第四次习题课

小测题讲解，知识提要，习题讲解和内容扩充

助教：邓先涛

2023 年 10 月 9 日

第二次小测题讲解

小测第 1 题

写出环 $\mathbb{C}[x]/(x^4-1)$ 的所有素理想.

素理想的定义和环同态定理中的理想对应

思维拓展

试利用该方法给出 $\mathbb{Q}[\sqrt{m}]$ 的整数环 R_m 的所有素理想.

证明

- 设 $R_1 \to R_2$ 是满同态，则 R_1 中包含 ker 的理想与 R_2 的理想一一对应，极大理想对应极大理想，素理想对应素理想.
- $\mathbb{C}[x]$ 是主理想整环，包含 x^4-1 的素理想只有 $(x-1)$、$(x+1)$、$(x-i)$ 和 $(x+i)$.
- $(\overline{x}-1)$、$(\overline{x}+1)$、$(\overline{x}-i)$ 以及 $(\overline{x}+i)$ 是商环 $\mathbb{C}[x]/(x^4-1)$ 的所有素理想.

小测第 2 题

设 α 是幺环 R 中的幂零元，即存在正整数 n 使得 $\alpha^n = 0$，证明：$1 + \alpha + \cdots + \alpha^{2023}$ 可逆.

因式分解技巧

思维拓展

本质上，对幺环中的幂零元 α，任给正整数 m，有 $\sum_{i=0}^{m} \alpha^i$ 可逆.

证明

- 存在 $m \in \mathbb{N}$ 使 $2024m > n$，即 $\alpha^{2024m} = 0$. 因此可对 $1 = 1 - \alpha^{2024m}$ 进行因式分解.
- $1 - \alpha^{2024m} = (1 - \alpha^{2024}) \sum_{i=0}^{m-1} \alpha^{2024i}$.
- $1 - \alpha^{2024} = (1 - \alpha)(1 + \alpha + \cdots + \alpha^{2023})$.

小测第 3 题

设 $\tau : \mathbb{C}[x, y] \to \mathbb{C}[t]$ 是环同态，满足 $\tau(x) = t^2$ 和 $\tau(y) = t^3$，且 $\forall a \in \mathbb{C}$，$\tau(a) = a$，求 $\ker(\tau)$.

带余除法：交换幺环上的首项系数为单位的多项式均有带余除法

思维拓展

能否刻画 $\mathbb{C}[x, y]$ 的所有素理想和极大理想？

证明

- 将 $\mathbb{C}[x, y] = \mathbb{C}[x][y]$ 看作 $\mathbb{C}[x]$ 的多项式环.
- 注意 $y^2 - x^3 \in \ker(\tau)$，考虑 $f(x, y) \in \ker(\tau)$ 对 $y^2 - x^3$ 做带余除法.
- $f(x, y) = (y^2 - x^3)q(x, y) + f_1(x)y + f_0(x)$，假设 $f(x, y) \in \ker(\tau)$，则 $f_0(t^2) + f_1(t^2)t^3 = 0$.
- 得 $f_0(x) = 0 = f_1(x)$，故 $\ker(\tau) = (y^2 - x^3)$.

小测第 4 题

证明：$I=(5,2+\sqrt{-6})$ 是 $\mathbb{Z}[\sqrt{-6}]$ 的极大理想.

- 环同态中理想对应：考察 $\mathbb{Z}[x]$ 的极大理想.
- 整数中的带余除法

思维拓展

设 I 是 R_m 的任一理想，则存在元素 $a,b\in R_m$ 使得 $I=(a,b)$.

证明

- 任给 $c=a+b\sqrt{-6}(a,b\in\mathbb{Z})\notin I$.
- 可以写作 $c=(a-2b)+b(2+\sqrt{-6})$，立刻推出 $5\nmid a-2b$，因此根据裴蜀引理，存在整数 u,v 使得 $5u+(a-2b)v=1$.
- 故 $1=5u+vc-vb(2+\sqrt{-6})\in I+(c)$.

小测第 5 题

设 R 是整环，$\pi \in R$ 非零不可逆，证明：π 是不可约元当且仅当 (π) 为 R 所以非平凡主理想构成的集合的极大元.

不可约元定义：$\pi = ab$ 推出 a 或 b 是单位.

思维拓展

素元与不可约元性质：能否构造一个非 UFD 的整环使得其中的素元与不可约元等价？

证明

- 前推后：若不然，则存在 $(\pi) \subsetneqq (\eta)$，立刻得到存在 $c \in R$ 使得 $\pi = c\eta$，推出矛盾.
- 后推前：考虑 $\pi = ab$，若 a 和 b 都不是单位，则 $(\pi) \subsetneqq (a)$ 矛盾.

重点知识提要

重点知识提要

- UFD、PID 和 ED 的概念与性质：了解三者的“大小”关系，并可以举出相应的例子；了解三者所对应的判定准则.
- 不可约元与素元的性质
- UFD 上多项式环的性质：域上的多项式环是主理想整环；UFD 上的多项式环仍是 UFD.
- 二次整数环定义：设 m 是无平方因子整数，且 $m \neq 0, 1$，定义

$$R_m = \begin{cases} \mathbb{Z}[\sqrt{m}], & m \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}], & m \equiv 1 \bmod 4. \end{cases}.$$

第四章习题讲解

第四章第 4 题

令 $F=\mathbb{Q}(\sqrt{m})$，证明：R_m 是 F 的子环.

证明

具有相同单位元，减法封闭，乘法封闭即可验证是子环.

子环的定义

思维拓展 1

设 $f(x)\in\mathbb{Z}[x]$ 是首一整系数多项式，若 $\alpha\in F$ 是多项式 $f(x)$ 的根，则 $\alpha\in R_m$.

思维拓展 2

设 $f(x)\in R_m[x]$ 是首一多项式，若 $\alpha\in F$ 是多项式 $f(x)$ 的根，则 $\alpha\in R_m$.

第四章第 5 题

设 m 是无平方因子整数且 $m \neq 0, 1$，令 $R_m^\times$ 记为 R_m 中所有单位构成的乘法群. 对于 $m < 0$，计算 $R_m^\times$.

整数上的不定方程

思维拓展

该问题在 $m > 0$ 的情况下是复杂的，你是否能在 $m > 0$ 情况下计算 $R_m^\times$？特别的，计算 $R_2^\times$.

证明

- 若 $m \equiv 2, 3 \bmod 4$，则 R_m 中单位 $a + b\sqrt{m} \iff |a^2 - mb^2| = 1$.
- 若 $m \equiv 1 \bmod 4$，则 R_m 中单位 $a + b\frac{1+\sqrt{m}}{2} \iff |a^2 + ab + \frac{1-m}{4}b^2| = 1$.
- 由于 $m < 0$，因此可以容易地对上述式子进行放缩，即可得到结果.

第四章第 12 题

证明 $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ 是欧几里得整环.

仿造教材上 R_{-3} 是欧几里得整环的证明

思维拓展

该方法能够处理的 m 的最大情况是多少?

证明

- 定义 $d(x) = |N(x)|$，这里 $N(x) = x \cdot \overline{x}$.
- 任给 $x \in R_5$，存在同奇同偶的 $a, b \in \mathbb{Z}$ 使得 $x = \frac{a+b\sqrt{5}}{2}$.
- 任给 $\alpha, \beta \in R_5$，有 $\frac{\alpha}{\beta} = t + s\sqrt{5}(t, s \in \mathbb{Q})$.
- 取同奇同偶的 a, b 使得 $|2s - a| \leq \frac{1}{2}$，$|2t - b| \leq 1$. 取 $q = \frac{a+b\sqrt{5}}{2}$.
- $\alpha = q\beta + (t + s\sqrt{5} - q)\beta = q\beta + r$ 满足欧几里得整环的性质.

第四章第 14 题

设 p 为奇素数，则在 $\mathbb{Z}$ 中 $x^2 = -1 \bmod p$ 有解的充要条件是 $p \equiv 1 \bmod 4$.

二次剩余或组合构造

思维拓展

试刻画并证明 $x^2 \equiv -1 \bmod p^n$ 有解的充要条件.

证明 1

$p \equiv 1 \bmod 4$ 等价于 $(\frac{-1}{p}) = 1$ 等价于 $x^2 \equiv -1 \bmod p$ 有解.

证明 2

- 若 $x^2 \equiv -1 \bmod p$ 有解，则 $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$.
- 若 $p \equiv 1 \bmod 4$，假设方程无解，定义 $V = \{(x, y) | xy = -1, x, y \in \mathbb{F}_p, x, y \neq \pm 1\}$.
- 4 整除 $|V| = p - 3$ 推出矛盾.

第四章第 16、17 题

找出 R_{-1} 中的所有不可约元.

整数的性质

思维拓展

试找出 R_{-2} 中的所有不可约元.

证明

- $p \equiv 1 \bmod 4$，存在 x 使得 $x^2 + 1 \in pR_{-1}$，这表明 p 不是不可约元，令 $p = \alpha\overline{\alpha}$，$\alpha$ 为第一类不可约元当且仅当 $N(\alpha) = p$.
- $p \equiv 3 \bmod 4$ 不可约，否则 $p = \alpha\beta$ 推出 $N(\alpha) = p = a^2 + b^2$ 矛盾.
- $2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$，即可产生第三种不可约元 $\pm 1 \pm \sqrt{-1}$.

第四章第 18 题

正整数 m 可表两整数的平方和的充要条件是 m 标准素分解中 $4k+3$ 型素数的幂指数为偶数.

$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$$

思维拓展

试思考正整数可以表为 x^2+ny^2 的充要条件是什么？试对 $n=2,3$ 进行一个类似的证明.

证明

- 根据提示公式，后推前显然.
- 前推后：注意到 R_{-1} 是唯一分解整环，将 $m=a^2+b^2$ 在 R_{-1} 中分解，模 4 余 3 的素数总是成对出现.

第四章第 23 题

设 D 是主理想整环，若 D 不是域，则 $D[x]$ 不是主理想整环.

证明

设 $0 \neq a \in D$ 不可逆，则 $I = (a, x) \subset D[x]$ 不是主理想.

理想生成集

思维拓展

证明：$D[x]$ 中的理想总可由有限多个元素生成.

第四章第 24 题

主理想整环的商环的每一个理想都是主理想.

环满同态中理想的对应

思维拓展

是否存在一个主理想整环，它的商环中的理想有无穷多个？

证明

考虑 $\pi : R \to R/I$ 为标准同态，是满同态，因此任给 J 为 R/I 中的理想，存在 R 中包含 I 的理想 (a) 使得 $\pi((a)) = J$，因此 $J = (\overline{a})$.

问题补充和方法扩张

问题 1

关于唯一分解整环和主理想整环的思考：

- PID 中两元素的最大公因子有 $\gcd(a,b)=ua+bv$，试举例说明该性质在 UFD 中不成立. 如果某个 UFD 中有上述性质，那么该 UFD 是 PID.
- PID 中任意理想升链稳定，试举例说明该性质在 UFD 中不成立.
- PID 要求每一个理想都是主理想，如果仅要求整环中的素理想是主理想，那么能否推出该整环是 PID?
- UFD 的定义中有两个条件需要满足，如果仅要求整环中每一个元素均可写作有限多不可约元的乘积，那么能否推出该整环是 UFD? 如果仅要求整环中每一个元素均可写作有限多素元的乘积，那么能否推出该整环是 UFD?

问题 2

设 $p \equiv 1 \bmod 4$ 是素数，素数 q 满足 $(\frac{q}{p}) = -1$，则 $\mathbb{Z}[\sqrt{pq}]$ 不是 UFD.

简要说明

考察 $pq = p \times q = \sqrt{pq} \cdot \sqrt{pq}$，由条件即可判定 p 和 q 是不可约元，因此不可约.

问题 3

设 $a \in \mathbb{Z}$，p 是素数，$f(x) = (x-a)^n + pF(x) \in \mathbb{Z}[x]$，其中 $F(x) \in \mathbb{Z}[x]$ 满足 $p \nmid F(a)$ 且 $\deg(F) \leq n$.

证明：$f(x)$ 模 p^2 是不可约的，即不存在 $h(x), g(x) \in \mathbb{Z}[x]$ 使得 $f(x) \equiv h(x)g(x) \bmod p^2$.

简要说明

- 令 $h_0(x) \equiv h(x) \bmod p$，$g_0(x) \equiv g(x) \bmod p$，则 $(x-a)^n \equiv g_0(x)h_0(x) \bmod p$. 注意到多项式环 $\mathbb{Z}/p\mathbb{Z}[x]$ 唯一分解，因此 $h_0(x) \equiv (x-a)^u$，$g_0(x) \equiv (x-a)^v \bmod p$，其中 $u+v=n$.
- $h(x) = (x-a)^u + pH(x)$，$g(x) = (x-a)^v + pG(x)$，因此

$$pF(x) \equiv p\big((x-a)^v H(x) + (x-a)^u G(x)\big) \bmod p^2.$$

根据 $p \nmid F(a)$，不妨设 $u = 0$. 进一步得到 $H(x)$ 为常值多项式，因此 $f(x)$ 没有非平凡分解.