第五周作业参考解答及补充

作业

1. (习题 2.1.3)

证明：只有有限个元素的整环一定是一个域.

proof

整环 R 有乘法消去律 (习题 1.1.1 的 (1), 证明乘法消去律事实上只需要分配律加无零因子), 而习题 1.3.9 告诉我们, 满足消去律的有限半群是群. 因此 $(R\setminus\{0\},\cdot)$ 是群, 即 R 是一个域. □

2. (习题 2.1.4)

证明：只有有限个理想的整环是一个域.

proof

事实上条件可以再减弱一点, 一个 Artin 整环一定是域.

设 $a\neq 0$, 考虑理想降链

$$(a)\supseteq(a^2)\supseteq\cdots$$

因此 $\exists n\in\mathbb{Z}_{>0}$, $(a^n)=(a^{n+1})$. 即有 $a^n\in(a^{n+1})$, 那么 $\exists b\in R$, $a^n=a^{n+1}b$, 从而 $ab=1_R$. □

注:

Artin 环定义为任意理想降链稳定的环, i.e. 若有理想降链

$$I_1\supseteq I_2\supseteq\cdots$$

则存在 $n\in\mathbb{Z}_{>0}$ 使得 $\forall m>n$, $I_m=I_n$, 也就是说从某一个 n 开始就稳定了 $I_n=I_{n+1}=\cdots$. 这个条件称为 descending chain condition(d.c.c.), 与之对应的是 ascending chain condtion(a.c.c.), 满足 a.c.c. 的正是 Noether 环.

3. (习题 2.1.9)

映射 $D:R[x]\longrightarrow R[x]$ 定义如下：$\forall f(x)=a_nx^n+\cdots+a_1x+a_0$,

$$D(f)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1.$$

$\forall\, a\in R$, $f,g\in R[x]$, 试证明：

(1) $D(f+g)=D(f)+D(g)$, $D(af)=aD(f)$;

(2) $D(f\cdot g)=D(f)\cdot g+f\cdot D(g)$.

($D(f)$ 称为 $f(x)$ 的导数. 记为 $f'(x)=D(f)$, $f^{(m)}(x)=\overbrace{D\cdots D}^{m}(f)$ 称为 $f(x)$ 的 m 次导数).

proof

按定义验证. 设 $f=a_nx^n+\cdots+a_1x+a_0$, $g=b_mx^m+\cdots+b_1x+b_0$.

(1) 不妨设 $n\geqslant m$, 且令 $b_k=0, k>m$.

$$\begin{aligned}D(f+g)&=D\left(\sum_{k=0}^{n}(a_k+b_k)x^k\right)=\sum_{k=1}^{n}k(a_k+b_k)x^{k-1}\\&=\sum_{k=1}^{n}ka_kx^{k-1}+\sum_{k=1}^{m}kb_kx^{k-1}=D(f)+D(g).\end{aligned}$$

$$D(af)=D\left(\sum_{k=0}^{n}aa_kx^k\right)=\sum_{k=1}^{n}kaa_kx^{k-1}=a\sum_{k=1}^{n}ka_kx^{k-1}=aD(f).$$

这里能把 a 提出来是因为 k 作为 $k1_R$(见习题 1.2.1 的新增的注记), 有 $ka=ak$.

(2)

$$\begin{aligned}D(f\cdot g)&=D\left(\sum_{k=0}^{n+m}\sum_{i+j=k}a_ib_jx^k\right)=\sum_{k=1}^{n+m}\sum_{i+j=k}ka_ib_jx^{k-1}\\&=\sum_{k=1}^{n+m}\sum_{i+j=k}(i+j)a_ib_jx^{i+j-1}\\&=\sum_{k=1}^{n+m}\sum_{i+j=k}(ia_ix^{i-1})b_jx^j+a_ix^i(jb_jx^{j-1})\\&=\sum_{k=0}^{n+m-1}\sum_{(i-1)+j=k}(ia_i)b_jx^k+a_i(jb_j)x^k\\&=D(f)\cdot g+f\cdot D(g).\end{aligned}$$

□

4. (习题 2.1.10)

如果 F 是特征零的域, 则 $f'(x)=0\Leftrightarrow\deg(f)=0$ 或 $f(x)=0$(即常数); 如果 F 的特征是 $p>0$, 则 $f'(x)=0\Leftrightarrow$ 存在 $g(x)\in F[x]$ 使得 $f(x)=g(x^p)$.

proof

$\mathrm{Char}(F)=0$, 即 $\forall n\in\mathbb{Z}_{>0}, n\neq 0$(这里 n 看做 $n1_F$, 见习题 1.2.1 的新增的

注记), 那么

$$f'(x) = na^{n-1} + \cdots + a_1 = 0 \implies 1 \leqslant k \leqslant n, ka_k = 0 \implies 1 \leqslant k \leqslant n, a_k = 0$$

故 $f(x) = a_0$, $\deg(f) = 0$ 或 $f = 0$, 反过来是平凡的.
若 $\mathrm{Char}(F) = p$, 则 $p = 0$, 那么设 $\deg(f) = n = kp + r, 0 \leqslant r < p, k \in \mathbb{N}$,

$$\begin{aligned} & f = a_0 + a_1 x + \cdots a_p x^p + \cdots + a_{2p} x^{2p} + \cdots + a_{kp} x^{kp} + a_n x^n. \\ \implies & f' = a_1 + \cdots + p a_p x^{p-1} + \cdots + kp a_{kp} x^{kp-1} + \cdots n a_n x^{n-1} \\ & \quad = a_1 + \cdots + (p-1) a_{p-1} x^{p-2} + (p+1) a_{p+1} x^p + \cdots (kp-1) a_{kp-1} x^{kp-2} \\ & \quad + (kp+1) a_{kp+1} x^k p + \cdots + n a_n x^{n-1}. \end{aligned}$$

此时 $f' = 0$ 有 $f = a_0 + a_p x^p + \cdots + a_{kp} x^{kp} = g(x^p)$. 这里 $g = a_0 + a_p x + \cdots + a_{kp} x^k$. 反过来也是类似的. □

5. (习题 2.2.1)

设 m, n 是两个正整数, 证明它们在 $\mathbb{Z}$ 中的最大公因数和它们在 $\mathbb{Z}[i]$ 中的最大公因数相同.

注意这里的相同指的在相伴的意义下相同.

proof

由于 $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, 在相伴的意义下, 可以假设 (m, n) 在 $\mathbb{Z}$ 和 $\mathbb{Z}[i]$ 中都是正整数, 分别记为 d 和 d'.
那么 PID 上 Bézout's Identity 成立, 有

$$d = mu + nv, \quad d' = m\alpha + n\beta.$$

其中 $u, v \in \mathbb{Z}$, $\alpha, \beta \in \mathbb{Z}[i]$. 设 $\alpha = a_1 + ia_2$, $\beta = b_1 + ib_2$, 由于我们假设的是 $d' \in \mathbb{Z}_{>0}$, 故 $d' = ma_1 + nb_1$, 从而 $d \mid m, d \mid n \implies d \mid d'$. 反过来也有 $d' \mid d$, 所以 $d = d'$. □

6. (习题 2.2.6)

令 $\mathbb{R}, \mathbb{C}$ 分别表示实数域和复数域, 试证明:

(1) 若 R 是由关于 $\cos t$ 和 $\sin t$ 的实系数多项式组成的函数环, 则 $R \cong \mathbb{R}[x, y]/(x^2 + y^2 - 1)$;

(2) $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ 是唯一分解整环 (提示: 证明其为 ED);

(3) $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ 不是唯一分解整环.

proof

(1) 考虑同态

$$\varphi : \mathbb{R}[x,y] \to R = \mathbb{R}[\cos t, \sin t],\ x \mapsto \cos t, y \mapsto \sin t,$$

这自然是一个满同态, 由同态基本定理, 关键在于证明

$$\ker(\varphi) = (x^2 + y^2 - 1)$$

若多项式 $f(x,y)$ 满足 $\varphi(f) = f(\cos t, \sin t) = 0$, 将 f 看成是关于 y 的多项式

$$f(x,y) = a_0(x) + a_1(x)y + \cdots + a_n(x)y^n,\ a_i(x) \in \mathbb{R}[x],\ 0 \leqslant i \leqslant n$$

由于 x^2+y^n-1 关于 y 是首一的, 因此可以做带余除法, 得 $f = gq+r$, 其中 $r(x,y) = r_0(x) + r_1(x)y$. 带入 $x = \cos t, y = \sin t$ 得 $r(\cos t, \sin t) = 0$, 即

$$r_0(\cos t) + r_1(\cos t)\sin t = 0$$

做代换 $t \mapsto -t$, 得

$$r_0(\cos t) - r_1(\cos t)\sin t = 0$$

两式相加得 $r_0 = 0$, 相减得 $r_1 = 0$, 从而 $r = 0$. 因此 $f \in (x^2 + y^2 - 1)$, 即 $\ker(\varphi) \subseteq (x^2 + y^2 - 1)$. 另一方面 $x^2 + y^2 - 1 \in \ker(\varphi)$, 故 $\ker(\varphi) = (x^2 + y^2 - 1)$

(2) 做基变换 $u = x + iy, v = x - iy$, 他有逆变换 $x = \dfrac{u+v}{2}, y = \dfrac{u-v}{2i}$. 因此有同构 $\mathbb{C}[u,v] \cong \mathbb{C}[x,y]$. 从而

$$\mathbb{C}[x,y]/(x^2 + y^2 - 1) \cong \mathbb{C}[u,v]/(uv - 1)$$

而同态

$$\mathbb{C}[u,v] \to \mathbb{C}[u,u^{-1}],\ u \mapsto u, v \mapsto u^{-1}$$

是满的, 且 kernel 是 $(uv-1)$, 证明类似于 (1). 因此

$$\mathbb{C}[u,v]/(uv - 1) \cong \mathbb{C}[u,u^{-1}]$$

这个环称为 Laurent 多项式环, 这个环上可以做带余除法, 非零多项式的次数定义为最高次数 $-$ 最低次数. 即 $f = a_n u^n + a_{n+1}u^{n+1} + \cdots + a_m u^m, n, m \in \mathbb{Z}, n < m$ 的次数为 $\deg(f) = m - n$. 因此这是一个 ED, 从而是 UFD.

(3) 由 (2), $\mathbb{C}[\cos t, \sin t]$ 是 UFD, 用待定系数, 假设

$$\cos t = (a_1 \cos t + a_2 \sin t + a_3)(b_1 \cos t + b_2 \sin t + b_3)$$

其中 $a_i, b_i \in \mathbb{C}, i = 1, 2, 3$. 我们要忽略掉 $a_1 = b_3 = 1$ 其余都是 0 这种平凡的情况, 左右展开得到

$$\begin{aligned} a_1 b_1 - a_2 b_2 &= 0, \\ a_1 b_2 + a_2 b_1 &= 0, \\ a_1 b_1 + a_3 b_3 &= 0, \\ a_1 b_3 + a_3 b_1 &= 1, \\ a_2 b_3 + a_3 b_2 &= 0. \end{aligned}$$

由第一个式子得 $b_1 = \dfrac{a_2}{a_1} b_2$, 带入第二个式子得 $a_2 = \pm i a_1$, 从而 $b_1 = \pm i b_2$.

由一, 三又能得到 $a_2 b_2 = -a_3 b_3$, 类似地, 带入第五个式子, 有 $a_3 = \pm a_2$, $b_2 = \pm b_3$.

再用四, 五得 $a_1 b_3 = a_3 b_1 = \dfrac{1}{2}$.

把上述关系带入

$$\begin{aligned} \cos t &= a_1 b_3 (\cos t \pm i \sin t \pm i)(\pm i \cos t \pm \sin t + 1) \\ &= \frac{1}{2}(\cos t \pm i \sin t \pm i)(\pm i \cos t \pm \sin t + 1) \end{aligned}$$

检查正负号, 得到结果

$$\cos t = \frac{1}{2}(\cos t + i \sin t - i)(i \cos t + \sin t + 1)$$

类似有

$$1 - \sin t = \frac{1}{2}(\cos t + i \sin t - i)(\cos t - i \sin t + i).$$

带入 $-t$ 就是 $1 + \sin t$ 的分解.

但这种方法比较难检查等式右边的因式确实为不可约元, 我们可以利用同构 $\mathbb{C}[x, y]/(x^2 + y^2 - 1) \cong \mathbb{C}[u, u^{-1}]$, 那么等式变为

$$x = \frac{1}{2}(u + u^{-1}) = \frac{u^{-1}}{2}(u - i)(u + i)$$

注意到 $U(\mathbb{C}[u, u^{-1}]) = \mathbb{C} \cup \{u^n \mid n \in \mathbb{Z}\}$. 右边为两个都是一次的且常数项不为 0, 容易验证不可逆 (注意这里 $x = \dfrac{1}{2}(u + u^{-1})$ 次数为 2). 对 $1 - \sin t$ 同理.

因此 $\cos t$ 和 $1 \pm \sin t$ 无法在 $\mathbb{R}[\cos t, \sin t]$ 中分解 (分解出的系数中一定带 i). 这样就有 $\cos^2 t = \cos t \cos t = (1 - \sin t)(1 + \sin t)$. 因此不是 UFD.

□

注:

(2) 中若允许正次数到无穷的话, 则该环称为 Laurent 形式级数域 (可以验证确实是一个域).

另外, 可以说 x^2+y^2-1 是单位圆的" 极小多项式". 但这种说法是有些不合理的, 因为这样 $a_{ij}x^iy^j$ 次数将定义成 $i+j$, $f(x,y)$ 的次数定义成单项次数的最大值, 一旦这么定义就无法做带余除法, 就无法得到满足某个点集 (一般是代数集, 即某些多项式的共同零点) 的多项式是其极小多项式的倍数.

一般地设 k 是一个域, $S\subseteq k[x_1,x_2,\cdots,x_n]$, 那么可以定义 S 中所有多项式的公共零点集

$$Z(S)=\{(a_1,a_2,\cdots,a_n)\in k^n\mid \forall f\in S,\ f(a_1,a_2,\cdots a_n)=0\}$$

按定义有 $S\subseteq S'\implies Z(S')\subseteq Z(S)$. 考虑 S 生成的理想 $I=(S)$(见**??**的注记), 则有 $Z(I)\subseteq Z(S)$. 另一方面, 根据 $I=\left\{\sum f_ig_i\middle| f_i\in k[x_1,x_2,\cdots,x_n],g_i\in S\right\}$, 立刻得到 $Z(S)\subseteq Z(I)$. 从而 $Z(S)=Z(I)$. 我们称 $Z(S)$ 这种点集为代数集 (algebraic set), 用 $\mathbb{A}_k^n$ 代替的 k^n 表示将它看作一个代数集 (因为按定义 $Z(\varnothing)=k^n$), 而 Hilbert's Basis Theorem 告诉我们 $k[x_1,x_2,\cdots,x_n]$ 是 Noether 环, 所以理想都是有限生成的, 那么总有 $Z(I)=Z(f_1,f_2,\cdots,f_r)$.

反过来, 对 $X\subseteq\mathbb{A}_k^n$, 定义

$$\mathscr{I}(X)=\{f\in k[x_1,x_2,\cdots x_n]\mid \forall(a_1,a_2,\cdots a_n)\in X, f(a_1,a_2,\cdots a_n)=0\}$$

可以验证 $\mathscr{I}(X)$ 是根理想 (**??**的注记). 当 k 是代数闭域 (algebraic closed field) 时, 有一一对应

$$\{\mathbb{A}_k^n\text{ 的代数集}\}\underset{Z}{\overset{\mathscr{I}}{\rightleftarrows}}\{k[x_1,x_2,\cdots x_n]\text{ 的根理想}\}$$

这就是 Strong Nullstellensatz.

那么 (1) 中 $I=(x^2+y^2-1)$, $Z(I)=\{(x,y)\in\mathbb{R}^2\mid\forall f\in I,\ f(x,y)=0\}=\{(x,y)\in\mathbb{R}^2\mid x^2+y^2=1\}$, 恰好是单位圆. 那么 (1) 的关键在于说明 $\mathscr{I}(Z(I))=I$. 可惜的是一般情况下这个并不成立, 比如还是在 $\mathbb{R}[x,y]$ 上考虑, 记 $J=(x^2+y^2)$, 那么 $Z(J)=(0,0)$, $\mathscr{I}(Z(J))=(x,y)\neq J$. 这里 x^2+y^2 是不可约的, 所以即使是单独一个不可约多项式也不一定可以有这个等式, x^2+y^2-1 这个不可约多项式还是比较特殊的.

域扩张中的极小多项式和不可约是一样的, 这是由于 $K[x]$ 是一个 PID, 不可约元对应极大理想, 从而对应极小多项式.

课上的补充内容

1. (Noetherian $\iff$ a.c.c.)

R 是诺特环当且仅当 R 满足 a.c.c.

其中 a.c.c. 指若有环 R 的理想升链

$$I_1 \subseteq I_2 \subseteq \cdots$$

则该链必稳定, 即 $\exists n \in \mathbb{Z}_{>0}$ 使得 I_n 后的理想都相等, $I_n = I_{n+1} = \cdots$.