

## 第七周作业参考解答及补充

### 作业

#### 1. (习题 2.1.11)

设  $R$  是一个环, 子环  $C(R) = \{a \in R \mid ab = ba \forall b \in R\}$  称为  $R$  的中心. 试证明:

- (1) 如果  $R$  是一个除环, 则  $C(R)$  是一个域;
- (2) 令  $\mathbb{H}$  表示 Hamilton 四元数环, 则  $C(\mathbb{H}) = \mathbb{R}$ .

*proof*

- (1) 除环的子环自然是除环,  $C(R)$  和  $R$  中所有元素交换, 故  $C(R)$  本身是交换环, 从而是域.
- (2) 设  $\alpha = a + ib + jc + kd \in C(\mathbb{H})$ , 则有

$$\alpha \cdot i = i \cdot \alpha$$

$$\alpha \cdot j = j \cdot \alpha$$

得到  $b = c = d = 0$ , 即  $\alpha \in \mathbb{R}$ .

□

#### 2. (习题 2.1.12)

设  $K$  是一个域. 如果  $C(R)$  包含一个同构于  $K$  的子域, 则称环  $R$  为  $K$ -代数. 试证明: 加法群  $(R, +)$  通过  $R$  的乘法成为一个  $K$ -向量空间.

*proof*

见 1.4.9 和 2.1.8 的注记.  $C(R)$  包含一个和  $K$  同构的子域, 等价地说就是有一个域同态  $K \rightarrow R$ .

□

**注:**

$C(R)$  包含一个同构于  $K$  的子域, 即存在同态  $K \xrightarrow{\varphi} R$  使得  $\varphi(K) \subseteq C(R)$  (这是因为域出发的同态一定是单的). 这和之前说的是一样的.

#### 3. (习题 2.1.13)

设  $R$  是一个  $K$ -代数,  $\dim_K(R)$  称为  $R$  的维数. 试证明:

- (1) 矩阵环  $M_n(K)$  是一个  $n^2$  维  $K$ -代数;

- (2) 任意  $n$  维  $K$ -代数必同构于  $M_n(K)$  的子环;
- (3) 如果  $R$  是一个有限除环, 则  $R$  是有限域上的有限维代数.

*proof*

- (1)  $M_n(K)$  是  $n^2$  维  $K$ -线性空间, 按之前 2.1.8 的注记只需验证

$$k_1 M_1 k_2 M_2 = k_1 k_2 M_1 M_2, k_1, k_2 \in K, M_1, M_2 \in M_n(K).$$

这可以根据  $M_n(K)$  的定义得到. 事实上  $C(M_n(K)) = \{kI_n \mid k \in K\} \cong K$ .

- (2) 由教材例 1.4.3, 对任意的环  $R$ , 我们用  $\text{End}_{\text{Ab}}(R)$  表示加法群的自同态环 (关于加法和复合). 有一个自然的环同态,

$$R \rightarrow \text{End}_{\text{Ab}}(R), \quad r \mapsto \lambda_r$$

其中  $\lambda_r : R \rightarrow R, a \mapsto ra$ , 即左乘  $r$  这个自同态 (这里换成右乘也是一样的). 这是一个单同态, 所以  $R$  同构于  $\text{End}_{\text{Ab}}(R)$  的一个子环.

那么当  $R$  是  $n$  维  $K$ -代数时,  $\lambda_r$  还是  $K$ -线性映射. 因此有单射  $R \hookrightarrow \text{Hom}_K(R) \cong M_n(K)$ .

- (3)  $R$  是有限除环, 因此  $C(R)$  是有限域 (2.1.11). 根据定义  $R$  是一个  $C(R)$ -代数, 且  $R$  有限, 故是有限维的 ( $|R| = [R : C(R)][C(R)]$ ).

□

#### 4. (习题 2.1.14)

设  $K$  是一个域,  $R$  是一个有限维  $K$ -代数. 试证明:

- (1)  $\forall \alpha \in R$ , 存在非零多项式  $f(x) \in K[x]$  使得  $f(\alpha) = 0$ ;
- (2) 如果  $R$  是除环,  $\alpha \neq 0$ , 则  $\alpha$  的极小多项式  $\mu_\alpha(x) \in K[x]$  不可约;
- (3) 如果  $R$  是除环,  $K$  是代数闭域 (即  $K[x]$  中次数大于零的多项式在  $K$  中必有根), 则  $R = K$ .

历史上, 有限维可除  $K$ -代数的分类是一个热门话题. 当  $K$  是实数域时,  $R$  必同构于实数域, 复数域或 Hamilton 四元数环之一 (Frobenius 定理); 当  $K$  是有限域时,  $R$  必为交换环 (Wedderburn 定理).

注:

零多项式是平凡的, 因此 (1) 我做了修改. 在域扩张中, 这样的元素称为  $K$  上的代数元 (algebraic element), 或者称  $\alpha$  在  $K$  上代数 (algebraic over  $K$ ). 给定域扩张  $L/K$ , 若  $\forall \alpha \in L$  都在  $K$  上代数, 则称该扩张是代数扩张.

虽然已经讲到域扩张了, 但这是很早之前写的, 我就不删了.

proof

- (1) 设  $\dim_K R = n$ . 则  $1, \alpha, \alpha^2, \dots, \alpha^n$  线性相关. 或者考虑线性映射  $r \mapsto \alpha r$ . 那么它对应的矩阵的特征多项式满足条件 (Cayley-Hamilton Theorem).
- (2) 按定义,  $\mu_\alpha$  是满足  $\alpha$  的次数最小的 (首一) 多项式. 假设  $\mu_\alpha$  可约, 即  $\mu_\alpha(x) = f(x)g(x)$ ,  $\deg(f), \deg(g) > 0$ , 则  $0 = \mu_\alpha(\alpha) = f(\alpha)g(\alpha)$ . 由于除环无零因子, 故  $\deg(\mu_\alpha) = \deg(f) + \deg(g)$ , 且  $f(\alpha) = 0$  或  $g(\alpha) = 0$ . 不妨设  $f(\alpha) = 0$ , 但  $\deg(f) < \deg(\mu_\alpha)$  与极小矛盾.
- (3) 代数闭域等价于任意多项式可分解成一次多项式的乘积. 这和代数基本定理是类似的. 此时  $K[x]$  中的不可约多项式即为所有一次多项式. 由 (2),  $\forall \alpha \in R$ , 极小多项式  $\mu_\alpha(x) = x - k_\alpha, k_\alpha \in K$ . 因此  $\alpha = k_\alpha \in K$ . 即  $R = K$ .

□

### 5. (习题 2.4.1)

设  $F$  是一个域,  $R = F[x_1, x_2, \dots, x_n]$ , 令  $R_m \subseteq R$  表示所有  $m$  次齐次多项式的集合 (并上零多项式). 证明:  $R_m$  是域  $F$  上的  $\binom{m+n-1}{m}$  维向量空间.

proof

设  $f \in R_m$ , 根据  $R_m$  的定义,  $f$  可以写成

$$f = \sum_{i_1+i_2+\dots+i_n=m} a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$$

$a_{i_1 i_2 \dots i_n} \in F$  允许为 0,  $i_k \geq 0, 1 \leq k \leq n$ . 那么  $f$  的表达式中共有  $\binom{m+n-1}{m}$  项. 记  $N = \binom{m+n-1}{m}$ ,  $I = \{(i_1, i_2, \dots, i_n) \in \mathbb{N}^n \mid i_1 + i_2 + \dots + i_n = m\}$ . 因此映射

$$R_m \rightarrow F^N, \quad f \mapsto (a_{i_1 i_2 \dots i_n})_{(i_1, i_2, \dots, i_n) \in I}$$

是 (线性) 同构.

□

### 6. (习题 2.4.2)

证明:  $f(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$  是  $m$  次齐次多项式当且仅当  $f(tx_1, tx_2, \dots, tx_n) = t^m f(x_1, x_2, \dots, x_n)$ , ( $t$  是一个新的不定元).

*proof*

” $\Rightarrow$ ” 这个方向提出公因式  $t^m$  即可, 下证” $\Leftarrow$ ”:

由于  $f$  可以唯一表示成齐次多项式的和, 即

$$f = f_0 + f_1 + \dots + f_k$$

其中  $k$  是  $f$  的最高次数. 那么有

$$f(tx_1, tx_2, \dots, tx_n) = f_0(x_1, \dots, x_n) + t f_1(x_1, \dots, x_n) + \dots + t^k f_k(x_1, \dots, x_n)$$

这是一个  $F[x_1, x_2, \dots, x_n]$  上的关于  $t$  的多项式. 若有  $f(tx_1, tx_2, \dots, tx_n) = t^m f(x_1, x_2, \dots, x_n)$ , 对比系数知  $f = f_m$ .  $\square$

#### 7. (习题 2.4.3)

设  $F$  是一个域,  $K \supseteq F$  是  $F$  的一个扩域, 试证明:  $a \in K$  是多项式  $f(x) \in F[x]$  的重根  $\Leftrightarrow f(a) = 0, f'(a) = 0$ .

*proof*

” $\Rightarrow$ ” 的部分按定义直接验证, 下证” $\Leftarrow$ ”:

由  $f(a) = 0$ , 可以得到  $f(x) = (x-a)f_1(x)$ . 那么  $f'(x) = f_1(x) + (x-a)f_1'(x)$ .

由  $f'(a) = f_1(a) = 0$ , 得到  $f_1(x) = (x-a)f_2(x)$ . 因此  $f(x) = (x-a)^2 f_2(x)$ , 即  $a$  是重根.  $\square$

#### 8. (习题 2.4.4)

设  $F$  是一个无限域,  $f(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$  是一非零多项式. 试证明: 存在  $a_1, a_2, \dots, a_n \in F$ , 使  $f(a_1, a_2, \dots, a_n) \neq 0$ .

*proof*

对  $n$  归纳.

$n = 1$  时,  $f(x_1)$  至多有  $\deg(f)$  个根, 由  $F$  无限, 存在  $a_1 \in F$  使得  $f(a_1) \neq 0$ .

现假设结论对  $n$  成立, 考虑多项式

$$f(x_1, \dots, x_n, x_{n+1}) \in F[x_1, \dots, x_n, x_{n+1}] = F[x_1, \dots, x_n][x_{n+1}].$$

从而

$$f(x_1, \dots, x_n, x_{n+1}) = c_m(x_1, \dots, x_n)x_{n+1}^m + \dots + c_0(x_1, \dots, x_n)$$

其中  $c_m(x_1, \dots, x_n) \neq 0$ . 由归纳假设存在  $(a_1, \dots, a_n) \in F^n$  使得  $c_m(a_1, \dots, a_n) \neq 0$ , 那么对多项式  $g(x_{n+1}) = f(a_1, \dots, a_n, x_{n+1}) \in F[x_{n+1}]$  使用  $n = 1$  的结论即可.  $\square$

### 9. (习题 2.4.5)

设  $\psi : R \rightarrow A$  是环同态,  $u = (u_1, u_2, \dots, u_n) \in A^n$  满足:

$$u_i u_j = u_j u_i, \quad u_i \psi(a) = \psi(a) u_i \quad (\forall a \in R, 1 \leq i, j \leq n).$$

请直接验证取值映射  $\psi_u : R[x_1, x_2, \dots, x_n] \rightarrow A$ ,

$$f = \sum_{i_1 i_2 \dots i_n} a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \mapsto \psi_u(f) := \sum_{i_1 i_2 \dots i_n} \psi(a_{i_1 i_2 \dots i_n}) u_1^{i_1} u_2^{i_2} \dots u_n^{i_n},$$

是一个环同态.

*proof*

参考 2.3.7, 实际上这题是把条件减到了最弱的情况, 取定的  $n$  个  $A$  中的  $u_1, u_2, \dots, u_n$ , 只需要它们互相之间是交换的且和所有  $\psi(a)$  也是交换的 (也就是说  $\forall i, u_i \in C(\psi(R))$ , 中心化子, 见 1.2.4), 那么映射

$$\psi_u : R[x_1, \dots, x_n] \rightarrow A, \quad x_i \mapsto u_i, \quad \psi_u|_R = \psi$$

就是环同态. 交换的条件是用于保持乘法上, 保 1 是平凡的, 保加法只需要分配律. 但要注意, 此时不能说  $A$  是  $R$ -代数, 因为按定义是要求任意给定  $u_1, \dots, u_n$ ,  $\psi_u$  都是同态, 才能说  $A$  是一个  $R$ -代数.  $\square$

### 10. (习题 2.4.6)

设  $K$  是一个域,  $A = \{(a_{ij})_{n \times n} | a_{ij} \in K[\lambda]\}$  是  $n$  阶  $\lambda$ -矩阵环,  $u = \lambda \cdot I_n \in A$  表示对角线上全为  $\lambda$  的矩阵. 试证明: 如果  $R = M_n(K)$ ,  $\psi : R \rightarrow R$  是恒等映射, 则取值映射  $\psi_u : R[x] \rightarrow A$  是一个环同构.

*proof*

按定义  $A = M_n(K[\lambda])$ , 由于  $K \subseteq K[\lambda]$ , 所以自然有  $R = M_n(K) \subseteq M_n(K[\lambda]) = A$ . 但事实上  $A = R[\lambda]$ , 在 1.2.8 可以看到这一点. 但是对一个矩阵  $B \in M_n(K)$ ,  $B\lambda$  和  $B(\lambda \cdot I_n)$  是一样的. 因此  $A = R[\lambda \cdot I_n] = R[u]$ .  $u$  和  $\lambda, x$  一样是和  $R$  无关的变量, 所以只是换了个字母而已, 那么  $\psi_u$  自然是同构.  $\square$

### 11. (习题 2.4.7)

设  $R$  是一个无零因子的非交换环,  $\psi: R \rightarrow R$  是恒等映射. 证明存在  $u \in R$  使得  $\psi_u: R[x] \rightarrow R, f(x) \mapsto f(u)$ , 不是一个映射.

*proof*

由非交换性知存在  $u, v \in R$  使得  $uv \neq vu$ . 而  $R[x]$  关于  $x$  是交换的, 所以可以取  $f(x) = vx = xv$ . 那么带入  $u$ , 有  $uv$  和  $vu$  两个值, 因此  $\psi_u$  在  $f(x)$  处不是良定义的,  $\psi_u$  不是一个映射.  $\square$

## 12. (习题 2.4.8)

设  $K$  是一个域,  $M_m(K)$  是  $m$ -阶矩阵环,  $\psi: K \rightarrow M_m(K)$  定义为  $\psi(a) = a \cdot I_m$  (对角线元素为  $a$  的数量矩阵). 令

$$u = (A, B) \in M_m(K) \times M_m(K), \quad AB \neq BA,$$

试证明  $\psi_u: K[x_1, x_2] \rightarrow M_m(K), f(x_1, x_2) \mapsto f(A, B)$ , 不是一个映射.

*proof*

和上题是类似的, 用于赋值的  $A$  和  $B$  是非交换的, 但  $x_1$  和  $x_2$  是交换的. 所以取  $f(x_1, x_2) = x_1x_2 = x_2x_1$  即可.  $\square$

**注:**

现在把涉及到多项式环的题目放在一起看, 2.3.7, 2.4.5, 2.4.6, 2.4.7, 2.4.8.

我们希望“多项式”可以满足我们一直以来的直觉, 其中最重要的一条应该是可以赋值, 也就是说我们希望一个多项式同时也是一个多项式函数. “赋值”这个操作在 2.3.7 解释为由环同态  $\psi: R \rightarrow A$  诱导的唯一的同态  $\psi_u: R[x] \rightarrow A$ ,  $\psi_u$  的含义就是代入  $u$ , 也就是说此时多项式  $f(x)$  确实是一个函数

$$f: R \rightarrow A, \quad u \mapsto f(u) = \psi_u(f(x)).$$

可以看到交换环的条件在多项式里是很重要的, 没有交换环, 多项式就不一定是函数了, 2.4.7 和 2.4.8 分别为一元和多元的反例.

$R[x_1, x_2, \dots, x_n]$  要求所有未定元  $x_1, x_2, \dots, x_n$  是两两交换, 以及所有  $x_i$  要和  $R$  中所有元素交换. 可以看到  $R$  是交换环等价于  $R[x]$  是交换环, 自然也等价于  $R[x_1, x_2, \dots, x_n]$  是交换环.  $R$  是交换环的时候,  $R[x_1, x_2, \dots, x_n]$  的结构已经很清楚, 就是自由交换  $R$ -代数, 它满足和其他自由对象类似的泛性质, 正是这个泛性质保证了赋值的唯一性, 从而多项式函数才是一个良定义的东西.

2.4.5 虽然减弱了条件, 但也失去了一般性, 所以  $R$  非交换的时候, 就没有那么好的泛性质了. 这也是为什么在定义  $R$ -代数的时候需要要求  $R$  是一个交换环.

而 2.4.6 其实有更深刻的含义. 泛性质有很多, 某个特定对象的泛性质都是“对任意的一些态射, 存在唯一的态射使得图表交换”这种形式. 这其实是和 Yoneda Lemma, representable functor, limit 等有关系. 这种对象其实是某个新的范畴

里的 final object(或者 initial object, 这俩是对偶的, 就差一个反范畴). 而 final object 的定义里就是该范畴里一个特殊的对象: 任意对象到 final object 存在唯一的态射. 正是这个存在唯一, 保证了 final object 在同构的意义下是唯一的. 所以当有两个东西满足同一个泛性质, 它们俩一定是同构的.

## 课上的补充内容

感觉就是  $R[x_1, \dots, x_n]$  的泛性质吧...

代数里是有很多这样的抽象废话, 理解起来需要亿点时间.