4.11)

设 $L \supset K$ 是一个域扩张, 证明: 下述集合

$$\mathrm{Gal}(L/K) = \left\{ L \xrightarrow{\sigma} L \mid \sigma \text{ 是域同构, 且} \sigma(a) = a \text{ 对任意} a \in K \text{ 成立} \right\}$$

关于映射的合成是一个群 (称为域扩张 $L \supset K$ 的伽罗瓦群).

*proof*

$\mathrm{Gal}(L/K) \subseteq \mathrm{Aut}(L)$, 只需说明 $\mathrm{Gal}(L/K)$ 是子群.
$\forall \varphi, \psi \in \mathrm{Gal}(L/K)$, 由于 $\psi|_K = \mathrm{id}_K$, 因此 $\psi^{-1}|_K = \mathrm{id}_K$, 故 $(\varphi \circ \psi^{-1})|_K = \mathrm{id}_K$, 即 $\varphi \circ \psi^{-1} \in \mathrm{Gal}(L/K)$.

## 课上的补充内容

好像没有....