矩阵理论作业 2

刘彦铭 学号:122033910081

编辑日期: 2022 年 10 月 3 日

1. Page 16 习题 1

   课上已经讲过解法:

   设 $f(x), g(x) \in \mathbb{F}[x]$, $(f(x), g(x)) = 1 \Rightarrow \exists\, u(x), v(x) \in \mathbb{F}[x]$ 使得 $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$.

   将上述多项式的 x 代换为 x^n 即得: $f(x^n) \cdot u(x^n) + g(x^n) \cdot v(x^n) = 1$.

   容易验证 $u(x^n), v(x^n) \in \mathbb{F}[x]$, 这就证明了 $(f(x^n), g(x^n)) = 1$.

2. Page 16 习题 4

   (1) 假设 $p(x) \in \mathbb{Q}[x]$ 也是满足 $p(\alpha) = 0$ 的最低次的首一多项式.

   由于都是最低次的，所以有 $\deg m_\alpha = \deg p$.

   作带余除法：存在多项式 $u, v \in \mathbb{Q}[x]$ 使得 $m_\alpha = u \cdot p + v$, 其中 $v = 0$ 或者 $\deg v < \deg p$.

   注意到 $v(\alpha) = m_\alpha(\alpha) - u(\alpha) \cdot p(\alpha) = 0$, 所以有 $v = 0$; 否则存在非零的多项式 $v \in \mathbb{Q}[x]$ 使得 $v(\alpha) = 0$ 且 $\deg v < \deg p$，这与 p 最低次的假设矛盾。

   所以 $m_\alpha = u \cdot p$. 因为 $\deg u = \deg m_\alpha - \deg p = 0$ 且 m_α, p 均首一, 所以 $u = 1$

   因此 $m_\alpha = p$, 这就说明了 m_α 的唯一性

   (2) 只需说明 $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ 是 $\mathbb{Q}[\alpha]$ 的一组基:

   - 线性无关:
     对任意的 $c_0, c_1, c_2, \cdots, c_{m-1} \in \mathbb{Q}$, 若 $f(\alpha) = \sum_{0 \le i < m} c_i \alpha^i = 0$, 由于 $\deg f = m - 1 < \deg m_\alpha$, 所以由 m_α 的定义知 $f = 0$, 即 $c_i = 0, \forall\ 0 \le i < m$. 这就证明了 $\{\alpha^i\}, 0 \le i < m$ 的线性无关性。
   - 可表示性:
     对 $\mathbb{Q}[\alpha]$ 上的任意一个元素 β, 由 $\mathbb{Q}[\alpha]$ 的生成方式可以知道, 存在多项式 $f \in \mathbb{Q}[x]$, 使得 $\beta = f(\alpha)$
     考虑带余除法 $f = q \cdot m_\alpha + r$ 其中 $q, r \in \mathbb{Q}[x]$, $r = 0$ 或 $\deg r < \deg m_\alpha = m$.
     于是 $\beta = f(\alpha) = q(\alpha) \cdot m_\alpha(\alpha) + r(\alpha) = r(\alpha) = \sum_{0 \le i < m} c_i \alpha^i$. 这就说明了 $\mathbb{Q}[\alpha]$ 上的任一元素都能由 $\{\alpha^i\}, 0 \le i < m$ 线性表示

3. Page 16-17 习题 5 (尝试做一下)

   (1) 设 p 是 R 上的任意一个素元。对于任意的非零的 $p_1, p_2 \in R$, 如果 $p = p_1 p_2$, 那么有 $p \mid p_1 p_2$. 由于 p 是素元，所以 $p \mid p_1$ 或者 $p \mid p_2$ 。不失一般性，假设 $p \mid p_1$ ，于是存在 $k \in R$, 使得 $p_1 = kp = kp_1p_2 = (kp_2)p_1$ (运用 R 上的乘法交换律和结合律)。由于 R 是一个整环（这里略去证明）没有零因子，所以 $p_1 = (kp_2)p_1 \Rightarrow (kp_2 - 1)p_1 = 0 \Rightarrow kp_2 = 1$, 这就证明了 p_2 是可逆元。

(2) **命题 1** 主理想整环 R 上的不可分解元都是素元。

证明. 假设 $c \in R$ 是一个不可分解元。对于主理想整环 R 上的任意理想 (a), 如果 $(c) \subset (a) \subset R$, 那么存在 $k \in R, c = ka$. 由于 c 是不可分解的，所以 k 是可逆元即 $(c) = (a)$ 或者 a 是可逆元即 $(a) = R$ 。这就验证了 (c) 是一个极大理想。

假设不可分解元 c 不是素元，那么存在非零的 $a, b \in R$ 使得 $c \mid ab$ 但 $c \nmid a$, $c \nmid b$.

$c \nmid a \Rightarrow a \notin (c) \Rightarrow (c) \subset (a, c) \subset R$ 且 $(c) \neq (a, c)$. 其中 (a, c) 表示由 a, c 生成的理想。由于 (c) 是极大的，所以 $(a, c) = R$. 所以存在 $x, y \in R$ 使得 $ax + cy = 1$; 同理，存在 $n, m \in R$ 使得 $bn + cm = 1$. 稍做变换可以得到 $ab \cdot xn + c \cdot (y + m - ymc) = 1$. 说明 ab 与 c 生成的理想 $(ab, c) = (1) = R$. 但由于 $c \mid ab$ 所以 $(ab, c) = (c)$. 这就导出了 c 是单位元的平凡情形。所以 c 不是素元的假设不成立。 □

命题 2 欧几里得整环都是主理想整环。

证明. 设 I 是一欧几里得整环 R 上的理想，设 $\phi : R \to \mathbb{N}$ 是定义在这一欧几里得环上的度量。可以从 I 中选取出度量最小的元素 $a \in I$. 对于任意的 $b \in I$, 由于在欧几里得环上存在 $q, r \in R$ 使得 $b = q \cdot a + r$, 其中 $r = 0$ 或者 $\phi(r) < \phi(a)$. 显然 $r = b - q \cdot a \in I$, 所以 $\phi(r) < \phi(a)$ 不能成立，因此 $r = 0$。这就说明了 $I \subset (a) \subset I$, 即 $I = (a)$ 是可由 a 生成的主理想。 □

由命题 1、2 知，只需要验证 $R \in \{\mathbb{Z}, \mathbb{F}[x], \mathbb{Z}[i]\}$ 是欧几里得环。其中 $\mathbb{Z}, \mathbb{F}[x]$ 是十分常见的欧几里得环，这里略去验证，只验证 $\mathbb{Z}[i]$ 是欧几里得环:

证明. 定义度量 $\phi : \mathbb{Z}[i] \to \mathbb{N}, \phi(a) = |a|^2 = a \cdot \bar{a}$. 对于任意非零的 $a, b \in \mathbb{Z}[i] \subset \mathbb{Q}[i]$, $\dfrac{a}{b} = \dfrac{a\bar{b}}{b\bar{b}} = x + yi$, 其中 $x, y \in \mathbb{Q}$. 取距离 x, y 最近的整数 m, n, 有 $|m - x| \leq 0.5, |n - y| \leq 0.5$. 构造 $q = m + ni \in \mathbb{Z}[i]$, $r = a - qb \in \mathbb{Z}[i]$, 使得 $a = qb + r$, 且其中 $r = 0$ 或者 $\phi(r) = \phi(((x - m) + (y - n)i) \cdot b) = \phi((x - m) + (y - n)i) \cdot \phi(b) \leq 0.5 \cdot \phi(b) < \phi(b)$. □

(3) $(2 + \sqrt{-5}) \nmid 3$ 但 $(2 + \sqrt{-5}) \mid 3 \times 3$. 所以 $2 + \sqrt{-5}$ 不是素元。同理 $2 - \sqrt{-5}, 3$ 都不是素元。考虑到在 $\mathbb{Z}[\sqrt{-5}]$ 上复数的模长的相关定义和性质仍然成立，故枚举 $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ 可能的因子时，只需要考虑模长平方小于等于 9 的，即只考虑 $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ 其中 $a, b \in \mathbb{Z}, a^2 + 5b^2 \leq 9$. 简单的穷举即可验证他们都是不可分解元。