分圆多项式与分圆域

Jiahai Wang

September 2024

目录

Chapter 1

分圆多项式

Chapter 2

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

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

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

Theorem 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：

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

Theorem 2.2. $x^m-1=\prod\limits_{d|m}\Phi_d(x)$。

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

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

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。

Lemma 2.3. 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 $1,\zeta_m,\zeta_m^2,\cdots,\zeta_m^{m-1}$ 在 $\mathcal{O}_K/P$ 中互不相同，且若 P 的剩余类域指数为 f 则 $p^f\equiv 1 \pmod m$。

Theorem 2.4. $\Phi_m(x)$ 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 $\mathcal{O}_K\to\mathcal{O}_K/P$ 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 $g(\zeta_m^p)=0$ 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 $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\simeq U(\mathbb{Z}/m\mathbb{Z})$。 □

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。

Lemma 2.5. 设 $K/\mathbb{Q}$ 是一个代数数域且 $[K:\mathbb{Q}]=n$，设 $\alpha_1,\alpha_2,\cdots,\alpha_n\in\mathcal{O}_K$ 是 K 的一组 $\mathbb{Q}$ 基。记 $d=\Delta(\alpha_1,\alpha_2,\cdots,\alpha_n)$，则

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

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

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

两边乘以 α_j 并取迹得

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

这构成了一个关于 $r_1, r_2, \cdots, r_n$ 的 n 元线性方程组。注意到 $\mathrm{tr}(w\alpha_j), \mathrm{tr}(\alpha_i\alpha_j) \in \mathbb{Z}$。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 $dw \in \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$。进而我们就得到了 $d\mathcal{O}_K \subset \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$。

Lemma 2.6. 判别式 $\Delta(1, \zeta_m, \zeta_m^2, \cdots, \zeta_m^{\phi(m)-1})$ 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。

Corollary 2.7. 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 $w \equiv \sum a_i \zeta_m^i \pmod{p}$。

Corollary 2.8. 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 $w^{p^n} \equiv w \pmod{p}$。 □

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 $w^{p^n} \equiv w \pmod{P}$。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。 □

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。 □

Corollary 2.9. 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 $\sigma_p P = P$。 □

Theorem 2.10. 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 $\{P_1, P_2, \cdots, P_g\}$ 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

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

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 $|\mathcal{O}_K/L| = l$。

□

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 $1, \zeta_l, \zeta_l^2, \cdots, \zeta_l^{l-2}$ 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 $\{a_i\}(1 \le i \le l-2)$ 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 $\mathrm{tr}(\zeta_l^i) = -1\,(l \nmid i)$，而 $\mathrm{tr}(1) = l-1$。于是

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

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

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

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

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 $l \mid b_i(0 \le i \le l-2)$。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 $\mathbb{Z}[\zeta_l] = \mathcal{O}_K$。