日期	科目	姓名，学号
2021 年 12 月 14 日	近世代数	吴天阳 2204210460

习题 2.2

3. 如果环 R 中的元素 a 有一个正整数 n，使得 $a^n = 0$，那么称 a 是**幂零元**。证明：如果 a 是有单位元的环 R 中的一个幂零元，那么 $1 - a$ 可逆。

证明. 由于

$$(1-a)(1+a+a^2+\cdots+a^{n-1}) = 1-a^n = 1$$

$$(1+a+a^2+\cdots+a^{n-1})(1-a) = 1-a^n = 1$$

所以 $1-a$ 的逆元为 $1+a+a^2+\cdots+a^{n-1}$，故 $1-a$ 可逆。 □

5. 设 $I_1, I_2, \cdots, I_s$ 都是环 R 的理想，并且

$$R = I_1 + I_2 + \cdots + I_s,$$

$$I_i \cap (\sum_{j \neq i} I_j) = (0), \quad i = 1, 2, \cdots, s.$$

证明：(1) 环 R 的每个元素 x 都可以唯一表示成

$$x = x_1 + x_2 + \cdots + x_s, \quad x_i \in I_i, i = 1, 2, \cdots, s;$$

(2) 有环同构

$$R \cong I_1 \oplus I_2 \oplus \cdots \oplus I_s,$$

此时称 R 是它的理想 $I_1, I_2, \cdots, I_s$ 的**内直和**。

证明. (1). 由于 $R = I_1 + I_2 + \cdots + I_s$，则 $\forall x \in R$, $\exists x_i \in I_i$, $i = 1, 2, \cdots, s$，使得

$$x = x_1 + x_2 + \cdots + x_s$$

下证唯一性，若 x 有两种表示法，$x = x_1 + x_2 + \cdots + x_s = x_1' + x_2' + \cdots + x_s'$，不妨令 $x_1 \neq x_1'$，则

$$x_1 - x_1' = (x_2' - x_2) + (x_3' + x_3) + \cdots + (x_s' - x_s)$$

又

$$\begin{cases} x_1 - x_1' \in I_1 \\ x_2' - x_2 \in I_2 \\ \quad \vdots \\ x_s' - x_s \in I_s \end{cases}$$

若 $x_i = x_i'\quad \forall i \geqslant 2$，则 $x_1 - x_1' = 0 \Rightarrow x_1 = x_1'$，矛盾。

若 $x_i \neq x_i'\quad \exists i \geqslant 2$，则

$$(x_2' - x_2) + \cdots + (x_s' - x_s) = x_1 - x_1' \in I_1 \cap (\sum_{j\neq 1} I_j) \neq (0)$$

与 $I_1 \cap (\sum_{j\neq 1} I_j) = (0)$ 矛盾。

综上，$\forall x \in R$，可以唯一表示成

$$x = x_1 + x_2 + \cdots + x_s, \quad x_i \in I_i, i = 1, 2, \cdots, s;$$

(2). 由群直和性质知，

$$(R, +) \cong (I_1, +) \oplus (I_2, +) \oplus \cdots \oplus (I_s, +) \cong (I_1 \oplus I_2 \oplus \cdots \oplus I_s, +)$$

其对应的群同构 σ 为：

$$R \to I_1 \oplus I_2 \oplus \cdots \oplus I_s$$

$$x \mapsto (x_1, x_2, \cdots, x_s) \quad \text{其中} x_i \in I_i$$

下证 σ 对乘法保序，对 $\forall i \neq j$，有

$$x_i x_j \in I_i I_j \subset I_i \cap I_j \subset I_i \cap (\sum_{j\neq i} I_j) = (0)$$

则 $x_i x_j = 0\ (\forall i \neq j)$，设 $x, y \in R,\ x = x_1 + x_2 \cdots + x_s,\ y = y_1 + y_2 + \cdots + y_s$，则

$$\begin{aligned}\sigma(xy) &= \sigma((x_1 + \cdots + x_s)(y_1 + \cdots + y_s)) \\ &= \sigma(x_1 y_1 + \cdots + x_s y_s) \\ &= (x_1 y_1, \cdots, x_s y_s) \\ &= \sigma(x)\sigma(y)\end{aligned}$$

综上，σ 为环同构，故 $R \cong I_1 \oplus I_2 \oplus \cdots \oplus I_s$。 □

7. 韩信点兵问题：“有一队士兵，三三数余二，五五数余一，七七数余四，问：这队士兵有多少人?”

解答. 该问题等价于求解同余方程：

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

由于

$$70 \equiv 1 \pmod 3, \quad 70 \equiv 0 \pmod{35}$$

$$21 \equiv 1 \pmod 5, \quad 21 \equiv 0 \pmod{21}$$

$$15 \equiv 1 \pmod 7, \quad 15 \equiv 0 \pmod{15}$$

则解为

$$x \equiv 2 \cdot 70 + 1 \cdot 21 + 4 \cdot 15 \equiv 11 \pmod{105}$$

综上，这队士兵人数为 $11 + 105k$ $(k \in \mathbb{Z}_{\geqslant 0})$。

8. 在 $\mathbb{Z}_{91}$ 中，求 $\bar{1}$ 的全部平方根。

解答. 由于 $91 = 7 \cdot 13$，该问题等价于求解如下同余方程：

$$\begin{cases} x \equiv \pm 1 \pmod 7 \\ x \equiv \pm 1 \pmod{13} \end{cases}$$

又由于

$$78 \equiv 1 \pmod 7, \ 78 \equiv 0 \pmod{13}$$

$$14 \equiv 1 \pmod{13}, \ 14 \equiv 0 \pmod 7$$

则

$$x \equiv 78 + 14 \equiv 1 \pmod{91}$$

$$x \equiv 14 - 78 \equiv 27 \pmod{91}$$

$$x \equiv 78 - 14 \equiv 64 \pmod{91}$$

$$x \equiv -78 - 14 \equiv 90 \pmod{91}$$

综上，$\mathbb{Z}_{91}$ 中 $\bar{1}$ 的全部平方根为 $\bar{1}, \overline{27}, \overline{64}, \overline{90}$。

习题 2.3

1. 设 F 是一个代数封闭域 (即 $F[x]$ 中每一个不可约多项式都是一次多项式)，求 $F[x]$ 的全部素理想。

解答. 由于 $F[x]$ 为主理想整环，则

$$P\text{为}F[x]\text{的素理想} \iff P = (p(x))\text{或}(0)$$

其中 $p(x)$ 为 $F[x]$ 中的不可约多项式，则 $F[x]$ 的全部素理想为

$$(0),\ x+c$$

其中 $c \in F$。

4. 设 $m = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$，其中 $p_1, p_2, \cdots, p_s$ 是两两不等的素数，$r_i > 0, i = 1, 2, \cdots, s$。求 $\mathbb{Z}/(m)$ 的全部素理想。

解答. 由理想对应定理知，

$$\{I : I\text{为}\mathbb{Z}/(m)\text{的理想}\} \cong \{I\text{为}\mathbb{Z}\text{的理想} : (m) \subset I\} \cong \{(k) : (m) \subset (k),\ k \in \mathbb{N}\}$$

设 $\mathbb{Z}/(k)$ 为 $\mathbb{Z}/(m)$ 的素理想，由环同构第二定理知

$$(\mathbb{Z}/(m))/((k)/(m)) \cong \mathbb{Z}/(k)$$

则 $\mathbb{Z}/(k)$ 为整环 $\iff (k)$ 为 $\mathbb{Z}$ 的素理想 $\iff k$ 为素数。

所以 $\mathbb{Z}/(k)$ 为 $\mathbb{Z}/(m)$ 的素理想，当且仅当，k 为素数且 $(m) \subset (k) \iff k|m$。

综上，$\mathbb{Z}/(m)$ 的所有素理想为

$$\mathbb{Z}/(p_i) \quad i = 1, 2, \cdots, s$$

10. 设 R 是有单位元 $1(\neq 0)$ 的交换环，证明：R 的极大理想一定是素理想。

证明.

$$M\text{为}R\text{的极大理想} \iff R/M\text{为域} \Rightarrow R/M\text{为整环} \iff M\text{为}R\text{的素理想}$$

□

12. 设 R 是偶数环 $2\mathbb{Z}$，证明：$4\mathbb{Z}$ 是 R 的一个极大理想，但是 $R/4\mathbb{Z}$ 不是域。

证明. 存在 I 为 $2\mathbb{Z}$ 的理想，且 $4\mathbb{Z} \subsetneq I$，则存在 $k \in \mathbb{Z}$，使得 $2(2k+1) = 4k+2 \in I$，由于 $4k \in 4\mathbb{Z} \subset I$，则 $2 \in I$，所以 $\forall k \in \mathbb{Z}$，有 $2k \in I$，则 $I = 2\mathbb{Z} = R$，故 $4\mathbb{Z}$ 为 R 的极大理想。

由于 $R/4\mathbb{Z} = \{4\mathbb{Z}, 2+4\mathbb{Z}\}$，其中 $4\mathbb{Z}$ 为 $R/4\mathbb{Z}$ 中的零元，则 $(2+4\mathbb{Z})(2+4\mathbb{Z}) = 4\mathbb{Z}$，则 $2+4\mathbb{Z}$ 为 $R/4\mathbb{Z}$ 中的非零的零因子，故 $R/4\mathbb{Z}$ 不是域。 □

习题 2.4

1. 构造含 9 个元素的有限域，写出它的全部元素。

解答. $\mathbb{Z}_3$ 为含有 3 个元素的有限域，令 $m(x)=x^2+1$，由于 $m(\bar{0})=\bar{1}, m(\bar{1})=\bar{2}, m(\bar{2})=\bar{2}$，所以 $m(x)$ 是 $\mathbb{Z}_3[x]$ 上的不可约多项式，则 $\mathbb{Z}_3[x]/(m(x))$ 为含有 $3^2=9$ 个元素的有限域。

如下定义 $\mathbb{Z}_3$ 到 $\mathbb{Z}_3[x]/(m(x))$ 上的映射 σ：

$$\sigma:\mathbb{Z}_3\to\mathbb{Z}_3[x]/(m(x))$$
$$\bar{a}\mapsto\bar{a}+(m(x))$$

不难验证，σ 为单同态，所以可以在 $\mathbb{Z}_3[x]/(m(x))$ 中将 $\bar{a}$ 与 $\bar{a}+(m(x))$ 视为相同的元素，记 $u=x+(m(x))$，则

$$\begin{aligned}\mathbb{Z}_3[x]/(m(x)) &= \{c_0+c_1u : c_0,c_i\in\mathbb{Z}_3\}\\ &= \{\bar{0},\bar{1},\bar{2},u,\bar{1}+u,\bar{2}+u,\bar{2}u,\bar{1}+\bar{2}u,\bar{2}+\bar{2}u\}\end{aligned}$$

5. 证明 $t=\sqrt{2}+\sqrt{3}$ 是一个代数数，并且求 t 在 $\mathbb{Q}$ 上的极小多项式。

证明. 由于

$$t^2=5+2\sqrt{6}\Rightarrow(t^2-5)^2=24\Rightarrow t^4-10t^2+1=0$$

所以 t 为代数数，设 $m(x)=x^4-10x^2+1=(x^2)^2-10x^2+1$，将 $m(x)$ 视为 $\mathbb{R}$ 上的多项式，则 $x^2=5\pm2\sqrt{6}=(\sqrt{2}+\sqrt{3})^2$或$(\sqrt{2}-\sqrt{3})^2$，所以

$$m(x)=(x-(\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(\sqrt{3}-\sqrt{2}))$$

则 $m(x)$ 在 $\mathbb{Q}$ 中没有一次或二次多项式作为因子，故 $m(x)$ 不可约且是首一多项式，则 $m(x)$ 为 t 在 $\mathbb{Q}$ 上的极小多项式。 □

11. 证明：对于任意整数 m, n，复数 $m+ni$ 是代数整数，称这种形式的代数整数为**高斯整数**。

证明. 设 $t = m + ni$，则

$$(t-m)^2 = -n^2 \Rightarrow t^2 - 2mt + m^2 + n^2 = 0$$

则复数 $m+ni$ 为整系数多项式 $x^2 - 2mx + m^2 + n^2$ 的根，则 $m+ni$ 为代数整数。 □