第二次作业解答

习题 1. 设 $f = x^5 - 12x^3 + 36x - 12 \in \mathbb{Q}[x]$. 判断 f 是不是不可约多项式.

解. 考虑素数 $p = 3$。多项式 f 的各项系数为:

$$a_5 = 1,\ a_4 = 0,\ a_3 = -12,\ a_2 = 0,\ a_1 = 36,\ a_0 = -12.$$

显然 $p \nmid a_5$，且 p 整除所有其他系数 a_4, a_3, a_2, a_1, a_0（因为 0 可被任何素数整除，而 $-12, 36$ 都是 3 的倍数)。同时 $p^2 = 9$ 不整除常数项 $a_0 = -12$（因为 $9 \nmid 12$)。由 Eisenstein 判别法，f 在 $\mathbb{Q}$ 上不可约。 □

习题 2. 设 $f(x) \in \mathbb{R}[x] \setminus \mathbb{R}$ 且 f 没有实根. 利用微积分和代数知识给出 $f(x)$ 恒正或恒负的两个不同的证明.

解. **证明一（微积分方法)：**由于 $f(x)$ 是多项式，其次数至少为 1。考虑极限行为:

$$\lim_{x\to+\infty} f(x) = \text{sgn(首项系数)}\cdot\infty, \quad \lim_{x\to-\infty} f(x) = \text{sgn(首项系数)}\cdot(-1)^{\deg f}\cdot\infty.$$

若 $\deg f$ 为奇数，则两端极限符号相反，由介值定理必存在实根（是连续函数)，与无实根矛盾，故 $\deg f$ 为偶数。此时两端极限同号，均为 $+\infty$（若首项系数为正）或 $-\infty$（若首项系数为负)。不妨设 f 首项系数为正，则两端极限均为 $+\infty$，于是存在 $N > 0$，使得当 $|x| \geqslant N$ 时，$f(x) > 0$。现在我们说明当 $|x| < N$ 时，$f(x) > 0$：否则，存在 $|c| < N$，使得 $f(c) \leqslant 0$，但由 $f(x)$ 无实根，$f(c) \neq 0$，故 $f(c) < 0$，则由介值定理，存在 $c < b < N$，使得 $f(b) = 0$，与 $f(x)$ 无实根矛盾。因此 $f(x)$ 恒正（首项系数正）或恒负(首项系数负)。

证明二（代数方法)： f 是实系数多项式，无实根，故其所有复根均为非实数的共轭对。设 f 的首项系数为 $a \in \mathbb{R}$，则 f 可分解为

$$f(x) = a\prod_{i=1}^{m}(x - \alpha_i)(x - \overline{\alpha_i}),$$

其中 $\alpha_i \in \mathbb{C} \setminus \mathbb{R}$。每个二次因子

$$(x - \alpha_i)(x - \overline{\alpha_i}) = x^2 - 2\,\mathrm{Re}(\alpha_i)x + |\alpha_i|^2$$

的判别式 $4(\mathrm{Re}(\alpha_i)^2 - |\alpha_i|^2) = -4(\mathrm{Im}(\alpha_i))^2 < 0$，且二次项系数为 $1 > 0$，故该二次式恒正。于是 $f(x) = a \cdot$ (正因子乘积)。因此 $f(x)$ 的符号完全由 a

决定：若 $a>0$，则 $f(x)>0$ 对所有 $x\in\mathbb{R}$ 成立；若 $a<0$，则 $f(x)<0$ 对所有 $x\in\mathbb{R}$ 成立。 □

习题 3. 设 F 是域. 验证: $U\subset \mathrm{M}_n(F)$ 是不是子空间, 其中

(i) $U=\{A\in \mathrm{M}_n(F)\mid \mathrm{tr}(A)=0\}$,

(ii) $U=\{A\in \mathrm{M}_n(F)\mid \det(A)=0\}$,

(iii) $U=\{A\in \mathrm{M}_n(F)\mid AA^t=O\}$ 且 $F=\mathbb{R}$。

解. (i) 零矩阵的迹为 0，故 $0\in U$。对任意 $A,B\in U$，有 $\mathrm{tr}(A+B)=\mathrm{tr}\,A+\mathrm{tr}\,B=0$，故 $A+B\in U$。对任意 $c\in F$，$\mathrm{tr}(cA)=c\,\mathrm{tr}\,A=0$，故 $cA\in U$。因此 U 是子空间。

(ii) 零矩阵的行列式为 0，故 $0\in U$。但加法不封闭：取 $n=2$，$A=\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $B=\begin{pmatrix}0&0\\0&1\end{pmatrix}$, 则 $\det A=\det B=0$, 但 $A+B=I$, $\det I=1\neq 0$, 故 $A+B\notin U$。因此 U 不是子空间。

(iii) 当 $F=\mathbb{R}$ 时, 若 $A\in U$, 则 $AA^t=O$。考虑 $(AA^t)_{ii}=\sum_{j=1}^n a_{ij}^2=0$, 故对每个 i,j 有 $a_{ij}=0$，即 $A=O$。因此 $U=\{O\}$，它显然是子空间（平凡子空间）。 □

习题 4. 设 F 是域, $f,g\in \mathrm{Map}(S,F)$. 证明: f 和 g 线性无关当且仅当存在 $x,y\in S$ 使得

$$\det\begin{pmatrix}f(x)&g(x)\\f(y)&g(y)\end{pmatrix}\neq 0.$$

解. 必要性：假设 f,g 线性无关。若对任意 $x,y\in S$ 行列式均为零, 则任意两点处的向量 $(f(x),g(x))$ 与 $(f(y),g(y))$ 线性相关。取一个使得 $(f(x_0),g(x_0))\neq(0,0)$ 的点 x_0 (这样的点存在, 否则 $f=g=0$, 线性相关)。则对任意 $y\in S$, 有 $(f(y),g(y))$ 与 $(f(x_0),g(x_0))$ 共线，即存在 $\lambda_y\in F$ 使得 $(f(y),g(y))=\lambda_y(f(x_0),g(x_0))$。取非零向量 $(\alpha,\beta)\in F^2$ 满足 $\alpha f(x_0)+\beta g(x_0)=0$ (即垂直于 $(f(x_0),g(x_0))$)，则对任意 y，$\alpha f(y)+\beta g(y)=\lambda_y(\alpha f(x_0)+\beta g(x_0))=0$, 故 $\alpha f+\beta g=0$，这与 f,g 线性无关矛盾。因此存在 x,y 使得行列式非零。

充分性：设存在 x,y 使行列式非零, 即向量 $(f(x),g(x))$ 与 $(f(y),g(y))$ 线性无关。若 f,g 线性相关, 则存在不全为零的 $\alpha,\beta\in F$ 使得 $\alpha f+\beta g=0$, 从而对任意 $z\in S$ 有 $\alpha f(z)+\beta g(z)=0$。特别地，$\alpha f(x)+\beta g(x)=0$ 且

$\alpha f(y)+\beta g(y)=0$，这意味着 (α,β) 同时与两个线性无关的向量正交，故 $(\alpha,\beta)=(0,0)$，矛盾。因此 f,g 线性无关。 □

习题 5. 设 $V_1,\dots,V_k$ 是线性空间 V 的子空间, 且 $V_1+\cdots+V_k$ 是直和. 证明:

(i) 如果 $\mathbf{v}_i\in V_i\setminus\{\mathbf{0}\}$, $i=1,\dots,k$, 则 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性无关,

(ii) 如果 $S_i\subset V_i$ 是线性无关集, $i=1,\dots,k$, 则 $S_1\cup\cdots\cup S_k$ 是线性无关集.

解. (i) 设 $\sum_{i=1}^k a_i\mathbf{v}_i=\mathbf{0}$，其中 $a_i\in F$。由于 $a_i\mathbf{v}_i\in V_i$，而和是直和，故零向量的表示唯一，从而每个 $a_i\mathbf{v}_i=\mathbf{0}$。又 $\mathbf{v}_i\neq\mathbf{0}$，所以 $a_i=0$ 对每个 i 成立。因此 $\mathbf{v}_1,\dots,\mathbf{v}_k$ 线性无关。

(ii) 任取 $S=S_1\cup\cdots\cup S_k$ 中的有限个向量，设它们为 $\mathbf{u}_1,\dots,\mathbf{u}_m$，并设每个 $\mathbf{u}_j$ 属于某个 V_{i_j}。将属于同一个 V_i 的向量合并：令 $\mathbf{w}_i$ 为所有来自 V_i 的向量的线性组合（系数取自对应的 $\mathbf{u}_j$ 的系数），则 $\mathbf{w}_i\in V_i$，且 $\sum_{i=1}^k\mathbf{w}_i=\mathbf{0}$。由直和性质，每个 $\mathbf{w}_i=\mathbf{0}$。而 $\mathbf{w}_i$ 是 S_i 中向量的线性组合，且 S_i 线性无关，故这些系数全为零。因此所有 $\mathbf{u}_j$ 的系数均为零，即 S 线性无关。 □

唯一分解整环

定义 1 (理想)**.** 设 R 是一个环。

- R 的一个非空子集 I 称为 R 的一个**左理想**，如果：

  1. 对任意 $a,b\in I$，有 $a-b\in I$；
  2. 对任意 $r\in R$，$a\in I$，有 $ra\in I$。

  若将条件 2 改为 $ar\in I$，则称为**右理想**。若 I 同时是左理想和右理想，则称 I 为**双边理想**，简称为**理想**。在交换环中，左右理想没有区别，统称为理想。

- 设 $S\subseteq R$，则包含 S 的最小理想称为由 S **生成的理想**，记作 (S)。当 $S=\{a_1,\dots,a_n\}$ 时，记作 $(a_1,\dots,a_n)$。特别地，由一个元素生成的理想 $(a)=\{ra\mid r\in R\}$ 称为**主理想**。

定义 2. 设 R 是一个整环（交换、含幺、无零因子）。

- **单位**：元素 $u \in R$ 称为单位，若存在 $v \in R$ 使得 $uv = 1$。全体单位构成乘法群 $U(R)$。
- **相伴**：若 $a = ub$ 对某个单位 u 成立，则称 a 与 b 相伴，记作 $a \sim b$。
- **不可约元**：非零非单位的元素 $p \in R$ 称为不可约元，若 $p = ab$ 蕴含 a 或 b 是单位。
- **素元**：非零非单位的元素 $p \in R$ 称为素元，若 $p \mid ab$ 蕴含 $p \mid a$ 或 $p \mid b$。

注. 在整数环 $\mathbb{Z}$ 中，不可约元就是通常的素数（及其相反数），而素元也是素数。两者是一致的。但在一般整环中，二者不一定等价。

定义 3 (唯一分解整环)**.** 设 R 是一个整环。

- 称 R 为**唯一分解整环**（Unique Factorization Domain, UFD），如果满足：
  1. 每个非零非单位的元素 $a \in R$ 都可以写成有限个不可约元的乘积 $a = p_1 p_2 \cdots p_n$；
  2. 若有两种分解 $a = p_1 \cdots p_n = q_1 \cdots q_m$（其中 p_i, q_j 均为不可约元），则 $n = m$ 且存在一个置换 σ 使得 p_i 与 $q_{\sigma(i)}$ 相伴（即相差一个单位）。

定理 1. 在整环 R 中，每个素元都是不可约元。

证明. 设 p 是素元，且 $p = ab$。则 $p \mid ab$，由素元定义知 $p \mid a$ 或 $p \mid b$。不妨设 $p \mid a$，则 $a = pc$ 对某个 $c \in R$。代入 $p = ab$ 得 $p = pcb$，由于 $p \neq 0$ 且 R 为整环，消去 p 得 $1 = cb$，故 b 是单位。同理若 $p \mid b$ 则 a 为单位。因此 p 不可约。 □

注. 逆命题一般不成立。存在整环中的不可约元不是素元，例如在环 $R = \mathbb{Z}[\sqrt{-5}]$ 中，考虑元素 2。可以验证 2 是不可约元，但 $2 \mid (1+\sqrt{-5})(1-\sqrt{-5}) = 6$，而 2 不整除 $1 + \sqrt{-5}$ 也不整除 $1 - \sqrt{-5}$，故 2 不是素元。

定理 2. 在唯一分解整环（UFD）中，不可约元与素元等价。

证明. 我们只需证明 UFD 中的不可约元一定是素元。设 p 是唯一分解整环 R 中的不可约元，且 $p \mid ab$，即存在 $d \in R$ 使得 $ab = pd$。我们需要证明 $p \mid a$ 或 $p \mid b$。

考虑 a, b, d 的不可约因子分解。由于 R 是 UFD，每个非零非单位元都有唯一的不可约因子分解（在相伴意义下）。- 若 a 或 b 是单位，则结论显然成立（例如若 a 是单位，则 $p \mid ab$ 意味着 $p \mid b$）。- 若 a 或 b 是零，结论也显然成立。

下设 a, b 均为非零非单位元。设

$$a = p_1 p_2 \cdots p_m, \quad b = q_1 q_2 \cdots q_n, \quad d = r_1 r_2 \cdots r_k$$

其中 p_i, q_j, r_t 均为不可约元。则

$$ab = (p_1 \cdots p_m)(q_1 \cdots q_n) = p \cdot (r_1 \cdots r_k).$$

现在，p 本身也是不可约元。由 UFD 中因子分解的唯一性，p 必须与某个 p_i 或某个 q_j 相伴（因为等式左边和右边的不可约因子在相伴意义下必须一一对应）。若 p 与某个 p_i 相伴，则 $p \mid a$。若 p 与某个 q_j 相伴，则 $p \mid b$。

因此 $p \mid a$ 或 $p \mid b$，即 p 是素元。 □

定义 4 (主理想整环)**.** 整环 R 称为**主理想整环** (Principal Ideal Domain, PID)，如果 R 的每个理想都是主理想，即对 R 的任意理想 I，存在 $a \in R$ 使得 $I = (a) = \{ra \mid r \in R\}$，我们称这样的理想为**主理想**。

例子 1. 常见的主理想整环：

- **整数环** $\mathbb{Z}$：任何理想都是某个非负整数生成的主理想。
- **域上的一元多项式环** $F[x]$：由于 $F[x]$ 是欧式环（见后），故是主理想整环。
- **高斯整数环** $\mathbb{Z}[i]$ 也是主理想整环（实为欧式环）。
- 非主理想整环的例子：$\mathbb{Z}[x]$ 不是主理想整环，因为理想 $(2, x)$ 不是主理想。

定理 3. 主理想整环是唯一分解整环。

证明. 我们需要证明两件事：

1. **存在性**：每个非零非单位元都可以写成有限个不可约元的乘积。
2. **唯一性**：如果两种分解 $p_1 \cdots p_m = q_1 \cdots q_n$（$p_i, q_j$ 不可约），则 $m = n$ 且适当重排后 p_i 与 q_i 相伴。

引理 1（真因子链有限）：设 R 是 PID。若 $a_1, a_2, a_3, \ldots$ 是 R 中的非零非单位元序列，且每个 a_{i+1} 是 a_i 的真因子（即 $a_i = a_{i+1}b_{i+1}$ 且 b_{i+1} 非单位），则序列必然有限。

引理 1 的证明. 由 $a_{i+1} \mid a_i$ 且 a_{i+1} 不是 a_i 的相伴元，可得主理想链：

$$(a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \cdots$$

考虑这些理想的并集 $I = \bigcup_{i=1}^{\infty}(a_i)$。易证 I 是 R 的理想。由于 R 是 PID，存在 $b \in R$ 使得 $I = (b)$。则 b 属于某个 (a_k)，从而 $(b) \subseteq (a_k)$。但另一方面，$I = (b)$ 包含所有 (a_i)，故 $(a_k) \subseteq (b)$。因此 $(a_k) = (b) = I$。这意味着对于所有 $i \geq k$，有 $(a_i) = (a_k)$，从而链在 k 项后稳定。这与真包含关系矛盾。因此序列必须有限。 □

为了下面两个引理，我们补充两个定义：称 R 中的理想 I 是**极大理想**，如果 $I \subsetneq R$ 且对任意真理想 J 满足 $R \supsetneq J \supseteq I$，都有 $I = J$；称 R 中的理想 $\mathfrak{p}$ 是**素理想**，如果对任意 $x, y \in R$，只要 $xy \in \mathfrak{p}$，就有 $x \in \mathfrak{p}$ 或者 $y \in \mathfrak{p}$。

引理 2（不可约元生成极大理想）：设 R 是 PID，$p \in R$ 是不可约元，则 (p) 是极大理想。

引理 2 的证明. 设 $(p) \subseteq I \subseteq R$，$I$ 是理想。由于 R 是 PID，存在 $a \in R$ 使得 $I = (a)$。则 $p \in (a)$，故 $p = ab$ 对某个 $b \in R$。由 p 不可约知 a 或 b 是单位。若 a 是单位，则 $I = R$。若 b 是单位，则 $a \sim p$，从而 $(a) = (p)$。因此 (p) 极大。 □

引理 3（极大理想是素理想）：在任意交换环中，极大理想都是素理想。

引理 3 的证明. 设 M 是极大理想，$ab \in M$ 但 $a \notin M$。考虑理想 $M + (a)$。由于 $a \notin M$，$M + (a)$ 真包含 M，由极大性得 $M + (a) = R$。则存在 $m \in M$，$r \in R$ 使得 $m + ra = 1$。乘以 b 得 $mb + rab = b$。由于 $mb \in M$，$rab \in M$（因 $ab \in M$），故 $b \in M$。因此 M 是素理想。 □

由引理 2 和引理 3 立即得到：在 PID 中，不可约元生成的理想是素理想，从而不可约元是素元。

存在性：设 $a \in R$ 是非零非单位元。若 a 本身是不可约元，则分解已经存在。否则 a 可分解为 $a = a_1 b_1$，其中 a_1, b_1 均非单位。若 a_1, b_1 都是不可约元，则得到分解。否则继续分解其中可约的因子。若此过程无限进行，则会产生一个无限的真因子链，与引理 1 矛盾。因此有限步后所有因子都成为不可约元，从而得到 a 的不可约因子分解。

唯一性：假设 a 有两种不可约因子分解：

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

其中 p_i, q_j 均为不可约元。我们对 m 使用数学归纳法。

当 $m = 1$ 时，$a = p_1$ 是不可约元。此时 $p_1 = q_1 \cdots q_n$。若 $n > 1$，则 p_1 被分解为多个非单位元的乘积，这与 p_1 不可约矛盾。故 $n = 1$，且 $p_1 = q_1$，唯一性成立。

假设结论对分解长度小于 m 的情形成立，考虑 $m \geq 2$ 的情形。由 $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ 知 $p_1 \mid q_1 \cdots q_n$。由于在 PID 中不可约元就是素元，p_1 是素元。因此 p_1 整除某个 q_j。重排下标可设 $p_1 \mid q_1$。由于 q_1 是不可约元，p_1 与 q_1 相伴，即存在单位 u 使得 $q_1 = u p_1$。代入原等式：

$$p_1 p_2 \cdots p_m = (u p_1) q_2 \cdots q_n$$

消去 p_1（整环中可消去非零元）得：

$$p_2 \cdots p_m = u q_2 \cdots q_n$$

右边 u 是单位，因此 $u q_2 \cdots q_n$ 仍是一组不可约元的分解（乘以单位不改变不可约性）。于是 $p_2 \cdots p_m$ 有两种分解，长度分别为 $m-1$ 和 $n-1$。由归纳假设，$m-1 = n-1$，即 $m = n$，且适当重排后 $p_2, \ldots, p_m$ 分别与 $q_2, \ldots, q_m$ 相伴。加上已证明的 p_1 与 q_1 相伴，唯一性得证。

综合存在性与唯一性，我们完成了 PID 是 UFD 的证明。 □

定义 5 (欧氏整环)**.** 整环 R 称为**欧氏整环**（Euclidean Domain, ED），如果存在一个函数 $\varphi : R \setminus \{0\} \to \mathbb{N}$（称为欧式函数）满足：

1. 对任意 $a, b \in R$，$b \neq 0$，存在 $q, r \in R$ 使得

$$a = bq + r,$$

且要么 $r = 0$，要么 $\varphi(r) < \varphi(b)$。

2. 对任意非零 $a, b \in R$，有 $\varphi(a) \le \varphi(ab)$。（有时条件 2 可省略，因为可以从带余除法推导出适当形式，但通常为了定义的一致性，我们保留它。）

例子 2. 常见的欧氏整环：

- **整数环** $\mathbb{Z}$：取 $\varphi(n) = |n|$。
- **域上的一元多项式环** $F[x]$：取 $\varphi(f) = \deg f$，并约定 $\varphi(0)$ 无定义或另作处理。
- **高斯整数环** $\mathbb{Z}[i]$：取 $\varphi(a+bi) = a^2 + b^2$。
- **域**本身是平凡的欧氏整环（所有非零元均为单位，可取常值函数）。

定理 4. 每个欧氏整环 R 都是主理想整环，从而是唯一分解整环。

证明. 设 I 是 R 的非零理想。选取 $b \in I \setminus \{0\}$ 使得 $\varphi(b)$ 最小（在欧式函数值中）。对任意 $a \in I$，由带余除法，存在 $q, r \in R$ 使得 $a = bq + r$，且 $r = 0$ 或 $\varphi(r) < \varphi(b)$。由于 $a, b \in I$，有 $r = a - bq \in I$。若 $r \neq 0$，则 $\varphi(r) < \varphi(b)$ 与 b 的极小性矛盾。故 $r = 0$，从而 $a = bq \in (b)$。因此 $I = (b)$ 是主理想。 □