Abstract Algebra Homework

Gan Luo

2023.12.9

目录

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 pirme element in Euclidean domain $\mathbb{Z}[i]$, so p is reducibel in $\mathbb{Z}[i]$.

$\exists z_1, z_2 \in \mathbb{Z}[i], p = z_1 z_2$, so let's cosider 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). ◇

Note:-

- the norm of an element in $\mathbb{Z}[i]$ means $N(a+bi) = a^2 + b^2$
- Euler's Creterion: 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 reducibel in $\mathbb{Z}[i]$. If $p \equiv 3 \pmod 4$, then p is irreducibel 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α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$\overline{\alpha}\mid p$，所以有$p=\alpha\overline{\alpha}r, r\in\mathbb{Z}[i]$, let's consider the norm of p, $N(p)=p^2=N(\alpha)N(\alpha)N(r)$，若$\alpha$非平凡，那么$N(\alpha)=p$, $p=\alpha\overline{\alpha}$, $N(\alpha)=p$,由于α在$\mathbb{Z}[i]$中不可约.

因此，$\alpha\in\mathbb{Z}[i]$不可约 if and only if α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, $R=\{f(x)\in F[x] | f(x)=a_0+\sum_{i=2}^{n}a_ix^i\}$. 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, $a=a_1...a_n, a_i$ is irreducibel. Since P is prime, $a_k\in P, k\in\{1,...,n\}$. 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: $F[x_1,x_2,...,x_n,...]$

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 invertibel, such that $a = uf^n, b = vg^n$.

Solution:

(i) If a or b is invertibel, WLOG, a is invertibel, 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 $ab = (a_1 ... a_n)(b_1 ... b_m) = c^n = (c_1 ... c_t)^n$, 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$a = ud_1^{e_1} ... d_n^{e_n}, u$可逆,$b = vd_{n+1}^{e_{n+1}} ... d_{n+s}^{e_{n+s}}, v$可逆，因此$a = uf^n, b = vg^n$.◇

Question 6: 5a-5

求$x^2 + 2 = y^3$所有整数解.

Solution:

$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3$ 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 $x + \sqrt{-2} = a_1 ... a_n, y = b_1 ... b_m$, then $x - \sqrt{-2} = \overline{a_1} ... \overline{a_n}$, a_i, b_j are irreducibel, since the fractorization 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 $a = -1, x = 5, y = 3$.◇

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

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

😆

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, $ab = 1$, $\forall r \in R^*, r = (rb)a, \delta(a) \leqslant \delta(r)$.

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

1.2 homework 6a Part1