

# Abstract Algebra

## Homework

Gan Luo

2023.12.9

# 目录

## Chapter 1

Page 2

1.1	homework 5a Part4	2
1.2	homework 6a Part1	5

# Chapter 1

## 1.1 homework 5a Part4

### Question 1: Page 102, problem 17

$p$  is a prime,  $p \equiv 1 \pmod{4}$ , prove that there exist  $a, b \in \mathbb{Z}$ , such that  $a^2 + b^2 = p$

**Solution:**

$p \equiv 1 \pmod{4}$ , so there exist  $x, x^2 \equiv -1 \pmod{p}$ , then  $p \mid (x^2 + 1)$  in  $\mathbb{Z}$ , then  $p \mid (x + i)(x - i)$  in  $\mathbb{Z}[i]$ , but  $p \nmid (x + i), p \nmid (x - i)$ , so  $p$  is a prime element in Euclidean domain  $\mathbb{Z}[i]$ , so  $p$  is reducible in  $\mathbb{Z}[i]$ .

$\exists z_1, z_2 \in \mathbb{Z}[i], p = z_1 z_2$ , so let's consider the norm of  $p$ ,  $N(p) = p^2 = N(z_1)N(z_2)$ , since  $z \in \mathbb{Z}[i]$  is a unit (reversible) if and only if  $N(z) = 1$ ,  $N(z_1) = N(z_2) = p$ .

We have  $z_1 = a + bi$  with  $a, b \neq 0$ . And the statement that the norm of  $z_1$  is  $p$  is exactly the statement that  $a^2 + b^2 = p$ .

So we have shown that  $p \equiv 1 \pmod{4}$  means that  $p$  can be written as a sum of two squares (in a completely nonconstructive way).  $\diamond$

**Note:-**

- the norm of an element in  $\mathbb{Z}[i]$  means  $N(a + bi) = a^2 + b^2$
- Euler's Criterion:  $p$  is an odd prime,  $a \in \mathbb{Z}, (a, p) = 1$

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \pmod{p}, \text{ if there exist an integer } x \text{ such that } x^2 \equiv a \pmod{p}, \\ -1 & \pmod{p}, \text{ if there is no such integer.} \end{cases}$$

So since  $p \equiv 1 \pmod{4}$ , we have  $-1^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ , so there exist  $x, x^2 \equiv -1 \pmod{p}$ .

- $p$  is an odd prime. If  $p \equiv 1 \pmod{4}$ , then  $p$  is reducible in  $\mathbb{Z}[i]$ . If  $p \equiv 3 \pmod{4}$ , then  $p$  is irreducible in  $\mathbb{Z}[i]$ .

### Question 2: Page 102, problem 18

证明环  $\mathbb{Z}[i]$  的不可约元, 在相伴意义下, 只有以下三种:

(1)  $1 + i$ ; (2)  $a + bi, a, b \in \mathbb{Z}, a^2 + b^2 \equiv 1 \pmod{4}$  为素数; (3)  $p \equiv 3 \pmod{4}$  为素数.

**Solution:**

$\alpha \in \mathbb{Z}[i]$ 不可约, 因此 $\alpha$ 是素元,  $\alpha\mathbb{Z}[i]$ 是素理想,  $\alpha\mathbb{Z}[i] \cap \mathbb{Z} = (p) = p\mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想, 因此 $\alpha \mid p$ .故 $\alpha$ 不可约可以推出 $\alpha$ 是素数在 $\mathbb{Z}[i]$ 中的因子.

反之, 若 $\alpha \mid p$ , 由于 $p$ 是有理素数, 那么 $\bar{\alpha} \mid p$ , 所以有 $p = \alpha\bar{\alpha}r, r \in \mathbb{Z}[i]$ , let's consider the norm of  $p, N(p) = p^2 = N(\alpha)N(\bar{\alpha})N(r)$ , 若 $\alpha$ 非平凡, 那么 $N(\alpha) = p, p = \alpha\bar{\alpha}, N(\alpha) = p$ , 由于 $\alpha$ 在 $\mathbb{Z}[i]$ 中不可约.

因此,  $\alpha \in \mathbb{Z}[i]$ 不可约 if and only if  $\alpha$ 是素数 $p$ 的非平凡因子.

$p = 2 = (1+i)(1-i), i(1+i) = i-1 = -(1-i), N(i) = 1, 1+i$ 与 $1-i$ 在 $\mathbb{Z}[i]$ 中相伴,  $\alpha = 1+i$ .

$p \equiv 1 \pmod{4}$ , so there exist integer  $a, b$ , such that  $a^2 + b^2 = p = (a+bi)(a-bi)$ , 故 $\alpha = a+bi$ .

$p \equiv 3 \pmod{4}$ , 若存在 $a, b \in \mathbb{Z}$ , 使得 $p = a^2 + b^2$ , 根据下面的小定理, 有 $p \mid a$  and  $p \mid b$ , 因此矛盾, 故 $\alpha = p \equiv 3 \pmod{4}$

### Theorem 1.1.1

Let  $p$  be a prime. If  $p \equiv 3 \pmod{4}$ ,  $p \mid a^2 + b^2$ , then  $p \mid a$  and  $p \mid b$ .

**证明:** Using Fermats Little Theorem:  $a^p \equiv a \pmod{p}, b^p \equiv b \pmod{p}$ .

Since  $p \equiv 3 \pmod{4}$ , we have  $a^{p+1} + b^{p+1} \equiv a^2 + b^2 \equiv 0 \pmod{p}$ . Because  $4 \mid p+1$ , we can write  $p+1 = 4k$ , so  $a^{4k} + b^{4k} = a^{4k} + (b^2)^{2k} \equiv a^{4k} + (-a^2)^{2k} = 2a^{4k} \pmod{p}$ .

由于 $p \nmid 2, p \mid a^{4k}$ , so  $p \mid a$ , 同理 $p \mid b$ .

☺

### Question 3: 5a-1

$F$  is a field,  $R = \{f(x) \in F[x] \mid f(x) = a_0 + \sum_{i=2}^n a_i x^i\}$ . Prove that  $R$ 是 $F[x]$ 的子环;  $x^2, x^3$ 是不可约元, 但不是素元(so  $R$  is not UFD).

**Solution:**

子环验证略.

To prove that  $x^2, x^3$  are irreducibel in  $R$ , just consider the deg.

$x^2, x^3$  are not prime,  $x^2 \mid x^3 \cdot x^3, x^2 \nmid x^3$  and  $x^3 \mid x^2 \cdot x^4, x^3 \nmid x^4, x^3 \nmid x^2$

### Question 4: 5a-2

$R$ 为UFD,  $P$ 为 $R$ 的非零素理想, 证明:  $P$ 中有素元.

**Solution:**

$P$  is nonzero, so  $\exists a \in P, a \neq 0, a$  is irreversibel. Since  $R$  is UFD,  $a = a_1 \dots a_n, a_i$  is irreducibel. Since  $P$  is prime,  $a_k \in P, k \in \{1, \dots, n\}$ . Since  $R$  is UFD,  $a_k$  is prime.  $\diamond$

### Note:-

- 诺特环的同态像是诺特环.
- (Hilbert基定理)  $R$ 为交换诺特环, 那么 $R[x]$ 为诺特环.
- 非UFD的诺特环:  $\mathbb{Z}[\sqrt{-5}]$   
 $\mathbb{Z}$ 为PID, 故为诺特环, 因此 $\mathbb{Z}[x]$ 是诺特环, 由于 $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}/(x^2 + 5)$ , 故 $\mathbb{Z}[\sqrt{-5}]$ 是诺特环
- 非诺特环的UFD:  $F[x_1, x_2, \dots, x_n, \dots]$

### Question 5: 5a-4

$R$  is UFD,  $ab = c^n$ ,  $a, b, c \in R^*$ ,  $n \in \mathbb{N}_+$ ,  $a, b$  are coprime, prove that there exist  $u, v, f, g \in R$ ,  $u, v$  are invertible, such that  $a = uf^n, b = vg^n$ .

**Solution:**

(i) If  $a$  or  $b$  is invertible, WLOG,  $a$  is invertible, then  $a = a \cdot 1^n, b = 1 \cdot c^n$ .

(ii) If  $a$  and  $b$  are irreversibel, then  $c^n$  is irreversibel, since  $R$  is UFD, so  $ab = (a_1 \dots a_n)(b_1 \dots b_m) = c^n = (c_1 \dots c_t)^n$ , where  $a_i, b_j, c_s$  are irreducibel.

使用相同的相伴代表元, 由于  $a, b$  互素, 因此没有不可逆的公因子, 所以  $a = ud_1^{e_1} \dots d_n^{e_n}, u$  可逆,  $b = vd_{n+1}^{e_{n+1}} \dots d_{n+s}^{e_{n+s}}, v$  可逆, 因此  $a = uf^n, b = vg^n$ .  $\diamond$

### Question 6: 5a-5

求  $x^2 + 2 = y^3$  所有整数解.

**Solution:**

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3 \text{ in } \mathbb{Z}[\sqrt{-2}].$$

•  $\mathbb{Z}[\sqrt{-2}]$  is UFD.

•  $x + \sqrt{-2}, x - \sqrt{-2}$  无不可逆公因子

If  $x + \sqrt{-2} = a_1 \dots a_n, y = b_1 \dots b_m$ , then  $x - \sqrt{-2} = \overline{a_1} \dots \overline{a_n}, a_i, b_j$  are irreducibel, since the factorization is unique,  $2n = 3m$ , so  $n = 3t, m = 2t$ .

$x + \sqrt{-2}, x - \sqrt{-2}$  互素, 因此,  $x + \sqrt{-2} = (a + bi)^3 = a^3 - 6ab + (3ab - 2b^3)\sqrt{-2}$ , then  $b(3a - 2b^2) = 1$ , so  $b \in U(\mathbb{Z}[\sqrt{-2}]) = \{1, -1\}$ .

$b = 1$ , then  $a = 1, x = -5, y = 3$ , or  $a = -1, x = 5, y = 3$ .

$b = -1$ , no solution.

So, all solutions are:  $a = 1, x = -5, y = 3$ , or  $a = -1, x = 5, y = 3$ .  $\diamond$

#### Claim 1.1.1

$\mathbb{Z}[\sqrt{-2}]$  is UFD.

**证明:** 思路: 证明  $\mathbb{Z}[\sqrt{-2}]$  是 ED, 从而是 UFD.

$\forall \alpha, \beta \in \mathbb{Z}[\sqrt{-2}], \alpha\beta^{-1} = u + v\sqrt{-2}, u, v \in \mathbb{Q}$ , choose  $a, b \in \mathbb{Z}, \alpha\beta^{-1} = u + v\sqrt{-2} = (a + b\sqrt{-2}) + [(u - a) + (v - b)\sqrt{-2}]$ ,  $|a - u| \leq \frac{1}{2}, |v - b| \leq \frac{1}{2}$ .

So  $\alpha = \beta(a + b\sqrt{-2}) + \beta[(u - a) + (v - b)\sqrt{-2}]$ , since  $\alpha - \beta(a + b\sqrt{-2}) = \beta[(u - a) + (v - b)\sqrt{-2}] \in \mathbb{Z}[\sqrt{-2}]$ , let  $q = a + b\sqrt{-2}, r = \beta[(u - a) + (v - b)\sqrt{-2}] \in \mathbb{Z}[\sqrt{-2}]$ , then  $\alpha = \beta q + r, q, r \in \mathbb{Z}[\sqrt{-2}], \delta(r) = N(r) = N(\beta)N((u - a) + (v - b)\sqrt{-2}) = N(\beta)[(u - a)^2 + 2(v - b)^2] \leq N(\beta)\frac{3}{4} < N(\beta)$ , so  $\mathbb{Z}[\sqrt{-2}]$  is ED, thus UFD.  $\diamond$

☺

#### Claim 1.1.2

$x + \sqrt{-2}, x - \sqrt{-2}$  无不可逆公因子

证明: 若有  $a \in \mathbb{Z}[\sqrt{-2}]$  不可约,  $a \mid x + \sqrt{-2}, x \mid x - \sqrt{-2}$ , 那么  $a \mid 2\sqrt{-2}$ .

由于UFD中, 不可约元是素元, 所以  $a \mid \sqrt{-2}, a = \pm\sqrt{-2}$ , 但  $\sqrt{-2} \nmid x + \sqrt{-2}$ , 矛盾, 因此没有不可逆的公因子.  $\diamond$

#### Question 7: 5a-6

$R[x]$ 是PID  $\iff R$ 是域.

**Solution:**

( $\Rightarrow$ ):  $R[x]$ 是PID,  $x$ 在 $R[x]$ 中不可约  $\iff (x)$ 是极大理想  $\Rightarrow R[x]/(x) \cong R$ 为域.

( $\Leftarrow$ ):  $R$ 是域, 同高代方法.

#### Question 8: 5a-7

$R$  is ED, prove that  $\forall a \in R, a \neq 0, a$  is invertibel  $\iff \delta(a) = \min \delta(R^*)$

**Solution:**

( $\Rightarrow$ ):  $a$  is invertibel,  $ab = 1, \forall r \in R^*, r = (rb)a, \delta(a) \leq \delta(r)$ .

( $\Leftarrow$ ):  $\delta(a) = \min \delta(R^*), 1 = aq + r, r = 0, a$  is invertibel.

## 1.2 homework 6a Part1

#### Question 9: 6a-1

$K$ 是域 $F$ 的代数扩域,  $L$ 是 $K$ 的包含 $F$ 的子环, 证明 $L$ 是域

**Solution:**

$L$ 是域 $K$ 的子环, 因此 $L$ 是整环.

$\forall s \in L \subset K, s \neq 0$ , 因为 $K$ 是 $F$ 的代数扩域, 所以 $s$ 在 $F$ 上是代数的, 存在极小多项式  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in F[x], f(s) = 0$ , 由于 $f(x)$ 在 $F[x]$ 上不可约, 因此 $a_0 \neq 0$ , 所以  $s(a_n s^{n-1} + \dots + a_1)(-a_0^{-1}) = 1, s^{-1} = (a_n s^{n-1} + \dots + a_1)(-a_0^{-1}) \in F \subset L$ , 因此 $L$ 是域.

#### Question 10: 6a-2

$\alpha \in \mathbb{Q}(\sqrt[5]{3}) \setminus \mathbb{Q}$ , 证明  $\sqrt[5]{3} \in \mathbb{Q}(\alpha)$

**Solution:**

实际上, 就是要证明: 如果  $\alpha \in \mathbb{Q}(\sqrt[5]{3}) \setminus \mathbb{Q}$ , 那么  $\mathbb{Q}(\sqrt[5]{3}) = \mathbb{Q}(\alpha)$ .

可以巧妙地利用5是素数这一点.

因为  $\alpha \in \mathbb{Q}(\sqrt[5]{3})$ , 所以  $\mathbb{Q}(\alpha) \in \mathbb{Q}(\sqrt[5]{3})$ . 因为  $\alpha \in \mathbb{Q}(\sqrt[5]{3}) \setminus \mathbb{Q}$ , 所以  $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 2$ . 而  $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5 = [\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$ , 所以  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5, [\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}(\alpha)] = 1$ , 从而  $\mathbb{Q}(\sqrt[5]{3}) = \mathbb{Q}(\alpha), \sqrt[5]{3} \in \mathbb{Q}(\alpha)$ .  $\diamond$

#### Question 11: 6a-3

$K = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ , 给出 $K$ 的子域 $F, \alpha \in K$ , 使得  $[F : \mathbb{Q}] = 3, [F(\alpha), \mathbb{Q}(\alpha)] = 3$ .

**Solution:**

$$F = \mathbb{Q}(\sqrt[3]{2}), [F : \mathbb{Q}] = \deg(x^3 - 2) = 3, \alpha = e^{\frac{2\pi i}{3}}, [F(e^{\frac{2\pi i}{3}}) : \mathbb{Q}(e^{\frac{2\pi i}{3}})] = [K : \mathbb{Q}(e^{\frac{2\pi i}{3}})] = 3$$

#### Question 12: 6a-5

$a_1, \dots, a_n \in \mathbb{N}_+$ , 两两互素, 都不是完全平方数, 证明:  $[\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}) : \mathbb{Q}] = 2^n$ .

**Solution:**

利用有限单扩张升链.

$F_0 = \mathbb{Q}, F_i = \mathbb{Q}(a_1, \dots, a_i)$ , 考察  $[F_{i+1} : F_i]$ , 因为  $a_1, \dots, a_n$  两两互素, 因此  $\sqrt{a_{i+1}} \notin F_i$ , 因此  $[F_{i+1} : F_i] > 1$ . 因为  $a_{i+1}$  不是完全平方数,  $a_{i+1} \in \mathbb{N}_+ \subset \mathbb{Q}$ , 所以  $[F_{i+1} : F_i] = 2$ , 从而  $[F_n : F_0] = 2^n$ .

#### Question 13: 6a-6

$\alpha_1, \dots, \alpha_n \in \mathbb{C}, \alpha_i^2 \in \mathbb{Q}$ , 证明: 域  $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$  不包含  $\sqrt[6]{2}$ .

**Solution:**

利用望远镜定理中的整除关系.

$F_0 = \mathbb{Q}, F_i = \mathbb{Q}(\alpha_1, \dots, \alpha_i)$ , it's easy to show that  $[F_{i+1} : F_i] = 1$  or  $2$ .

若  $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$  包含  $\sqrt[6]{2}$ , 那么  $[F_n : F_0] = 2^k = [F_n : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}]$ ,  $6 \mid 2^k$ , 矛盾.

#### Question 14: 6a-7

证明:  $\mathbb{Q}(\sqrt[3]{7} + 2i) = \mathbb{Q}(\sqrt[3]{7}, 2i)$ , 求  $\sqrt[3]{7} + 2i$  在  $\mathbb{Q}$  上极小多项式.

**Solution:**

显然有  $\mathbb{Q}(\sqrt[3]{7} + 2i) \subset \mathbb{Q}(\sqrt[3]{7}, 2i)$ , 要证明:  $\sqrt[3]{7}, 2i \in \mathbb{Q}(\sqrt[3]{7} + 2i)$ .

$\alpha = \sqrt[3]{7} + 2i, (\alpha - 2i)^3 = 7, \alpha^3 - 12\alpha + (8 - 6\alpha^2)i = 7, i = \frac{7 - \alpha^3 + 12\alpha}{8 - 6\alpha^2} \in \mathbb{Q}(\sqrt[3]{7} + 2i)$ , also  $\sqrt[3]{7} \in \mathbb{Q}(\sqrt[3]{7} + 2i)$ , then  $\mathbb{Q}(\sqrt[3]{7} + 2i) = \mathbb{Q}(\sqrt[3]{7}, 2i)$ . (就是计算极小多项式的中间步骤)

The degree of minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ :  $\deg(f(x)) = [\mathbb{Q}(\sqrt[3]{7} + 2i) : \mathbb{Q}] = 6$ .

$$f(x) = x^6 + 12x^4 - 13x^3 + 48x^2 + 168x + 113. \diamond$$

#### Question 15: 6a-8

域  $E$  是  $\mathbb{R}$  上的有限次扩张, 证明  $E = \mathbb{R}$  或  $E = \mathbb{C}$ .

**Solution:**

若  $E = \mathbb{R}$ , 那么  $E = \mathbb{R}$ .

若  $\exists a \in E \setminus \mathbb{R}, a \neq 0$ , 那么  $[\mathbb{R}(a) : \mathbb{R}] > 1$ , 又因为  $\mathbb{R}$  上的不可约多项式  $p(x)$  次数为 2, 因此  $[\mathbb{R}(a) : \mathbb{R}] = 2$ .

由于  $\mathbb{C}$  是  $\mathbb{R}$  的代数闭包, 那么  $p(x)$  在  $\mathbb{C}$  中必定有根  $\beta = c + di, d \neq 0$ , 那么  $\mathbb{R}(a) \subset E \subset \mathbb{C}, \mathbb{R}(a) = E = \mathbb{C}$ .