PASSION 数学社：代数部分讲义

报告人：孙贾航

基础知识部分

我们首先介绍一些来自代数的基础概念。任何熟悉这些术语的人都应该能够理解以下内容。

环与环同态. 一个 **环 (ring)** 是一个具有乘法恒等元的交换环。一个从一个环到另一个环的 **环同态 (ring homomorphism)** 必须将第一个环的乘法恒等元映射为第二个环的乘法恒等元。

一个 **整环 (domain)** 是一个在乘法下没有零因子的环。一个 **域 (field)** 是每个非零元素都有逆元的环。

$\mathbb{Z}$ 表示整数域 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 分别表示有理数、实数和复数域

任何环 R 都有一个商域 K，即包含 R 作为子环的一个域。在 K 中，任何元素都可以写成 R 的元素的比值。任何从环 R 到域 L 的 **单射环同态**可以扩展为从 K 到 L 的环同态。

多项式环. 对于任意环 R，$R[X]$ 表示系数在 R 中的多项式环。一个非零多项式

$$\sum a_i X^i$$

的次数是最大的整数 d，使得 $a_d \neq 0$；如果 $a_d = 1$，则称该多项式是 **首一的 (monic)**。

多元多项式环 $R[X_1, \ldots, X_n]$ 表示在多个变量上的多项式。对于 $n = 2$ 或 $n = 3$，我们也常写为 $R[X, Y]$ 或 $R[X, Y, Z]$。单项式为：

$$X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}, \quad i_j \geq 0.$$

任何 $F \in R[X_1, \ldots, X_n]$ 都可以唯一表示为：

$$F = \sum a_{(i)} X^{(i)},$$

其中 $X^{(i)}$ 为单项式，$a_{(i)} \in R$ 为系数。我们称 F 为 **齐次多项式 (homogeneous polynomial)**，如果它的所有非零项都具有相同次数。

Date: 2024 年 10 月 27 日.

整环和 UFD. 一个元素 $a \in R$ 是 **不可约的 (irreducible)**，如果它既不是单位元也不是零元，并且如果 $a = bc$，则 b 或 c 是单位元。

一个环 R 是一个 **唯一分解整环 (UFD)**，如果 R 的每个非零元素都可以唯一分解为不可约元素的乘积。

如果 R 是一个 UFD，且 K 是它的商域，那么 $K[X]$ 中的任何不可约元素在 $R[X]$ 中也是不可约的。这意味着，如果两个多项式 F 和 G 在 $R[X]$ 中没有共同因子，则它们也在 $K[X]$ 中没有共同因子。

设 R 是一个整环，则 $\deg(FG) = \deg(F) + \deg(G)$。环 $R[X_1, \ldots, X_n]$ 是 $R[X_1, \ldots, X_{n-1}]$ 的子环，并且 $R[X_1, \ldots, X_n]$ 具有如下性质：如果 φ 是从 R 到环 S 的一个环同态，且 $s_1, \ldots, s_n$ 是 S 中的元素，那么 φ 可以唯一扩展为一个从 $R[X_1, \ldots, X_n]$ 到 S 的环同态 $\tilde{\varphi}$，使得 $\tilde{\varphi}(X_i) = s_i$，对于 $1 \leq i \leq n$。F 在 $\tilde{\varphi}$ 下的像记作 $F(s_1, \ldots, s_n)$。环 $R[X_1, \ldots, X_n]$ 与 $R[X_1, \ldots, X_{n-1}][X_n]$ 是典范同构的。

环 R 中的一个元素 a 是 **不可约的 (irreducible)**，如果它既不是单位元也不是零元，并且对于任何分解 $a = bc$，其中 $b, c \in R$，要么 b 要么 c 是单位元。一个环 R 是 **唯一分解整环 (UFD)**，如果 R 中的每个非零元素都可以唯一地分解为不可约元素的乘积。

如果 R 是一个 UFD 且其商域为 K，那么（根据高斯引理）$K[X]$ 中的任何不可约元素在 $R[X]$ 中也不可约；这意味着，如果 F 和 G 在 $R[X]$ 中没有共同因子，那么它们在 $K[X]$ 中也没有共同因子。

如果 R 是 UFD，则 $R[X]$ 也是 UFD。因此，$k[X_1, \ldots, X_n]$ 是任意域 k 的 UFD。$k(X_1, \ldots, X_n)$ 表示 n 个变量的有理函数域。

如果 $\varphi : R \to S$ 是一个环同态，则 $\varphi^{-1}(0)$ 是 R 的一个理想，称为 φ 的 **核 (kernel)**，记作 $\ker(\varphi)$。如果 I 是一个理想且 $I \neq R$，则 I 是 **真理想 (proper ideal)**。如果没有任何比 I 更大的真理想包含于 I 中，则 I 是 **极大理想 (maximal ideal)**。一个理想 I 是 **素理想 (prime ideal)**，如果对于任意 $a, b \in R$，$ab \in I$ 蕴含 $a \in I$ 或 $b \in I$。

一个理想 I 是 **主理想 (principal ideal)**，如果它是由一个元素生成的。一个主理想环称为 **主理想整环 (PID)**。整数环 $\mathbb{Z}$ 和域上的多项式环 $k[X]$ 是主理想整环的例子。每个 PID 也是 UFD。一个 PID 中的主理想 $I = (a)$ 是素理想，当且仅当 a 是不可约的（或零）。

商环与剩余类环. 设 I 是 R 中的一个理想，商环 R/I 由 R 中模 I 的等价类组成，两个元素 $a, b \in R$ 等价，当且仅当 $a - b \in I$。包含 a 的等价类常记为 $\bar{a}$。商环 R/I 的类形成一个环，并且映射 $\pi : R \to R/I$，将每个元素映射到其 I-剩余类，是一个环同态。

如果 $\varphi : R \to S$ 是一个环同态且 $\varphi(I) = 0$，则存在一个唯一的环同态 $\bar{\varphi} : R/I \to S$，使得 $\varphi = \bar{\varphi} \circ \pi$。一个理想 I 是素理想，当且仅当 R/I 是一个整环；I 是极大理想，当且仅当 R/I 是一个域。

有理函数域与特征. 设 k 是一个域，I 是 $k[X_1,\dots,X_n]$ 的一个理想。则从 $k[X_1,\dots,X_n]$ 到 $k[X_1,\dots,X_n]/I$ 的商映射是一个环同态。我们将 k 看作 $k[X_1,\dots,X_n]/I$ 的子环，特别地，$k[X_1,\dots,X_n]/I$ 是 k 上的向量空间。

设 R 是一个整环。R 的 **特征 (characteristic)** 是使得 $1+\cdots+1$（共 p 次）等于 0 的最小正整数 p。如果不存在这样的 p，则 $\mathrm{char}(R)=0$。如果 $\varphi:\mathbb{Z}\to R$ 是环同态，则 $\ker(\varphi)=(p)$，其中 $p=\mathrm{char}(R)$。

令 I 是 R 的一个理想，则 R/I 表示 R 对 I 的 **商环 (quotient ring)**，其中两个元素 $a,b\in R$ 等价，当且仅当 $a-b\in I$。理想 I 是 **素理想 (prime ideal)**，如果 R/I 是一个整环；I 是 **极大理想 (maximal ideal)**，如果 R/I 是一个域。

复数域与代数闭包. 一个域 k 是 **代数闭域 (algebraically closed field)**，如果 $k[X]$ 中的任何非常数多项式都有根。$\mathbb{C}$ 是复数域，并且是代数闭域。

有限域. 有限域 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^*$ 是一个循环群，阶为 $q-1$。

分圆多项式和单位根. 在复数域 $\mathbb{C}$ 中，多项式 x^n-1 有 n 个根：

$$z_k=\cos\left(\frac{2\pi k}{n}\right)+i\sin\left(\frac{2\pi k}{n}\right),\quad k=0,1,\dots,n-1.$$

我们有以下推论：

$$x^{n-1}+x^{n-2}+\cdots+x+1=(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}).$$

将 ω^k 代入上式，我们得到：

$$1+\omega_n^k+\omega_n^{2k}+\cdots+\omega_n^{(n-1)k}=\begin{cases}0, & \text{如果} n\nmid k,\\ n, & \text{如果} n\mid k.\end{cases}$$

根据公式 $\omega_n^k=\exp\left(\frac{2\pi ik}{n}\right)$，单位根 $1,\omega_n,\omega_n^2,\dots,\omega_n^{n-1}$ 在乘法下构成一个 n 阶的循环群，记为 Ω_n。该群称为单位根群，其中 ω_n 是 Ω_n 的生成元。

分圆多项式的定义我们定义分圆多项式 $\Phi_n(x)$，它的根是 $x^n-1=\prod_{d\mid n}\Phi_d(x)$ 的所有 n 次单位根中的本原根。具体地，对于整数 n，$\Phi_n(x)$ 为以下形式的多项式：

$$\Phi_n(x)=\prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}}\left(x-e^{2\pi ik/n}\right).$$

$\Phi_n(x)$ 的系数为整数。$\Phi_n(x)$ 是不可约的。递归关系：$x^n-1=\prod_{d\mid n}\Phi_d(x)$。

习题部分

本报告涵盖竞赛中的典型题目和解题技巧，帮助大家理解常见的解法思路。

14 届初赛.

Problem 1. 设 $n \geq 2$ 为正整数，证明多项式

$$f(x) = x^n - x - 1$$

在有理数域 $\mathbb{Q}$ 上不可约。

Solution. 对于任意多项式

$$F(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,$$

我们用 $\widetilde{F}(x)$ 表示其互反多项式，即

$$\widetilde{F}(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1}x + a_m = x^{\deg F} F\left(\frac{1}{x}\right).$$

显然有 $\widetilde{\widetilde{F}}(x) = F(x)$，且若 $F(x) = G(x)H(x)$ 为多项式 $G(x)$ 和 $H(x)$ 的乘积，则 $\widetilde{F}(x) = \widetilde{G}(x)\widetilde{H}(x)$ 是 $\widetilde{G}(x)$ 和 $\widetilde{H}(x)$ 的乘积。

我们接下来证明 $f(x) = x^n - x - 1$ 在有理数域 $\mathbb{Q}$ 上不可约。

当 $n = 2$ 时，$f(x) = x^2 - x - 1$。该多项式在 $\mathbb{Q}$ 上显然不可约。

当 $n \geq 3$ 时，假设 $f(x)$ 在 $\mathbb{Q}$ 上可约，则存在整数系数多项式 $g(x), h(x) \in \mathbb{Z}[x]$ 使得

$$f(x) = g(x)h(x),$$

且 $1 \leq \deg g(x) = r < n$，这时 $\deg h(x) = n - r$。

进一步，由于 $f(x)$ 的首项系数为 *1*，常数项为 -1，可以假设 $g(x)$ 和 $h(x)$ 的首项系数均为 *1*，而它们的常数项只能是 ± 1。

令

$$k(x) = g(x)\widetilde{h}(x) \in \mathbb{Z}[x],$$

则有

$$\deg \widetilde{h}(x) = \deg h(x) = n - r.$$

所以 $\deg k(x) = n$，且

$$k(x)\widetilde{k}(x) = g(x)\widetilde{h}(x)\widetilde{g}(x)h(x) = f(x)\widetilde{f}(x). \tag{1}$$

由于

$$f(x) = x^n - x - 1,$$

所以其互反多项式为

$$\widetilde{f}(x) = -x^n - x^{n-1} + 1.$$

将 $k(x)$ 设为

$$k(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,$$

$$f(x)\widetilde{f}(x) = -x^{2n} - x^{2n-1} + x^{n+1} + 3x^n + x^{n-1} - x - 1.$$

$$k(x)\widetilde{k}(x) = b_n b_0 x^{2n} + b_n b_i x^{2n-i} + b_0 b_i x^{n+i} + 3x^n + b_n b_i x^i + b_0 b_i x^{n+i} + b_0 b_n.$$

其中 $b_n, b_0 = \pm 1$。比较 *(1)* 式两端 x^n 的系数，可得

$$b_0^2 + b_1^2 + \cdots + b_n^2 = 3.$$

由于 $b_i \in \{\pm 1\}$，所以有且只有一个 $b_i = \pm 1$，其余 $b_i = 0$。

观察 $k(x)\widetilde{k}(x)$ 的常数项，可得

$$b_0 = -b_n.$$

由于 $n \geq 3$，所以 $n - 1 \geq 2$，必有 $b_n = -b_0$，展开讨论 i 的情况即可得到

$$k(x) = \pm f(x) \quad 或 \quad k(x) = \pm\widetilde{f}(x).$$

若 $k(x) = \pm f(x)$，则 $\widetilde{h}(x) = \pm h(x)$，所以 $f(x)$ 和 $\widetilde{f}(x)$ 必有公共根。假设 α 是 $f(x)$ 和 $\widetilde{f}(x)$ 的公共根，则

$$\alpha^n = -\alpha^{n-1} + 1.\alpha^n = \alpha + 1.$$

这意味着

$$-\alpha^{n-1} = \alpha.$$

从这里我们可以验证 $\alpha = 1$ 或 $\alpha = 0$ 都不满足。因此，$f(x)$ 在 $\mathbb{Q}$ 上不可约。

Problem 2. 第二种解法

Solution (selmer). 为了证明定理 *1*，我们需要研究方程

$$x^n - (x + 1) = 0 \tag{2}$$

的根在复平面上的分布。

这种分布将会非常**规律**。

将下式代入 *(2)*：

$$x = re^{i\varphi} = r(\cos\varphi + i\sin\varphi),$$

并分别取实部和虚部，我们得到：

$$r^n \cos n\varphi = (r\cos\varphi + 1), \quad r^n \sin n\varphi = r\sin\varphi \tag{3}$$

通过对两边平方后相加，我们得到：

$$\cos\varphi = \frac{r^{2n} - r^2 - 1}{2r}. \tag{1}$$

292 ERNST S. SELMER

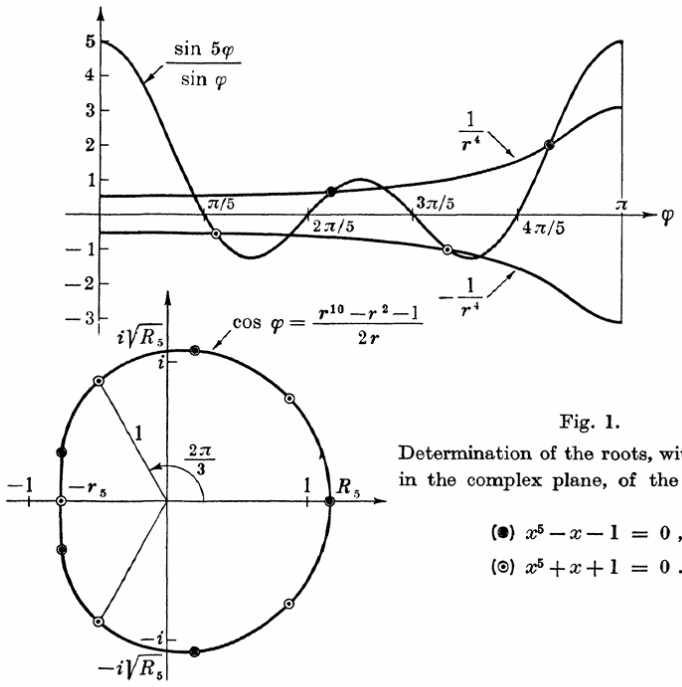

Fig. 1.
Determination of the roots, with location in the complex plane, of the equations

(●) $x^5 - x - 1 = 0$,
(◎) $x^5 + x + 1 = 0$.

(4.4) $R_n \approx 1 + n^{-1}\ln 2, \quad r_n \approx 1 - n^{-1}\ln n$.

图 1. n=5

这可以看作是一个在极坐标 (r, φ) 中的曲线方程，包含了 *(2)* 的所有根。*(2)* 的根的**辐角** φ 可以通过图形化方法容易地确定，如上图原论文给的图片。从 *(3)* 式的第二个等式，我们得到：

$$\frac{\sin n\varphi}{\sin \varphi} = \frac{1}{r^{n-1}}. \tag{2}$$

令 $f(x)$ 为 n 次的多项式，且其零点为 x_j $(j \neq 0)$。我们定义：

$$S(f(x)) = \sum_{j=1}^{n} \left(x_j - \frac{1}{x_j} \right), \tag{4}$$

即，所有根之和减去它们倒数之和。

显然，S 对于任何分解 $f(x)$ 的因子是**可加的**。作为一个对称函数，S 是有理数，并且如果 $f(x)$ 的标准形式中的常数项为 ± 1，则 S 是整数。在这种情况下，$f(x)$ 的任何分解因子的标准形式也必须有常数项 ± 1。

对于 *(2)* 中的多项式 $f(x)$，我们有：

$$S(f_k(x)) = 1 \tag{3}$$

另一方面，代入 $x_j = re^{i\varphi}$，$x_j^{-1} = r^{-1}e^{-i\varphi}$ 到 *(4)* 式中，并按共轭虚根成对求和，我们得到：

$$\sum{}' \left(x_j - \frac{1}{x_j} \right) = \sum_{0<\varphi<\pi} 2\frac{r^2-1}{r}\cos\varphi. \tag{4}$$

对于可能的实根，需要去掉系数 *2*。

对于多项式 $f_k(x)$, *(4)* 式的求和只在 $\pi/2 < \varphi < 2\pi/3$ 区间内包含负项，其中 $\cos\varphi < 0$，且 $r > 1$。从 *(4)* 式可以看出，求和中负项的绝对值小于 *1*，因此不会影响最终结果。因此，对于 $f(x)$ 的任何分解，其整数分割为：

$$1 = 0 + 1. \tag{5}$$

接下来，我们引入精确的数学表述，定义 $\cos\varphi$ 由 *(3)* 给出。由 *(3)* 式可以得出：

$$2\frac{r^2-1}{r}\cos\varphi = 2\frac{r^n - r^{2-n} - r}{r} = \frac{r^{2n} - r^2 - 1}{r^2}.$$

由于 $r^{2n-3}(r^2-1) \geq r^2 - 1$，即使 $r = 1$ 时取等号，这意味着对于可能的因子 $x^2 + x + 1$，我们有：

$$\frac{1}{r^2} \geq 1.$$

如果我们记得 *(5.3)* 中的求和是按照共轭虚根成对进行的，我们得到以下不等式：

$$S = \sum \left(x_j - \frac{1}{x_j} \right) \geq \sum \left(1 - \frac{1}{r^2} \right). \tag{5.5}$$

这里，求和现在包括所有实根和复根。

另一方面，这些根的模的乘积必须为 *1*，即：

$$\prod r = 1, \quad \text{或} \quad \prod \frac{1}{r^2} = 1.$$

所有 r^{-2} 的几何平均值因此等于 *1*。由于它始终小于等于算术平均值（只有当 $r = 1$ 时取等号），所以我们得出：

$$S \geq 0.$$

只有当因子为 $x^2 + x + 1$ 时才能取等号。这就完成了证明。

习题二.

Problem 3. 已知多项式

$$f(x) = \sum_{i=0}^{n-1} a_i x^i,$$

定义循环矩阵 C 为：

$$C = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}.$$

求矩阵 C 的行列式 $\det(C)$。

Solution. 由多项式 $f(x) = a_1 + a_2x + a_3x^2 + \cdots + a_nx^{n-1}$，构造矩阵 V：

$$V = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \xi_1 & \xi_2 & \xi_3 & \cdots & \xi_n \\ \xi_1^2 & \xi_2^2 & \xi_3^2 & \cdots & \xi_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_1^{n-1} & \xi_2^{n-1} & \xi_3^{n-1} & \cdots & \xi_n^{n-1} \end{pmatrix}.$$

$$AV = \begin{pmatrix} f(\xi_1) & f(\xi_2) & f(\xi_3) & \cdots & f(\xi_n) \\ \xi_1 f(\xi_1) & \xi_2 f(\xi_2) & \xi_3 f(\xi_3) & \cdots & \xi_n f(\xi_n) \\ \xi_1^2 f(\xi_1) & \xi_2^2 f(\xi_2) & \xi_3^2 f(\xi_3) & \cdots & \xi_n^2 f(\xi_n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi_1^{n-1} f(\xi_1) & \xi_2^{n-1} f(\xi_2) & \xi_3^{n-1} f(\xi_3) & \cdots & \xi_n^{n-1} f(\xi_n) \end{pmatrix}.$$

因此，

$$|AV| = f(\xi_1)f(\xi_2)\cdots f(\xi_n) \cdot |V|.$$

由于 ξ_i 是不同的 n 次方根，V 是范德蒙德矩阵，且 $|V| \neq 0$。因此，

$$|A| = f(\xi_1)f(\xi_2)\cdots f(\xi_n).$$

我们得到了矩阵 A 的行列式为：

$$|A| = f(\xi_1)f(\xi_2)\cdots f(\xi_n).$$

习题三.

Problem 4. 设 $f(x) = x^{2021} + a_{2020}x^{2020} + a_{2019}x^{2019} + \cdots + a_2x^2 + a_1x + a_0$ 为整数系数多项式，且 $a_0 \neq 0$。假设对于任意 $0 \leq k \leq 2020$，有 $|a_k| \leq 40$。证明：方程 $f(x) = 0$ 的根不可能全部为实数。

Solution. 假设 $f(x)=0$ 的 2021 个根分别为 $x_1,x_2,\ldots,x_{2021}$。由于 $a_0\neq 0$，所以 $x_i\neq 0$，其中 $1\leq i\leq 2021$。若这些根全为实数，由 *Cauchy* 不等式可得：

$$\left(\sum_{i=1}^{2021} x_i\right)^2\cdot\left(\sum_{i=1}^{2021}\frac{1}{x_i}\right)^2\leq 2021^2.$$

根据 *Vieta* 定理，有：

$$\sum_{i=1}^{2021} x_i=-a_{2020},\qquad \sum_{1\leq i<j\leq 2021} x_ix_j=a_{2019}.$$

由此我们得到：

$$\sum_{i=1}^{2021} x_i^2=\left(\sum_{i=1}^{2021} x_i\right)^2-2\sum_{1\leq i<j\leq 2021} x_ix_j=a_{2020}^2-2a_{2019}.$$

我们再考虑多项式 $g(x)=x^{2021}f\left(\frac{1}{x}\right)$，得到其根为 $\frac{1}{x_1},\frac{1}{x_2},\ldots,\frac{1}{x_{2021}}$。继续利用 *Vieta* 定理：

$$\sum_{i=1}^{2021}\frac{1}{x_i}=-\frac{a_1}{a_0},\qquad \sum_{1\leq i<j\leq 2021}\frac{1}{x_ix_j}=\frac{a_2}{a_0}.$$

因此我们有：

$$\left(\sum_{i=1}^{2021}\frac{1}{x_i}\right)^2=\frac{a_1^2}{a_0^2}-\frac{2a_2}{a_0}$$

最终推导得：

$$\left(\sum_{i=1}^{2021} x_i\right)^2\cdot\left(\sum_{i=1}^{2021}\frac{1}{x_i}\right)^2\leq\left(40^2+2\cdot 40\right)\left(40^2+2\cdot 40\right)=1680^2.$$

矛盾，证毕。

总结

通过本次报告，希望大家掌握了一些代数竞赛中的解题思路。后续可以根据这些基础继续深入学习其他数学模块。