



分圆多项式与分圆域

作者: Jiahai Wang

时间: September 8, 2024

目录

第 1 章	分圆多项式	1
1.1	基本性质	1
1.2	系数的探究	2
第 2 章	分圆域 $\mathbb{Q}(\zeta_m)$	4
2.1	分圆域 $\mathbb{Q}(\zeta_m)$ 的 Galois 群	4
2.2	素数 p 在 $\mathbb{Z}[\zeta_m]$ 中的分解	5
2.3	素数分圆域的代数整数环	6

第1章 分圆多项式

1.1 基本性质

我们都知道, $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ 是个 n 次单位根, 它可以生成 $x^n - 1 = 0$ 的全部复根: $\varepsilon, \varepsilon^2, \dots, \varepsilon^n$ 。换句话说, 对于 $k = 1, 2, \dots, n-1$ 都有 $\varepsilon^k \neq 1$ 。

对于 n 次单位根 ω , 定义它的阶 $\text{ord}(\omega)$ 为满足 $\omega^k = 1$ 的最小正整数 k , 那么有 $\text{ord}(\varepsilon) = n$, 且对任意的 n 次单位根, 它的阶必然能整除 n 。

我们称阶为 n 的 n 次单位根为 n 次本原单位根。 n 次本原单位根当然 (一般) 不止 ε 一个。事实上, 若 d 是与 n 互素的正整数, 则

$$\varepsilon^{dk} = 1 \Leftrightarrow n \mid dk \Leftrightarrow n \mid k$$

从而 $\text{ord}(\varepsilon^d) = n$, ε^d 为一个 n 次本原单位根。

于是我们立刻得到: n 次本原单位根有 $\varphi(n)$ 个。

定义 1.1

给定正整数 n , 我们定义 n 级分圆多项式 $\Phi_n(x)$ 为

$$\Phi_n(x) = (x - \varepsilon_1)(x - \varepsilon_2) \cdots (x - \varepsilon_{\varphi(n)})$$

其中 $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{\varphi(n)}$ 是全部 n 次本原单位根。则 $\Phi_n(x)$ 是一个 $\varphi(n)$ 次多项式。

定理 1.1

对任意正整数 n , 有 $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$ 。

证明 令 $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, 则

$$x^n - 1 = (x - \varepsilon)(x - \varepsilon^2) \cdots (x - \varepsilon^n)$$

一方面, 对 $k = 1, 2, \dots, n$, ε^k 是 $\text{ord}(\varepsilon^k)$ 次本原单位根且 $\text{ord}(\varepsilon^k) \mid n$, 从而 $x - \varepsilon^k$ 是右边某一项的因式, 于是我们得到了 $x^n - 1 \mid \prod_{d \mid n} \Phi_d(x)$ 。

另一方面, 若 ω 既为 a 次本原单位根, 又为 b 次本原单位根, 则 $\omega^a = 1, \omega^b = 1$, 进而由本原单位根定义有 $a \geq b, b \geq a$, 则 $a = b$ 。那么 $a \neq b$ 时, $(\Phi_a(x), \Phi_b(x)) = 1$ 。对 n 的任意因子 d , $\Phi_d(x) \mid x^n - 1$, 故 $\prod_{d \mid n} \Phi_d(x) \mid x^n - 1$ 。

又这两个多项式都是首一的, 从而我们证明了 $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$ 。

推论 1.1

$$n = \sum_{d \mid n} \varphi(d)$$

根据莫比乌斯反演公式, 还可以得到:

定义 1.2

$$\Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(\frac{n}{d})}$$

注: 下一节会给出具体的证明

定理 1.2

对任意正整数 n , $\Phi_n(x) \in \mathbb{Z}[x]$.



证明 $n=1$ 时, $\Phi_1(x) = x-1 \in \mathbb{Z}[x]$.

假设命题对一切小于 n 的正整数成立, 则对于 n 阶分圆多项式:

由 $x^n - 1 = \Phi_n(x) \prod_{d|n, d < n} \Phi_d(x)$, 由归纳假设和高斯引理知 $\prod_{d|n, d < n} \Phi_d(x)$ 为本原多项式, 进而 $\Phi_n(x) \in \mathbb{Z}[x]$.

定理 1.3

对任意正整数 n , $\Phi_n(x)$ 是 $\mathbb{Z}[x]$ 中的不可约多项式.



证明 设 $\Phi_n(x) = P(x)Q(x)$, 其中 $P(x), Q(x)$ 为首一整系数多项式, 且 $P(x)$ 非常数且在 \mathbb{Z} 上不可约.

当 n 为素数时, 这个结论是相当经典的, 可以变形后使用爱森斯坦判别法. 对于一般情况, 我们证明的思路是说明 $\Phi_n(x)$ 的每个根都是 $P(x)$ 的根, 从而得到结论.

取 $P(x)$ 的一个根 z 和与 n 互素的素数 p , 则 z^p 是 $P(x)$ 或者 $Q(x)$ 的根.

假设 z^p 是 $Q(x)$ 的根, 则 z 是 $P(x)$ 和 $Q(x^p)$ 的公共根, 则 $P(x) \mid Q(x^p)$.

设 $Q(x^p) = P(x)R(x)$, 则 $P(x)R(x) \equiv Q(x^p) \equiv Q(x)^p \pmod{p}$.

再设 $x^n - 1 = \Phi_n(x)S(x)$, 则 $(x^n - 1) \equiv P(x)Q(x)S(x) \pmod{p}$, 这说明 $x^n - 1 \equiv 0 \pmod{p}$ 有重根, 这与 $(p, n) = 1$ 矛盾, 于是 z^p 是 $P(x)$ 的根.

我们知道: 对任意与 n 互素的正整数 s , z^s 是 $P(x)$ 的根. 从而 $\Phi_n(x)$ 的根都是 $P(x)$ 的根, 于是 $\Phi_n(x) = P(x)$ 为 $\mathbb{Z}[x]$ 中的不可约多项式.

定理 1.4

若 p 为素数, 且 $(p, n) = 1$, 则 $\Phi_n(x^p) = \Phi_n(x)\Phi_{pn}(x)$.



证明 对照一下即可

定理 1.5

$kn+1$ 型素数有无穷多



证明 这是一个经典的结论可以看《伽罗瓦理论: 天才的激情》/章璞著: -北京: 高等教育出版社

注: 这个是 Dirichlet 定理的特殊情况

1.2 系数的探究

Möbius 函数

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1, \\ 0 & n > 1, \end{cases}$$

可将 $\Phi_n(x)$ 化为

$$\begin{aligned} \Phi_n(x) &= \prod_{1 \leq k \leq n} (x - e^{2\pi i k/n})^{\sum_{d|(k,n)} \mu(d)} = \prod_{1 \leq k \leq n} \prod_{d|(k,n)} (x - e^{2\pi i k/n})^{\mu(d)} \\ &= \prod_{d|n} \prod_{\substack{1 \leq k \leq n \\ d|k}} (x - e^{2\pi i k/n})^{\mu(d)} = \prod_{d|n} \left[\prod_{1 \leq r \leq n/d} (x - e^{2\pi i r/(n/d)}) \right]^{\mu(d)}. \end{aligned}$$

注意到当 $r = 1, 2, \dots, n/d$ 时, $e^{2\pi ir/(n/d)}$ 遍历全体 n/d 次单位根, 得

$$\Phi_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}.$$

定理 1.6

若 $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ 、 $m = p_1 p_2 \cdots p_s$, 则有

$$\Phi_n(x) = \prod_{d|m} (x^{\frac{n}{m} \cdot \frac{m}{d}} - 1)^{\mu(d)} = \Phi_m(x^{n/m})$$



简化为 n 为奇无平方因子数的情况。

若 n 为偶无平方因子数, 设 $m = n/2$, 则可将 $d | n$ 分为两种不重叠的情况: 1. d 为偶数, 故 $d = 2\delta$, 其中 $\delta | m$. 2. d 为奇数, 故 $d | m$.

因此变为:

$$\begin{aligned} \Phi_{2m}(x) &= \prod_{\delta|m} (x^{m/\delta} - 1)^{\mu(2\delta)} \prod_{d|m} (x^{2m/d} - 1)^{\mu(d)} \\ &= \prod_{\delta|m} (x^{m/\delta} - 1)^{-\mu(\delta)} \prod_{d|m} (x^{2m/d} - 1)^{\mu(d)} \\ &= \prod_{\delta|m} \left(\frac{x^{2m/\delta} - 1}{x^{m/\delta} - 1} \right)^{\mu(\delta)} = \prod_{\delta|m} (x^{m/\delta} + 1)^{\mu(\delta)}. \end{aligned}$$

结合 $x^{m/d} + 1 = (-1) [(-x)^{m/d} - 1]$ 有:

定理 1.7

若 $m > 1$ 为奇数, 则

$$\Phi_{2m}(x) = \Phi_m(-x)$$



将 $n = pq$ 代入, 得:

$$x^{pq} - 1 = (x - 1) \cdot \frac{x^p - 1}{x - 1} \cdot \frac{x^q - 1}{x - 1} \cdot \Phi_{pq}(x),$$

有

$$\Phi_{pq}(x) = \frac{(x - 1)(x^{pq} - 1)}{(x^p - 1)(x^q - 1)}.$$

对两侧同乘 $x^{pq} - 1$, 遂有公式

$$(x^{pq} - 1)\Phi_{pq}(x) = \Phi_p(x^q)\Phi_q(x^p)(x - 1)$$

因为 $\deg \Phi_{pq} = (p - 1)(q - 1) < pq$, 所以 $x^{pq}\Phi_{pq}(x)$ 和 $-\Phi_{pq}(x)$ 展开式中的项不会合并。故将右侧次数不超过 $(p - 1)(q - 1)$ 的项整理出来便得 $-\Phi_{pq}(x)$ 的展开式, 于是 $\Phi_{pq}(x)$ 只包含 $\pm x^k$ 形式的项。

我们就证出了本文的主要结论:

定理 1.8 (Migotti 1883)

若 n 至多只能被两个不同的奇素数整除, 则 $\Phi_n(x)$ 的展开式中只含有形如 $\pm x^k$ 的项。



事实上 $105 = 3 \times 5 \times 7$ 就是第一个系数不为 ± 1 的例子:

$$\begin{aligned} \Phi_{105}(x) &= x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} \\ &\quad + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} \\ &\quad - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} \\ &\quad + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1. \end{aligned}$$

第2章 分圆域 $\mathbb{Q}(\zeta_m)$

考虑方程 $x^m - 1 = 0$ 的根 $\zeta_m = e^{\frac{2\pi i}{m}}$, 则我们有

$$(x-1)(x-\zeta_m)\cdots(x-\zeta_m^{m-1}) = x^m - 1 \quad (2.1)$$

于是数域 $F = \mathbb{Q}(\zeta_m)$ 是多项式 $x^m - 1$ 的分裂域。接下来我们就来研究一下 m 次分圆域 $F = \mathbb{Q}(\zeta_m)$ 的性质。

2.1 分圆域 $\mathbb{Q}(\zeta_m)$ 的 Galois 群

定理 2.1

设 G 为 F/\mathbb{Q} 的 Galois 群, 则存在从 G 到 $U(\mathbb{Z}/m\mathbb{Z})$ 的单同态 θ 满足对于 $\sigma \in G$ 有 $\sigma(\zeta_m) = \zeta_m^{\theta(\sigma)}$ 。

证明 由于 $\zeta_m^m = 1$, 我们知道 $\sigma(\zeta_m)^m = 1$, 于是 $\sigma(\zeta_m) = \zeta_m^{\theta(\sigma)}$ 其中 $\theta(\sigma) \in \mathbb{Z}/m\mathbb{Z}$ 。若 $\tau = \sigma^{-1}$, 则 $\zeta_m = \tau\sigma(\zeta_m) = \tau(\zeta_m^{\theta(\sigma)}) = \zeta_m^{\theta(\sigma)\theta(\tau)}$ 。因此 $\theta(\sigma)\theta(\tau) = \bar{1}$ 。于是这一映射是良定义的。

容易印证 θ 是一个群同态。当 $\theta(\sigma) = \bar{1}$ 时, $\sigma(\zeta_m) = \zeta_m$, 于是 σ 为 G 中的单位元, 因此 θ 是一个单同态。

根据这一性质我们可以得到推论: $[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ 整除 $\phi(m)$ 。事实上, 接下来我们想要证明更强的结论: $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ 。

我们先给出 m 次分圆多项式 $\Phi_m(x)$ 的定义:

$$\Phi_m(x) = \prod_{(a,m)=1} (x - \zeta_m^a) \quad (2.2)$$

定理 2.2

$$x^m - 1 = \prod_{d|m} \Phi_d(x).$$

证明 $x^m - 1 = \prod_{l=0}^{m-1} (x - \zeta_m^l) = \prod_{d|m} \prod_{(i,m)=d} (x - \zeta_m^i)$ 。当 $(i,m) = d$ 时, 设 $i = dj$, 则

$$\begin{aligned} \prod_{(i,m)=d} (x - \zeta_m^i) &= \prod_{(j,m/d)=1} (x - \zeta_m^{dj}) \\ &= \prod_{(j,m/d)=1} (x - \zeta_{m/d}^j) \\ &= \Phi_{m/d}(x) \end{aligned}$$

于是 $\Phi_m(x) = \prod_{(a,m)=1} (x - \zeta_m^a)$ 。

下面我们来研究 $\Phi_m(x)$ 的性质。

引理 2.1

设 p 是一个素数且 $p \nmid m$, 且 P 是 \mathcal{O}_K 中包含 p 的一个素理想, 则 $1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}$ 在 \mathcal{O}_K/P 中互不相同, 且若 P 的剩余类域指数为 f 则 $p^f \equiv 1 \pmod{m}$ 。

定理 2.3

$\Phi_m(x)$ 在 $\mathbb{Z}[x]$ 中是不可约的。

证明 设 $f(x) \in \mathbb{Z}[x]$ 为 ζ_m 的最小多项式, 我们先证明若素数 $p \nmid m$, 则 ζ_m^p 也是 $f(x)$ 的零点。记 P 是一个包含 p 的素理想。

由于 $x^m - 1$ 是 $f(x)$ 的倍式, 因此可以设 $x^m - 1 = f(x)g(x)$ 。 $w \in \mathcal{O}_K$ 则用 \bar{w} 表示 w 在 $\mathcal{O}_K \rightarrow \mathcal{O}_K/P$ 的自然同态的像。因此 $x^m - \bar{1} = \bar{f}(x)\bar{g}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$, 由于引理 1.3 知 $x^m - \bar{1}$ 在 \mathcal{O}_K/P 中有着互异的根, 因此 $\bar{f}(x), \bar{g}(x)$ 有着互异的零点, 由于 ζ_m^p 是 $x^m - \bar{1}$ 的根, 因此若 $\bar{f}(\zeta_m^p) \neq 0$, 则 $\bar{g}(\zeta_m^p) = 0$ 进而 $\bar{g}(\bar{\zeta}_m^p) = \bar{g}^p(\bar{\zeta}_m) = 0$ 。因此 $\bar{g}(\bar{\zeta}_m) = \bar{0} \Rightarrow \bar{f}(\bar{\zeta}_m) \neq 0$, 这与 $f(\zeta_m) = 0$ 矛盾。

进而我们可以推出, 若 $(a, m) = 1$, 则 ζ_m^a 是 $f(x)$ 的根, 这就表明 $\deg f(x) \geq \phi(m) = \deg \Phi_m(x)$ 。而另一方面, $\Phi_m(\zeta_m) = 0$, 于是 $f(x) | \Phi_m(x)$, 因此有 $f(x) = \Phi_m(x)$ 。这样就证明了 $\Phi_m(x)$ 是不可约的。

从这一定理我们也可以推出 $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ 以及 $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq U(\mathbb{Z}/m\mathbb{Z})$ 。

2.2 素数 p 在 $\mathbb{Z}[\zeta_m]$ 中的分解

我们本小节的主要结论是: 假设 $p \nmid m$, 则 (p) 在 \mathcal{O}_K 中是不分歧的。

在研究此问题前, 我们需要一些引理。

引理 2.2

设 K/\mathbb{Q} 是一个代数数域且 $[K : \mathbb{Q}] = n$, 设 $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathcal{O}_K$ 是 K 的一组 \mathbb{Q} 基。记 $d = \Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$, 则

$$d\mathcal{O}_K \subset \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \dots + \mathbb{Z}\alpha_n.$$

证明: 对于任一 $w \in \mathcal{O}_K$, 存在有理数 $r_1, r_2, \dots, r_n \in \mathbb{Q}$ 使得

$$w = \sum_{i=1}^n r_i \alpha_i.$$

两边乘以 α_j 并取迹得

$$\text{tr}(w\alpha_j) = \sum_{i=1}^n r_i \text{tr}(\alpha_i \alpha_j) \quad (j = 0, 1, \dots, n).$$

这构成了一个关于 r_1, r_2, \dots, r_n 的 n 元线性方程组。注意到 $\text{tr}(w\alpha_j), \text{tr}(\alpha_i \alpha_j) \in \mathbb{Z}$ 。根据 Cramer 法则知, 每个 r_i 可以写成一个整数除以 d 的形式 (因为方程组的系数矩阵等于 d)。于是 $dw \in \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \dots + \mathbb{Z}\alpha_n$ 。进而我们就得到了 $d\mathcal{O}_K \subset \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \dots + \mathbb{Z}\alpha_n$ 。



引理 2.3

判别式 $\Delta(1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{\phi(m)-1})$ 整除 $m^{\phi(m)}$ 。



通过这两个引理, 我们可以推出当 $p \nmid m$ 时, 代数整数环 \mathcal{O}_K 中的任一元素都可以在模 p 意义下与 $\mathbb{Z}[\zeta_m]$ 中的一个元素等价。

推论 2.1

设 $p \in \mathbb{Z}$ 为素数且 $p \nmid m$, 则对于任意的 $w \in \mathcal{O}_K$, 存在 $\sum a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$ 使得 $w \equiv \sum a_i \zeta_m^i \pmod{p}$ 。



推论 2.2

若 $p \nmid m$, 且 n 满足 $p^n \equiv 1 \pmod{m}$, 则对于任意 $w \in \mathcal{O}_K$ 满足 $w^{p^n} \equiv w \pmod{p}$ 。



证明 根据推论 2.3 知存在 $\sum a_i \zeta_m^i$ 使得 $w \equiv \sum a_i \zeta_m^i \pmod{p}$, 于是

$$w^p \equiv \sum a_i^p \zeta_m^{pi} \equiv \sum a_i \zeta_m^{pi} \pmod{p}.$$

重复 n 次得 $w^{p^n} \equiv w \pmod{p}$ 。

性质 若 p 是素数且 $p \nmid m$, 则 (p) 在 \mathcal{O}_K 中是不分歧的。

证明 假设 (p) 是分歧的, 则存在素理想 P 使得 $P^2 \subset (p)$ 。于是我们可以取 $w \in P$ 但 $w \notin P^2$ 。于是 $w^{p^n} \equiv w$

$(\text{mod } P)$ 。由于 $p^n \geq 2$ ，我们可以知道 $w \in P^2$ ，这与假设矛盾。因此 (p) 是不分歧的。

性质 对于任意 $w \in \mathcal{O}_K$ ，有 $\sigma_p(w) \equiv w^p \pmod{p}$ 。

证明 根据推论得存在 a_i 使得 $w \equiv \sum a_i \zeta_m^i \pmod{p}$ ，于是

$$\sigma_p(w) \equiv \sum a_i \zeta_m^{ip} \equiv \sum a_i^p \zeta_m^{ip} \pmod{p}.$$

同时

$$w^p \equiv \left(\sum a_i \zeta_m^i \right)^p \equiv \sum a_i^p \zeta_m^{ip} \pmod{p}.$$

于是我们就证明了这个性质。

推论 2.3

设 P 是 \mathcal{O}_K 中包含 p 的素理想，则 $\sigma_p P = P$ 。

证明 由于对于 $\forall w \in P$ ， $\sigma_p w \equiv w^p \equiv 0 \pmod{P}$ ，于是 $\sigma_p P \subset P$ 。又因为 $\sigma_p P$ 为极大理想，于是有 $\sigma_p P = P$ 。

定理 2.4

假设 p 是一个素数且 $p \nmid m$ ，且 f 是满足 $p^f \equiv 1 \pmod{m}$ 的最小的正整数 f ，则在 \mathcal{O}_K 中有

$$(p) = P_1 P_2 \cdots P_g,$$

其中各个素理想 P_i 的剩余类域指数 $|\mathcal{O}_K/P_i| = f$ 且 $g = \phi(m)/f$ 。

证明 由推论得 $\sigma_p \in G(P)$ ，于是 $\langle \sigma_p \rangle \subset G(P)$ 。设 g 为 (p) 的分裂次数，则考虑 G 在 $\{P_1, P_2, \dots, P_g\}$ 上的群作用，得到

$$|G(P)| = \frac{|G|}{g} = \frac{\phi(m)}{g} = f$$

由于 f 是满足 $p^f \equiv 1 \pmod{p}$ 的最小的正整数，因此

$$|\langle \sigma_p \rangle| = f = |G(P)|$$

即 $G(P) = \langle \sigma_p \rangle$

2.3 素数分圆域的代数整数环

我们想证明，当 l 为素数时， $K = \mathbb{Q}(\zeta_l)$ 的代数整数环 $\mathcal{O}_K = \mathbb{Z}[\zeta_l]$ 。

性质 设 l 为素数，则 (l) 在 $\mathbb{Q}(\zeta_l)$ 中完全分歧，且记 $L = (1 - \zeta_l)$ ，则 $(l) = L^{l-1}$ 。

证明 注意到 $l = \prod_{i=1}^{l-1} (1 - \zeta_l^i)$ 。设 $u_i = \frac{1 - \zeta_l^i}{1 - \zeta_l}$ ，我们试图证明它是代数整数环 \mathcal{O}_K 的单位元。事实上，由于 $l \nmid i$ ，我们能够找到 j 使得 $ij \equiv 1 \pmod{l}$ ，因此

$$u_i^{-1} = \frac{1 - \zeta_l}{1 - \zeta_l^i} = \frac{1 - \zeta_l^{ij}}{1 - \zeta_l^i} = 1 + \zeta_l^j + \cdots + \zeta_l^{j(i-1)} \in \mathcal{O}_K$$

于是 u_i 是单位元。

因此

$$l = \prod_{i=1}^{l-1} (1 - \zeta_l^i) = (1 - \zeta_l)^{l-1} \prod_{i=1}^{l-1} u_i$$

于是 $(l) = L^{l-1}$ 。同时，我们设 L 的剩余类域指数为 f ，则由于分歧指数 $e = l - 1$ ，因此根据 $efg = \phi(l) = l - 1$ ，得 $f = g = 1$ 。于是 $|\mathcal{O}_K/L| = l$ 。

性质 若 l 是素数，则代数整数环 $\mathcal{O}_K = \mathbb{Z}[\zeta_l]$ 。

证明 显然 $\mathbb{Z}[\zeta_l] \subset \mathcal{O}_K$ 。又因为 $1, \zeta_l, \zeta_l^2, \dots, \zeta_l^{l-2}$ 为 K 的一组 \mathbb{Q} 基，则对于任意 $\alpha \in \mathcal{O}_K$ ，存在一列有理数

$\{a_i\}(1 \leq i \leq l-2)$ 使得

$$\alpha = a_0 + a_1\zeta_l + \cdots + a_{l-2}\zeta_l^{l-2}$$

考虑 ζ_l^i 的迹, 容易计算 $\text{tr}(\zeta_l^i) = -1$ ($l \nmid i$), 而 $\text{tr}(1) = l-1$ 。于是

$$\text{tr}(\alpha\zeta_l^{-s}) = -a_0 - a_1 - \cdots - a_{s-1} + (l-1)a_s - a_{s+1} - \cdots - a_{l-2}$$

于是 $\text{tr}(\alpha\zeta_l^{-s} - \alpha\zeta_l) = la_s$ 。由于 $\text{tr}(\alpha\zeta_l^{-s} - \alpha\zeta_l) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, 于是 $la_s \in \mathbb{Z}$ 。

于是存在 $\{b_i\}(0 \leq i \leq l-2) \in \mathbb{Z}$, 满足

$$l\alpha = la_0 + la_1\zeta_l + \cdots + la_{l-2}\zeta_l^{l-2} = b_0 + b_1\lambda + \cdots + b_{l-2}\lambda^{l-2} \quad (*)$$

由于性质 3.1 得 $(l) = (\lambda)^{l-1}$, 于是 $\lambda \mid b_0$, 两边取范数得

$$N(\lambda) = \prod_{i=1}^{l-1} (1 - \sigma_i(\zeta_l)) = \prod_{i=1}^{l-1} (1 - \zeta_l^i) = l, \quad N(b_0) = b_0^{l-1}$$

于是 $l \mid b_0^{l-1} \Rightarrow l \mid b_0 \Rightarrow \lambda^{l-1} \mid b_0$ 。

再对 (*) 式两边模 λ^{l-2} 得 $\lambda^2 \mid b_1\lambda \Rightarrow \lambda \mid b_1 \Rightarrow l \mid b_1$ 。

重复这个过程得知 $l \mid b_i (0 \leq i \leq l-2)$ 。记 $b_i = lb'_i (b'_i \in \mathbb{Z})$, 则

$$\alpha = b'_0 + b'_1\lambda + \cdots + b'_{l-2}\lambda^{l-2}$$

这就推出了 $\alpha \in \mathbb{Z}[\zeta_l]$ 。于是 $\mathbb{Z}[\zeta_l] = \mathcal{O}_K$ 。