第六周作业参考解答及补充

作业

1. (习题 2.3.2)

设 F 是一个域, $p(x) \in F[x]$ 不可约, 令 $I = p(x)F[x]$ 表示由 $p(x)$ 生成的理想, 试证明：商环 $F[x]/I$ 是一个域, 且环同态

$$\varphi : F[x] \to F[x]/I, \quad f(x) \mapsto \overline{f(x)}$$

诱导了域嵌入 $\varphi|_F : F \hookrightarrow F[x]/I, a \mapsto \bar{a}$ (如果将 F 与它的像等同, 则 $\bar{x} \in F[\bar{x}] := F[x]/I$ 是 $p(x)$ 在扩域 $F[\bar{x}]$ 中的一个根).

proof

2.2.6 注记的最后已经提到过, 这里再详细解释一下. 由于 F 是域, 因此 $F[x]$ 是 PID, 因此若 $p(x)$ 是不可约的, 则 $I = p(x)F[x]$ 是极大理想. 因为不可约元按定义在所有主理想中是极大的, 这一点可以参考 2.2.2 的注记, 设 p 是不可约元就能得到

$$(p) \subseteq (p') \implies p' \mid p \implies p' \sim p \text{ 或} p' \sim 1 \implies (p') = (p) \text{ 或} (p') = (1)$$

. 因此由 2.1.6 知 $F[x]/I$ 是域.
所谓的域嵌入 (embbeding) 在这里实际上就是单同态, 这其实就是同态复合了一下

$$F \longhookrightarrow F[x] \longrightarrow\!\!\!\!\!\rightarrow F[x]/I$$

这是域之间的同态, 因此一定是单的. $\square$

2. (习题 2.3.3)

设 F 是一个域, $K \subset F$ 是一个子域, $f(x), g(x) \in K[x]$. 试证明：$f(x)$, $g(x)$ 在 $K[x]$ 中互素 $\Leftrightarrow$ $f(x)$, $g(x)$ 在 $F[x]$ 中互素.

proof

利用 PID 上满足 Bézout Identity 立得. 注意到和 2.2.1 不同的是, 互素的时候两个条件等价. $\square$

3. (习题 2.3.4)

设 F 是特征零的域, $f(x) \in F[x]$ 不可约. 证明 $f(x)$ 与 $f'(x)$ 互素.

proof

由于 $0 \leqslant \deg(f') < \deg(f)$ 且 f 不可约，若有非单位的公因式 $d(x)$，则 $\deg(f) > \deg(f') \geqslant \deg(d) > 0$ 且 $d(x) \mid f(x)$ 与不可约矛盾.

特征零是为了排除 $f' = 0$ 的情况. □

4. (习题 2.3.5)

设 $\mathbb{F}_2 = \mathbb{Z}/(2) = \{\bar{0}, \bar{1}\}$ 是一个二元域. 证明：

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}_2[x]$$

没有一次因子 (即不被一次多项式整除) $\Leftrightarrow a_n \left(1 + \sum_{i=1}^{n} a_i\right) \neq 0$. 写出 $\mathbb{F}_2[x]$ 中所有次数不超过 3 的所有不可约多项式.

proof

$\mathbb{F}_2$ 只有两个一次多项式 x 和 $x+1$. 其中比较简单的是

$$x \mid f(x) \iff a_0 = 0,$$

另一个

$$x + 1 \mid f(x) \iff f(x) = (x+1)g(x)$$

设 $g(x) = x^{n-1} + \cdots + b_{n-1}$, 对比系数

$$a_n = b_{n-1},\ a_{n-1} = b_{n-1} + b_{n-2},\ \cdots,\ a_1 = b_1 + 1$$

由于 $\mathbb{F}_2$ 里 $-1 = 1$, 因此可以得到

$$b_1 = a_1 - 1 = a_1 + 1,\ b_2 = a_2 - b_1 = a_2 + a_1 + 1,\ \cdots,\ a_n = b^{n-1} = 1 + \sum_{k=0}^{n-1} a_k$$

因此

$$x + 1 \mid f(x) \iff 1 + \sum_{k=1}^{n} = 2a_n = 0.$$

不过也可以不这么麻烦，一次多项式对应 $f(x)$ 的根，所以 $f(x)$ 无一次因子等价于 $f(0) \neq 0$ 且 $f(1) \neq 0$, 即 $a_0 \neq 0$ 和 $1 + \sum_{k=1}^{n} a_k \neq 0$.

次数不超过 3 的多项式只有有限个，可以列举出来，去掉比较明显的可约多项式

$$\begin{aligned} &x,\ x+1, \\ &x^2+1,\ x^2+x+1 \\ &x^3+1,\ x^3+x+1,\ x^3+x^2+1 \end{aligned}$$

注意 $x^2 + 1 = x^2 - 1 = (x-1)(x+1) = (x+1)^2$ 可约, $x^3 + 1$ 同理, 其余五个为不可约多项式. □

5. (习题 2.3.6)

设 p 是素数, $\mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/(p)\mathbb{Z}$, $a \mapsto \bar{a}$, 是商同态. 证明：

(1) 映射

$$\phi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x], \quad f(x) = \sum_{i=1}^{n} a_i x^i \mapsto \bar{f}(x) = \sum_{i=1}^{n} \bar{a}_i x^i$$

是环同态;

(2) 对于首项系数为 1 的多项式 $f(x) \in \mathbb{Z}[x]$, 如果存在素数 p 使 $\bar{f}(x)$ 在 $\mathbb{F}_p[x]$ 中不可约, 则 $f(x)$ 在 $\mathbb{Z}[x]$ 中也不可约.

proof

(1) 2.1.8 的注记或教材引理 2.3.2(原来教材有写延拓)

(2) 用反证法, 假设 $f(x)$ 可约, $f(x) = g(x)h(x)$, 则 $\deg(g), \deg(h) > 0$ 且 g, h 都是首一的. 那么根据同态有 $\bar{f} = \bar{g}\bar{h}$, 且 $\bar{g}$ 和 $\bar{h}$ 还是首一的次数大于 0 的多项式, 这和 $\bar{f}$ 不可约矛盾.

$\square$

6. (习题 2.3.7)

设 R, A 是两个环, $C(A) \subset A$ 是 A 的中心, $\psi : R \to C(A)$ 是一个环同态. 证明：$\forall u \in A$, 存在唯一环同态 $\psi_u : R[x] \to A$ 满足：

$$\psi_u(x) = u, \quad \psi_u(a) = \psi(a) \quad (\forall a \in R).$$

所以, $\forall f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, 它在 ψ_u 下的像

$$\psi_u(f(x)) = \psi(a_n)u^n + \psi(a_{n-1})u^{n-1} + \cdots + \psi(a_1)u + \psi(a_0) \in A$$

称为 $f(x)$ 在 $u \in A$ 的取值, 记为 $f(u) := \psi_u(f(x))$.

proof

2.1.8 的注记. 在这里重新阐述的详细一点. 给定环同态 $\psi : R \to C(A)$, 我们可以指定一个集合的映射

$$f_u : \{1\} \to A, 1 \mapsto u$$

所谓的自由交换 R-代数的泛性质是指, 对任意给定的集合映射 f_u, 存在唯一

的同态 $\psi_u: R[x] \to A$ 使得图表交换:

$$\begin{tikzcd} R[x] \arrow[rr, "\exists! \psi_u"] & & A \\ & \{1\} \arrow[ul, "i"] \arrow[ur, "f_u"'] & \end{tikzcd}$$

其中 $i: R \to R[x], 1 \mapsto x$.
因为 $\psi(R) \subseteq C(A)$, 因此 ψ_u 才能保持乘法, 这在 2.1.8 的注记里已经证明.
验证了 ψ_u 是环同态就相当于证明了存在性, 而唯一性是根据定义就能得到, ψ_u 是被给定的 ψ 和 f_u 唯一确定的. □

注:

这里 $\{1\}$ 可以换成任意集合 S

$$\begin{tikzcd} R[S] \arrow[rr, "\exists! \psi_u"] & & A \\ & S \arrow[ul, "i"] \arrow[ur, "f_u"'] & \end{tikzcd}$$

7. (习题 2.3.8)

设 R 是一个交换环, $f(x) \in R[x]$. 证明：$f(x)$ 是环 $R[x]$ 中的零因子当且仅当存在 $0 \neq r \in R$ 使得 $r \cdot f(x) = 0$.

proof

由于 $R \subseteq R[x]$, 只需证" $\Longrightarrow$ " 的方向.
记 $f(x) = \sum_{k=0}^{n} a_k x^k$, 设存在 $g(x) = \sum_{k=0}^{m} b_k x^k \neq 0$ 使得 $fg = 0$, 并要求 $g(x)$ 是次数最低的. 考虑最高次项, $a_n b_m = 0$. 那么 $a_n g(x)$ 是一个比 $g(x)$ 次数更小的多项式且 $f(x)(a_n g(x)) = a_n f(x) g(x) = 0$. 因此 $a_n g(x) = 0$, 从而 $a_n b_k = 0, 0 \leqslant k \leqslant m$. 那么此时 $n+m-1$ 项的系数变为 $a_{n-1} b_m = 0$, 于是可以重复讨论. 根据归纳法最后得到 $a_i b_m = 0, \forall i$ 且 $b_m \neq 0$, 因此 $b_m f(x) = 0$.
□

课上的补充内容

無い, たぶん…