第三周作业参考解答及补充

教材的符号有不清晰的地方, 主要是素理想那一块, 我进行了修正, 用 $\subseteq$ 表示子集, $\subsetneq$ 表示真子集.

作业

1. (习题 2.1.1)

设 R 是一个交换环, $I \subset R$ 是一个理想. 证明

$$\sqrt{I} = \{r \in R \mid \exists m \in \mathbb{N} \text{ 使得} r^m \in I\}$$

也是 R 的理想 (称为理想 I 的根).

注: 这题的根理想定义有误, 应是 $\mathbb{N}$ 而不是 $\mathbb{Z}$. 一旦出现负整数意味着有可逆元, 从而 $\sqrt{I}$ 是单位理想了.

proof

可以清楚地看出 $I \subseteq \sqrt{I}$. 先验证加法子群,

$$\begin{aligned} \forall a, b \in \sqrt{I},\ \exists m, n \in \mathbb{N},\ a^m, b^n \in I, \\ \implies (a-b)^{m+n} \in I \end{aligned}$$

这是因为单项 $a^i b^j$ 的指数 $i + j = m + n$, 故 $i < m$ 和 $j < n$ 不能同时成立, 即 $i \geqslant m$ 或 $j \geqslant n$, i.e. $a^i \in I$ 或 $b^j \in I$. 从而 $(a-b)^{m+n} \in I$, $a - b \in \sqrt{I}$.
再验证吸收律 (交换验证单边即可),

$$\forall a \in \sqrt{I}, r \in R,\ \exists m \in \mathbb{N},\ a^m \in I \implies (ar)^m = a^m r^m \in I$$

因此 $ar \in \sqrt{I}$.
注: 零理想的根 $\sqrt{\{0\}} = \{x \in R \mid \exists n \in \mathbb{N}, x^n = 0\}$ 是所有幂零元 (nilpotent) 组成的理想, 叫做 R 的幂零根 (nilradical), 一般记作 $\mathfrak{N}(R)$. 可以证明 $\mathfrak{N}(R) = \bigcap\limits_{\mathfrak{p} \text{ 是素理想}} \mathfrak{p}$.

2. (习题 2.1.2)

设 R 是一个交换环, $p > 0$ 是一个素数. 如果 $p \cdot x = 0 (\forall x \in R)$. 试证明: $(x+y)^{p^m} = x^{p^m} + y^{p^m} (\forall x, y \in R, m > 0)$

proof

事实上, 这个 p 就是环 R 的特征. 若 $\mathrm{Char}(R) \neq p$, 则由 $p1_R = 0_R$, $\mathrm{Char}(R) < p$. 那么 $(p, \mathrm{Char}(R)) = 1$, 有 Bezout's Theorem 得到 $1_R = 0_R$, 这就没什么考虑的必要了.
对特征 p 的交换环, 有一个特别的同态 F 称为 Frobenius 自同态,

$$F : R \to R, \quad a \mapsto a^p$$

我们说明这确实是一个同态.

保持乘法是因为交换环, 不平凡的是保持加法.

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + b^p.$$

其中 $1 \leqslant i \leqslant$ 时,

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdots i}$$

由于 p 是素数, $1, 2, \cdots i$ 都不整除 p, 而 $\binom{p}{i}$ 是整数, 因此只能是 $i! \mid (p-1)\cdots(p-i+1)$. 所以 $p \mid \binom{p}{i}$. 而 $px = 0$, $\forall x \in R$, 故 $(a+b)^p = a^p + b^p$.

因此 $\varphi : R \to R$, $x \mapsto x^{p^m}$ 也是自同态, $\varphi = F^m$, 这里 F^m 表示复合 m 次.

注: Frobenius 一般在域中使用的多一些. 虽然对交换环 Frobenius 都是可以定义的, 但是整环才能保证 Frobenius 是单射. Frobenius 一般不是满的, 但对有限域就是自同构了.

3. (习题 2.1.5)

理想 $P \subsetneq R$ 称为素理想, 如果: $ab \in P \Rightarrow a \in P$ 或 $b \in P$. 试证明: $P \subsetneq R$ 是素理想当且仅当 R/P 没有零因子.

proof

(1) " $\Longrightarrow$ ":

$$\forall \bar{a}, \bar{b} \in R/P,\ \bar{a}\bar{b} = \overline{ab} = \bar{0} \implies ab \in P \implies a \in P \text{ or } b \in P \implies \bar{a} = \bar{0} \text{ or } \bar{b} = \bar{0}.$$

(2) " $\Longleftarrow$ ":

$$ab \in P \implies \bar{a}\bar{b} = \overline{ab} = \bar{0} \implies \bar{a} = 0 \text{ or } \bar{b} = 0 \implies a \in P \text{ or } b \in P.$$

4. (习题 2.1.6)

理想 $m \subsetneq R$ 称为极大理想, 如果 R 中不存在真包含 m 的非平凡理想 (即: 如果 $I \supsetneq m$ 是 R 的理想, 则必有 $I = R$). 试证明: 当 R 是交换环时, $m \subsetneq R$ 是极大理想当且仅当 R/m 是一个域. 特别, 交换环中的极大理想必为素理想.

proof

(1) " $\Longrightarrow$ ":

$$\begin{aligned}\forall \bar{0} \neq \bar{a} \in R/m \implies a \notin m \implies m \subsetneq m + (a) \implies m + (a) = R = (1) \\ \implies \exists x \in m, b \in R,\ x + ab = 1 \implies \overline{ab} = \overline{1-x} = \bar{1}.\end{aligned}$$

(2) " $\Longleftarrow$ ":

$$\begin{aligned}m \subsetneq I \underset{\text{ideal}}{\subseteq} R \implies \exists a \in I \setminus m \text{ i.e. } \bar{a} \neq 0 \implies \exists b \in R,\ \bar{a}\bar{b} = \overline{ab} = \bar{1} \\ \implies \exists x \in m \subsetneq I,\ ab = 1 + x \implies 1 = ab - x \in I \implies I = (1) = R.\end{aligned}$$

或者用同态基本定理, 包含 m 的理想和 R/m 的理想有一个一一对应, 而域的理想只有 $\{0\}$ 和本身.

注: (1) 中用到了理想的和. 若 I, J 都是 R 的理想, $I+J := \{i+j \mid i \in I, j \in J\}$. 可以验证这确实是一个理想, 类似可以定义一族理想 $\{I_\alpha\}_{\alpha\in A}$ 的和,

$$\sum_{\alpha\in A} I_\alpha = \left\{\sum_{\alpha\in A} i_\alpha \middle| i_\alpha \in I_\alpha,\ \text{且只有有限个} i_\alpha \neq 0\right\}$$

即考虑所有可能的有限和.
另外 $\bigcap\limits_{\alpha\in A} I_\alpha$ 也是一个理想. 还有一个是理想的积, 相对要复杂一些,

$$\begin{aligned} IJ &:= (\{ij \mid i \in I, j \in J\}) \\ &= \left\{\sum_{k=1}^{n} i_k j_k \middle| \exists n \in \mathbb{N},\ 1 \leqslant k \leqslant n,\ i_k \in I, j_k \in J, \right\} \end{aligned}$$

他是所有乘积 ij 生成的理想. 那么一族理想的乘积就是考虑所有可能的有限乘积生成的理想.

5. (习题 2.1.7)

设 $I \subseteq \mathbb{Z}$ 是整数环的非零理想, 证明下述结论等价

(1) I 是极大理想;

(2) I 是素理想;

(3) 存在素数 p 使得 $I = (p)\mathbb{Z} = \{ap \mid \forall a \in \mathbb{Z}\}$.

proof

1. (1) $\implies$ (2): 由于域一定是整环, 由 2.1.5 和 2.1.6 知极大理想是素理想.
2. (2) $\implies$ (3): 由于 $\mathbb{Z}$ 是 PID(带余除法可证), 故存在整数 p 使得 $I = (p)$. 由于是素理想, 因此 $ab \in (p) \implies a \in (p)$ 或 $b \in (p)$. 即

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$

   则 p 是素数 (若不然, $p = qr$, 取 $a = q, b = r$ 即导出矛盾).
3. (3) $\implies$ (1): 设 $I = (p) \subsetneq J$, 则存在 $n \in J \setminus I$. 由于 p 是素数, 故有 $(n, p) = 1$. 由 Bezout's Theorem, $\exists u, v \in \mathbb{Z}$ 使得 $nu + pv = 1$, 从而 $1 \in J$, $J = \mathbb{Z}$.(这和 2.1.6 的证明是类似的)

   或直接用 $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ 是域.

6. (习题 2.1.8)

设 $p \in \mathbb{Z}$ 是素数, 证明 $(p)\mathbb{Z}[x] = \{pf(x) \mid \forall f(x) \in \mathbb{Z}[x]\}$ 是整系数多项式环的素理想, 但不是 $\mathbb{Z}[x]$ 的极大理想.

proof

事实上若 I 是 R 的理想, 我们有

$$\frac{R[x]}{IR[x]} \cong \frac{R}{I}[x]$$

这是根据同态基本定理得到, 考虑同态

$$\varphi : R[x] \to \frac{R}{I}[x], \quad a_0 + a_1x + \cdots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$$

可以验证这确实是一个同态.(事实上, 它是 $R \twoheadrightarrow R/I \hookrightarrow \dfrac{R}{I}[x]$ 的一个延拓.)
回到原题, 有

$$\frac{\mathbb{Z}[x]}{(p)\mathbb{Z}[x]} \cong \mathbb{Z}_p[x]$$

这里 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 是域. 因此 $\mathbb{Z}_p[x]$ 是 PID, 自然是整环, 但不是域 (x 没有逆). 因此由 2.1.5 和 2.1.6, $(p)\mathbb{Z}[x]$ 是素理想但不是极大理想.
注 (这个比较超纲看不懂可以不看): 给定环同态 $R \xrightarrow{\varphi} S$, 其中 R 是交换环. 若 $\varphi(R) \subseteq C(S)$(习题 2.1.11), 根据之前习题 1.4.9 说过的, 首先 S 上有一个 R-模结构. 其次有

$$(r_1s_1)(r_2s_2) = \varphi(r_1)s_1\varphi(r_2)s_2 = \varphi(r_1)\varphi(r_2)s_1s_2 = \varphi(r_1r_2)s_1s_2 = (r_1r_2)(s_1s_2).$$

即数乘和 S 本身的乘法是相容的. 这样的结构我们称为一个 R-代数 (R-algebra), 这也是习题 2.1.12 介绍的东西. 因此一个 R-代数就是带有加法, (R-) 数乘, 乘法的一个代数结构.
当 S 本身就是交换环时, 即乘法是交换的, 且 $C(S) = S$, 此时会变得简单很多. 这时 S 称为一个交换 R-代数, 这也是交换代数会考虑的情形. 我们会把 S 看作一个有序对 (S, φ), 一个交换 R-代数 S 也叫做一个 R-(交换) 环. 那么交换 R-代数构成的范畴是交换环范畴的余切片范畴 (coslice category).
而这里提到的延拓其实是多项式环的泛性质 (universal property), 或者说是自由交换 R-代数的泛性质, 因为 $R[x]$ 就是一个的自由交换 R-代数.

7. (习题 2.2.2)

设 R 是整环, $p \in R$ 称为一个素元如果它生成的理想 $P = (p)R$ 是素理想. 证明：R 中素元必为不可约元.

proof

由定义 $(p) \neq (1)$, 因此 p 不可逆. 设 $p = ab$, 则 $ab \in (p)$, 由素理想知 $a \in (p)$ 或 $b \in (p)$, 不妨设 $a \in (p)$, 则 $(a) \subseteq (p)$. 另一方面 $(p) \subseteq (a)$, 因此 $(p) = (a)$, 从而 b 是单位.
注: $x \sim y :\Leftrightarrow \exists u \in U(R), x = uy \iff (x) = (y) \iff x \mid y$ 且$y \mid x$.

8. (习题 2.2.3)

设 R 是一个主理想整环 (PID), $0 \neq r \in R$. 证明：在 R 中仅有有限个理想包含 r.

proof

R 是 PID, 即对任意理想 I, 存在 $a\in R$, 理想 $I=(a)$. 理想 I 包含 r 指 $r\in I$, 它等价于 $(r)\subseteq I=(a) \iff a\mid r$. 又因为 PID 是 UFD, 因此又唯一分解 $r=p_1p_2\cdots p_n$, 从而 r 因子个数在相伴的意义下 (上题的注记) 有限 ($\leqslant 2^n$), 即包含 r 的理想有限.

9. (习题 2.2.4)

(辗转相除法) 设 R 是欧氏环, $a,b\in R$ 非零. 由带余除法得

$$a=q_1b+r_1,\ b=q_2r_1+r_2,\ r_1=q_3r_2+r_3,\ \cdots,\ r_{k-2}=q_kr_{k-1}+r_k$$

满足 $\delta(r_k)<\delta(r_{k-1})<\cdots<\delta(r_2)<\delta(r_1)<\delta(b)$. 试证明：

(1) 存在 k 使得 $r_{k+1}=0$;

(2) r_k 是 a, b 的一个最大公因子;

(3) 求 u, $v\in R$ 使得 $r_k=ua+vb$.

proof

(1) 由于 $\delta(b)<\infty$, 且 $\delta(r_k)$ 是严格递减的自然数序列, 因此 $\delta(k)\leqslant\delta(b)-k$, 取 $k>\delta(b)$ 即可.

(2) 由 (1) 知最后一个等式为 $r_{k-1}=q_{k+1}r_k$. 且

$$(a,b)=(bq_1+r_1,b)=(b,r_1)=(q_2r_1+r_2,r_1)=(r_1,r_2)=\cdots=(r_{k-1},r_k)=r_k.$$

(3) 根据辗转相除法的算式反过来表示 r_k.

$$\begin{aligned} r_k&=r_{k-2}-q_kr_{k-1}=u_1r_{k-2}+v_1r_{k-1}, \quad u_1=1,v_1=-q_k\\ &=u_1r_{k-2}+v_1(r_{k-3}-q_{k-1}r_{k-2}), \quad (r_{k-3}=q_{k-1}r_{k-2}+r_{k-1})\\ &=u_2r_{k-3}+v_2r_{k-2}, \quad u_2=-q_k,v_2=1+q_kq_{k-1}\\ &=\cdots\\ &=u_ka+v_kb \end{aligned}$$

递归关系是 $u_i=v_{i-1},v_i=u_{i-1}-v_{i-1}q_{k-i+1}$.

注: (1) 是著名的无穷递降的思路, 即递归的得到一列对象且对应着一个严格递减的自然数序列, 根据自然数有下界 0 来得到矛盾或得出某个结论.
另外 (3) 的题干表述可能有些问题, 这里并不需要把 u,v 具体表达出来.

10. (习题 2.2.5)

设 $R=\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\mid\forall a,b\in\mathbb{Z}\}\subset\mathbb{C}$, 定义：$N(a+b\sqrt{-5})=a^2+5b^2$. 试证明：

(1) $U(R)=\{1,-1\}$;

(2) R 中任意元素都有不可约分解;

(3) 3, $2+\sqrt{-5}$, $2-\sqrt{-5}\in R$ 是不可约元;

(4) $9 = 3 \cdot 3 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$ 是 9 的两个不相同的不可约分解.

proof

(1) 验证 N 满足 $N(\alpha\beta) = N(\alpha)N(\beta)$, 这和复数中 $|z_1 z_2| = |z_1||z_2|$ 是类似的, 且 $N(\alpha) \in \mathbb{N}$. 那么若 α 是单位, 则存在 β 使得 $\alpha\beta = 1$, 故 $N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1$, 故只能有 $N(\alpha) = N(\beta) = 1$, 解得 $\alpha = \pm 1$.

(2) 因为 R 是 Noether 环.(但其实没那么好说明, 如果知道 Hilbert's Basis Theorem 就没问题)

或者可以用 $N(\alpha)$ 保持乘法的特性. 对任意 $\alpha \in R$, 若它不可约, 则已经是一个分解了; 否则 $\alpha = \beta\gamma$, 其中 β, γ 不是单位, 且有 $N(\alpha) = N(\beta)N(\gamma)$. 因此 $N(\beta), N(\gamma) < N(\alpha)$, 由于 $N(\alpha) < \infty$, 因此这样分解是有限的, 这和 Noether 环 $\implies$ 存在分解的过程是类似的.

(3) 由于 $N(3) = N(2+\sqrt{-5}) = N(2-\sqrt{-5}) = 9 = 3^2$, 若它们可约, 则存在 α 使得 $N(\alpha) = 3$, 这是不可能的.

另外, 若 $N(\alpha)$ 是素数, 则一定不可约, 但是反过来不对, 比如这里 9 并不是素数.

(4) 由 (3).

注:

1. 这个 N 是范数 (norm). 它其实是 $\mathbb{Q}$-线性映射 $\beta \mapsto \alpha\beta$ 所对应矩阵的行列式. 这个概念在模论和代数数论都有提及.

2. (1) 和 (2) 的结论是可以推广的, 对于一个代数数域 $K/\mathbb{Q}$(即 $\mathbb{Q}$ 的有限扩张), $\alpha \in \mathcal{O}_K$ 是单位当且仅当 $N_{K/\mathbb{Q}}(\alpha) = 1$. 其中 $\mathcal{O}_K$ 是对应的代数整数环. $\mathcal{O}_K$ 是存在不可约分解的环. 其证明方法和 (2) 几乎一模一样. 具体细节参考代数数论的教材.

课上的补充内容

1. ($\mathbb{Z}$ 是 PID)

若 $I \subseteq \mathbb{Z}$ 是理想, 则 $\exists n \in \mathbb{Z}_{>0}$ 使得 $I = (n)$.

2. (集合论相关)

I. 设 $f: X \to Y$ 是映射, $X_1 \subseteq X, Y_1 \subseteq Y$,

(1) X_1 的像 (image)$f(X_1)$ 是一个 Y 的子集, $f(X_1) := \{f(x) \in Y \mid x \in X_1\}$,

(2) Y_1 的原像 (preimage)$f^{-1}(Y)$ 是一个 X 的子集, $f^{-1} = \{x \in X \mid f(x) \in Y_1\}$. 当 Y_1 是单点集 $\{y\}$ 时, $f^{-1}(Y_1)$ 可以简记为 $f^{-1}(y)$.

II. 映射 $f: X \to Y$ 是

(1) 单的 (injective), 如果 $f(x) = f(y) \implies x = y$,

(2) 满的 (surjective), 如果 $f(X) = Y$.

(3) 双射, 如果 f 既单又满.

(4) 可逆的, 如果存在 $g : Y \to X$ 使得 $g \circ f = \mathrm{id}_X$, $f \circ g = \mathrm{id}_Y$.

III. 若 $f : X \to Y$, $g : Y \to X$, 则

$$g \circ f = \mathrm{id}_X \implies f \text{ 单}, g \text{ 满}$$

因此可逆映射是双射.

IV. 若 $f : X \to Y$ 满且有交换图表

$$\begin{tikzcd} X \arrow[rr, "\varphi"] \arrow[dr, two heads, "f"'] & & Z \\ & Y \arrow[ur, "g"'] & \end{tikzcd}$$

则 g 唯一. 换句话说, $g_1 \circ f = g_2 \circ f \implies g_1 = g_2$. 在一般的范畴中, 满足这条性质的态射叫一个满态射 (epimorphism).

类似的, 若 f 是单的, 且有交换图表

$$\begin{tikzcd} Z \arrow[rr, "\varphi"] \arrow[dr, "g"'] & & Y \\ & X \arrow[ur, hook, "f"'] & \end{tikzcd}$$

则 g 唯一. 即 $f \circ g_1 = f \circ g_2 \implies g_1 = g_2$. 满足这条性质的态射叫一个单态射 (monomorphism).