数论基础

Lectured by Prof. Zhao Lilu

Adaus

2022 年 5 月 21 日

前言

预备知识: 初等数论, 高等代数 (线性代数和多项式), 数学分析, 复变函数, 近世代数.

参考文献: 代数数论入门 by 冯克勤

课程内容包括解析数论和代数数论,如果课时允许,会补充组合数论的内容.由于各种各样的原因,这份笔记与教学的内容和顺序并不完全重合,笔记中可能出现的所有的笔误和数学错误完全是我个人的原因,若您发现任何问题请与我联系.

Adaus

目录

Ι	解相	近	1		
1	素数分布(初等证明)				
	1.1	基本定理	1		
	1.2	一些数论函数及其性质	4		
2	Riemann zeta 函数与素数定理				
	2.1	Riemann zeta 函数的基本性质	8		
	2.2	素数定理	13		
3	算术级数中的素数分布 I				
	3.1	有限 Abel 群的特征	16		
	3.2	Dirichlet L 函数及其性质	19		
	3.3	Dirichlet 定理的证明	28		
4	算术级数中的素数分布 II				
	4.1	算术级数中的素数定理	30		
II	代	数理论	32		
5	代数数域和代数整数环				
	5.1	代数数域	32		
	5.2	范, 迹和判别式	34		
	5.3	代数整数环	38		
	5.4	单位根	46		
6	素班	型想分解	49		

	6.1	Dedekind 整环	49	
II	I		57	
附录				
\mathbf{A}	代数	学	57	
	A.1	分圆多项式	57	
	A.2	有限生成自由 Abel 群	59	
В	分析	学	6 0	
	B.1	解析延拓	60	
	B.2	Poisson 求和公式	60	
\mathbf{C}	"初等"方法			
	C.1	Dirichlet 除数问题	62	
	C.2	Chebyshev 估计	63	
D	π是	无理数	66	

Part I

解析理论

1 素数分布(初等证明)

本章旨在回顾一些初等的内容, 并同接下来的解析方法做一个对比. 为有助于回顾复习, 要用到的一些初等数论的结果会以引理的形式给出.

1.1 基本定理

定理 1.1. 有无穷多个素数.

下面我们看 Euler 怎么证明定理1.1.

证明. 考虑算术基本定理, 当 s > 1 时,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \tag{1}$$

$$= \prod_{p} (1 - \frac{1}{p^s})^{-1} \tag{2}$$

而

$$\lim_{s \to 1^+} \sum_{n=1}^{\infty} \frac{1}{n^s} = \infty$$

于是 (1.2) 等号右边是一个无穷乘积, 即素数有无穷多个.

定义 1.2. 我们称

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (s \in \mathbb{C}, Re(s) > 1)$$

为 Riemann zeta 函数.

注. 设 a(n) 是积性的数论函数, 且对于固定的 $\epsilon_0 \geq 0$, $|a(n)| \leq n^{\epsilon_0}$, 则当 $s > 1 + \epsilon_0$ 时,

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{n} \left(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots\right)$$
 (3)

等号右边的式子一般称为 Euler 乘积.

我们再给一个拓扑的证明 (Hillel Furstenberg, 2020 年 Abel 奖得主).

证明. 对 $a \in \mathbb{Z}, b \in \mathbb{Z}^+$, 引入记号

$$a(\text{mod } b) := \{ n \in \mathbb{Z} | n \equiv a(\text{mod } b) \}$$

我们引入一个 \mathbb{Z} 上的拓扑 (\mathbb{Z},τ) 如下. 对于任意子集 $A\subset \mathbb{Z}, A\in \tau$ 当且仅当要么 $A=\varnothing$,要么 $\forall a\in A, \exists b\in \mathbb{Z}^+, \text{ s.t. } a \pmod{b}\subset A.$

验证这是一个拓扑是容易的.

根据定义, $\emptyset \in \tau$, $\mathbb{Z} = 0 \pmod{1} \in \tau$.

如果 $\{A_{\lambda}\}\in \tau(\lambda\in\Lambda)$, 则只需考虑它们不全是空集的情况,根据定义, $\forall a\in \bigcup_{\lambda}A_{\lambda}, \exists b\in\mathbb{Z}^{+}, \text{ s.t. } a \pmod{b}\subset\bigcup_{\lambda}A_{\lambda}.$

如果 $A_1, A_2 \in \tau$ 非空, 则 $\forall a \in A_1 \cap A_2, \exists b \in \mathbb{Z}^+$, s.t. $a \pmod{b} \subset A_1 \cap A_2$. 易见 $a \in \mathbb{Z}, b \in \mathbb{Z}^+$, $a \pmod{b} \in \tau$.

对任意 $n \neq \pm 1 (n \in \mathbb{Z})$, 都存在素数 p, s.t. p|n, i.e. $n \in 0 \pmod{p}$, 并且对于 ± 1 , 不存在这样的素数.

因此

$$\mathbb{Z}\setminus\{1,-1\}=\bigcup_p 0 (\bmod\ p)$$

而

$$\{1,-1\} = \bigcap_p (\mathbb{Z} \setminus 0 \pmod{p}) \notin \tau$$

故

$$\bigcap_{p} (\mathbb{Z} \setminus 0 \pmod{p}) = \bigcap_{p} (1 \pmod{p} \cup \dots \cup (p-1) \pmod{p})$$

等式右边不是有限交

思考. 4k+1 型素数是否有无穷多个.

4k-1 型素数是否有无穷多个.

定理 1.3. 设 q 是固定的正整数,则有无穷多个形如 qk+1 形素数 $(k \in \mathbb{Z}^+)$

证明. 考虑分圆多项式

$$\Phi_n(x) = \prod_{\substack{k=1\\(k,n)=1}}^{n} (x - e^{2\pi i \frac{k}{n}}) \in \mathbb{Z}[x]$$

它与 $x^k - 1$ $(1 \le k < n)$ 在 $\mathbb{Z}[x]$ 中互素.

假设只有有限个素数 $p_1, \ldots, p_m \equiv 1 \pmod{q}$

取 t 为充分大的正整数, 记 $a=tqp_1\dots p_m$. 考虑 $\Phi_q(tqp_1\dots p_m)$ 的素因子 p. 于是 $p|a^q-1$. 因此 $p\neq p_1,\dots,p\neq p_m,p\nmid q$. 于是 $p|\Phi_q(a)|a^q-1$.

设 k 是使得 $p|a^j - 1(j \in \mathbb{Z}^+)$ 成立的最小的 j.

断言. k = q.

下面我们证明断言. 记 $r = \frac{q}{k} \in \mathbb{Z}^+$. 假设 k < q, 即 r < 1.

我们有如下多项式的整除关系

$$\Phi_q(x)|x^q - 1 = (x^k - 1)(x^{k(r-1)} + \dots + x^k + 1)$$

则

$$\Phi_q(x)|(x^{k(r-1)} + \dots + x^k + 1)$$

因此,代入 a有

$$\Phi_q(a)|(a^{k(r-1)} + \dots + a^k + 1)$$

而 $a^k \equiv 1 \pmod{p}$, 于是

$$p|\sum_{j=0}^{r-1} (a^k)^j \equiv r \pmod{p}$$

因此 p|r|a, 与假设矛盾. 这证明了断言.

接下来根据费马小定理, 我们有 $p|a^{p-1}-1$, 则 q|p-1. 因此 $p\equiv 1 \pmod q$. 与假设矛盾.

注. m=0 的情况是有可能的.

1.2 一些数论函数及其性质

现在我们介绍一些函数.

(1) Von Mangoldt 函数 $\Lambda: \mathbb{Z}^+ \to \mathbb{R}$

$$\Lambda(n) = \begin{cases} \log p & n = p^k, p 是素数, k \in \mathbb{Z}^+, \\ 0 & \text{otherwise.} \end{cases}$$

(2) 对一个固定的实数 x, 所有比 x 小的素数个数给出一个函数

$$\pi(x) = \sum_{n \le x} \mathbf{1}_{\mathbb{P}}(n)$$
$$= \sum_{n \le x} 1$$

其中 $1_{\mathbb{P}}$ 是素数集合的特征函数.

(3) 在 $\pi(x)$ 的和式中考虑一个权重

$$\theta(x) = \sum_{n \le x} \mathbf{1}_{\mathbb{P}}(n) \log n$$
$$= \sum_{p \le x} \log p$$

(4)
$$\psi(x) = \sum_{n \le x} \Lambda(x)$$

我们给出一些 Von Mangoldt 函数的性质.

命题 1.4.
$$\sum_{d|n} \Lambda(d) = \log n$$

证明. 循定义验证即可.

命题 1.5. 当 Re(s) > 1 时, $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ 绝对收敛.

证明. 由命题1.4, 我们有

$$\Lambda(n) \le \sum_{d|n} \Lambda(d) = \log n$$

于是
$$\frac{\Lambda(n)}{n^s} \le \frac{\log n}{n^s}$$

至此, 我们粗略的看看下列两个无穷级数的乘积.

$$(\sum_{n=1}^{\infty} \frac{1}{n^s})(\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}) = \sum_{m=1}^{\infty} \sum_{k=1}^{\infty} \frac{1}{m^s} \frac{\Lambda(k)}{k^s}$$
$$= \sum_{n=1}^{\infty} \sum_{\substack{m,k \\ mk=n}} \frac{1}{m^s} \frac{\Lambda(k)}{k^s}$$
$$= \sum_{n=1}^{\infty} \frac{\log n}{n^s} = -\zeta'(s)$$

这几乎得到了 $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ 的表达式,但我们还不清楚 $\zeta(s)$ 的零点,不能将它挪到等式右边.某种程度上它也推动着我们去探索 $\zeta(s)$ 的零点.之后我们会看到这实际上给出了 Von Mangoldt 函数的 Dirichlet 级数.

为了证明素数定理,我们需要做一些准备工作.

定理 1.6. 下列叙述等价.

- (1) $\pi(x) \sim \frac{x}{\log x}$
- (2) $\theta(x) \sim x$
- (3) $\psi(x) \sim x$

证明. $(2 \Leftrightarrow 3)$:

$$0 \le \psi(x) - \theta(x) = \sum_{\substack{k \ge 2 \\ p^k \le x}} \log p$$

$$\le \sum_{\substack{k \ge 2 \\ p^k \le x}} \log x$$

$$\le \sum_{p \le \sqrt{x}} \log p \quad \sum_{2 \le k \le \frac{\log x}{\log p}} 1$$

$$\le \sqrt{x} \log x$$

于是
$$\frac{\psi(x)}{x} - \frac{\theta(x)}{x} \to 0 \ (x \to +\infty)$$
 $(1 \Leftrightarrow 2)$ 只需看下列两个不等式:

对任意正数 $\epsilon > 0$

$$\theta(x) \le \pi(x) \log x$$

$$\theta(x) \ge \sum_{x^{1-\epsilon} \le p \le x} \log x^{1-\epsilon} = (1-\epsilon)(\pi(x) + O(x^{1-\epsilon})) \log x$$

等价性立即可得

注 (Chebyshev). 存在常数 c_1, c_2 满足 $0 < c_1 < 1 < c_2$ 使得

$$c_1 < \frac{\pi(x)}{x/\log x} < c_2$$

我们将在附录证明这个结果.

注 (Riemann). $\zeta(s)$ 可以解析延拓到 $\mathbb{C}\setminus\{1\}$, 并且 1 是单极点. Riemann 还证明了在 Re(s)<0 的范围内所有的零点是 $-2,-4,\ldots$, 即所有负偶数, 且它们是单零点.

猜想 1.7 (Riemann). 若 $0 \le Re(s) \le 1$, 且 $\zeta(s) = 0$, 则 $Re(s) = \frac{1}{2}$.

注. Riemann 猜想 ⇒ 素数定理.

 $\zeta(1+it) \neq 0 \ \forall t \in \mathbb{R} \Rightarrow$ 素数定理.

引理 1.8. 若 $\int_1^\infty \frac{\psi(x)-x}{x^2} dx$ 收敛, 则 $\psi(x) \sim x$.

证明. 用反证法. 假设 $\psi(x) \sim x$ 不成立. 则要么存在 $c_1 > 1$, 使得有一个严格递增趋于无穷的序列 $\{x_n\}$ 满足

$$\psi(x_n) \ge c_1 x_n$$

要么存在 $0 < c_2 < 1$,使得有一个严格递增趋于无穷的序列 $\{y_n\}$ 满足

$$\psi(y_n) \le c_2 y_n$$

若第一种情况成立,则

$$\int_{x_n}^{c_1 x_n} \frac{\psi(x) - x}{x^2} dx \ge \int_{x_n}^{c_1 x_n} \frac{c_1 x_n - x}{x^2} dx$$
$$= c_1 - 1 - \log c_1 > 0$$

这同假设矛盾. 类似地, 若第二种情况成立, 则

$$\int_{c_2 y_n}^{y_n} \frac{\psi(x) - x}{x^2} dx \le \int_{c_2 y_n}^{y_n} \frac{c_2 y_n - x}{x^2} dx$$
$$= -c_2 + 1 + \log c_2 < 0$$

这也同假设矛盾.

2 Riemann zeta 函数与素数定理

我们约定复变量的符号为 $s = \sigma + it$.

2.1 Riemann zeta 函数的基本性质

定理 2.1. 当 Re(s) > 1 时, $\zeta(s) \neq 0$.

证明. s 是实数时结论是显然的.

我们考察 Euler 乘积的形式

$$|\zeta(s)| = |\prod_{p} (1 - \frac{1}{p^s})^{-1}|$$

$$= \prod_{p} |(1 - \frac{1}{p^s})^{-1}|$$

$$\geq \prod_{p} (1 + \frac{1}{p^\sigma})^{-1}$$

$$\geq \prod_{p} (1 - \frac{1}{p^\sigma})$$

$$\geq (\prod_{p} (1 - \frac{1}{p^\sigma})^{-1})^{-1}$$

$$\geq \frac{1}{\zeta(\sigma)} \in \mathbb{R}^+$$

即 $\zeta(s) \neq 0$.

注. 现在回过头看第一节的结果, 我们有当 Re(s) > 1 时,

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$$

定理 2.2. 当 Re(s) > 1 时, 我们有

$$\zeta(s) = \frac{s}{s-1} - s \int_{1}^{+\infty} \{x\} x^{-s-1} dx \tag{4}$$

并且 (4) 给出了 $\zeta(s)$ 在 $Re(s) > 0 (s \neq 1)$ 的解析延拓且 s = 1 是单极点.

证明. 当 Re(s) > 2 时, 我们有

$$\sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s}) = \sum_{n=1}^{\infty} nn^{-s} - \sum_{n=1}^{\infty} n(n+1)^{-s}$$
$$= \sum_{n=1}^{\infty} n^{-s+1} - \sum_{n=1}^{\infty} (n+1)^{-s+1} + \sum_{n=1}^{\infty} (n+1)^{-s}$$
$$= \zeta(s)$$

继续计算有

$$\zeta(s) = \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s})$$

$$= s \sum_{n=1}^{\infty} n \int_{n}^{n+1} x^{-s-1} dx$$

$$= s \sum_{n=1}^{\infty} \int_{n}^{n+1} [x] x^{-s-1} dx$$

$$= s \sum_{n=1}^{\infty} \int_{n}^{n+1} (x - \{x\}) x^{-s-1} dx$$

$$= s \sum_{n=1}^{\infty} \int_{n}^{n+1} x^{-s} dx - s \sum_{n=1}^{\infty} \int_{n}^{n+1} \{x\} x^{-s-1} dx$$

$$= \frac{s}{s-1} - s \int_{1}^{+\infty} \{x\} x^{-s-1} dx$$

不难发现 $\frac{s}{s-1} - s \int_1^{+\infty} \{x\} x^{-s-1} dx$ 是 $\zeta(s)$ 到 $Re(s) > 0 (s \neq 1)$ 的延拓且 s=1 是单极点.

现在为了将 $\zeta(s)$ 延拓到整个复平面上, 我们需要回顾一些关于 Gamma 函数 Γ 的重要性质. 更多细节请读者查阅 [3], Ch.6.

在 Re(s) > 0 上我们定义 Gamma 函数为

$$\Gamma(s) = \int_0^{+\infty} x^{s-1} e^{-x} dx.$$

不难验证我们有

$$\Gamma(s+1) = s\Gamma(s)$$

由此我们可以将 Γ 延拓成复平面上的亚纯函数且只有单极点 $s=0,-1,-2,\ldots,$ 且没有零点 (考察 $\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s}$).

接下来我们就可以着手将 $\zeta(s)$ 延拓到整个复平面上.

对
$$x > 0$$
,引入函数 $\theta(x) = \sum_{-\infty}^{+\infty} e^{-n^2 x \pi} (= 1 + 2 \sum_{n=1}^{\infty} e^{-n^2 x \pi}).$

引理 2.3. x > 0 时, $\theta(\frac{1}{x}) = \sqrt{x}\theta(x)$.

证明. 考虑 Poisson 公式有

$$\theta(x) = \sum_{n \in \mathbb{Z}} \int_{-\infty}^{+\infty} e^{u^2 x \pi - 2\pi i n u} du$$

$$= \sum_{n \in \mathbb{Z}} \int_{-\infty}^{+\infty} e^{-x \pi (u + i n \frac{1}{x})^2 - \pi n^2 \frac{1}{x}} du$$

$$= \sum_{n \in \mathbb{Z}} e^{-\pi n^2 \frac{1}{x}} \int_{-\infty}^{+\infty} e^{-\pi x (u + i n \frac{1}{x})^2} du$$

$$= \sum_{n \in \mathbb{Z}} e^{-\pi n^2 \frac{1}{x}} \int_{-\infty}^{+\infty} e^{-\pi x u^2} du$$

$$= \theta(\frac{1}{x}) \frac{1}{\sqrt{x}}$$

定理 2.4. 对 $s \in \mathbb{C}$,

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = -\frac{1}{s(1-s)} + \int_{1}^{+\infty} (x^{\frac{s}{2}-1} + x^{\frac{1-s}{2}-1}) \frac{\theta(x) - 1}{2} dx.$$

一个立即得到的推论是

推论 2.5.
$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s) \ (s \neq 0,1).$$

思考. 如何判断 $\zeta(s)$ 的零点问题.

下面我们来证明定理2.4.

证明.

$$\begin{split} \Gamma(\frac{s}{2})\zeta(s) &= \int_{0}^{+\infty} x^{\frac{s}{2}-1} e^{-x} dx \sum_{n=1}^{\infty} \frac{1}{n^{s}} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^{s}} \int_{0}^{+\infty} x^{\frac{s}{2}-1} e^{-x} dx \\ &= \frac{(x = \pi n^{2}y)}{2} \sum_{n=1}^{\infty} \frac{1}{n^{s}} \int_{0}^{+\infty} \pi^{\frac{s}{2}-1} n^{s-2} y^{\frac{s}{2}-1} e^{-\pi n^{2}y} \pi n^{2} dy \\ &= \pi^{\frac{s}{2}} \sum_{n=1}^{\infty} \int_{0}^{+\infty} y^{\frac{s}{2}-1} r^{-\pi n^{2}y} dy \\ &= \pi^{\frac{s}{2}} \int_{0}^{+\infty} y^{\frac{s}{2}-1} \sum_{n=1}^{\infty} e^{-\pi n^{2}y} dy \\ &= \pi^{\frac{s}{2}} \int_{0}^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy \end{split}$$

将积分拆开如下

$$\begin{split} \pi^{\frac{s}{2}} \int_{0}^{\infty} y^{\frac{s}{2}-1} \frac{\theta(y)-1}{2} dy &= \pi^{\frac{s}{2}} \int_{1}^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y)-1}{2} dy + \pi^{\frac{s}{2}} \int_{0}^{1} y^{\frac{s}{2}-1} \frac{\theta(y)-1}{2} dy \\ &= \frac{(y=\frac{1}{x})}{2} \pi^{\frac{s}{2}} \int_{1}^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y)-1}{2} dy + \pi^{\frac{s}{2}} \int_{1}^{+\infty} x^{-\frac{s}{2}-1} \frac{\theta(\frac{1}{x})-1}{2} dx \\ &= \pi^{\frac{s}{2}} \int_{1}^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y)-1}{2} dy + \pi^{\frac{s}{2}} \int_{1}^{+\infty} x^{-\frac{s}{2}-1} \frac{\sqrt{x}\theta(x)-1}{2} dx \\ &= \pi^{\frac{s}{2}} \int_{1}^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y)-1}{2} dy + \pi^{\frac{s}{2}} \int_{1}^{+\infty} x^{-\frac{s}{2}-1} \frac{\sqrt{x}(\theta(x)-1)+\sqrt{x}-1}{2} dx \\ &= \pi^{\frac{s}{2}} \int_{1}^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y)-1}{2} dy + \pi^{\frac{s}{2}} \int_{1}^{+\infty} x^{-\frac{s}{2}-1} \frac{\theta(x)-1}{2} dx - \pi^{\frac{s}{2}} \frac{1}{s(1-s)}. \end{split}$$

上面证明了 Re(s) > 2 时原式成立. 由解析函数的性质, 我们有原式对 Re(s) > 0 时也成立, 并且它给出了等式左边到 $\mathbb{C} \setminus \{0,1\}$ 的延拓.

推论 2.6. 上述定理给出了 $\zeta(s)$ 到 $\mathbb{C}\setminus\{1\}$ 的解析延拓, 且 s=1 是单极点. 并且 $\zeta(0)\neq 0$, $\zeta(-2)=\zeta(-4)=\cdots=0$ 是单零点 (有时称作平凡零点).

推论 2.7. Re(s) < 0 时, 负偶数是 $\zeta(s)$ 的所有零点.

事实上我们现在才能真正叙述 Riemann 猜想, 除去之前给出的叙述, 我们还能将其叙述为: $\zeta(s)$ 的所有非平凡零点的实部为 $\frac{1}{2}$.

定理 2.8. $\zeta(1+it) \neq 0 \ (\forall t \in \mathbb{R})$.

证明. 不妨 $t \neq 0$. 考虑 $s = \sigma + it$.

$$\begin{split} \zeta(\sigma+it) &= \prod_{p} (1-\frac{1}{p^{\sigma+it}}) \\ &= \exp\big(\log \prod_{p} (1-\frac{1}{p^{\sigma+it}})\big) \\ &= \exp\big(\sum_{p} \sum_{m=1}^{\infty} \frac{1}{mp^{m(\sigma+it)}}\big) \\ &= \exp\big(\sum_{p} \sum_{m=1}^{\infty} \frac{\cos\big(\log p\big)mt - i\sin\big(\log p\big)mt}{mp^{m\sigma}}\big). \end{split}$$

于是

$$|\zeta(\sigma + it)| = \exp\left(\sum_{p} \sum_{n=1}^{\infty} \frac{\cos(\log p)mt}{mp^{m\sigma}}\right).$$

考察

$$|\zeta(\sigma)^3 \zeta(\sigma + it)^4 \zeta(\sigma + 2it)| = \exp\left(\sum_{p} \sum_{m=1}^{\infty} \frac{3 + 4\cos(\log p)mt + \cos(\log p)m2t}{mp^{m\sigma}}\right).$$

对于等号右边的分子, 我们有

$$3 + 4\cos(\log p)mt + \cos(\log p)m2t = 2(\cos mt \log p + 1)^2 \ge 0.$$

于是

$$|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)| \ge 1.$$

倘若对某个 t, 1+it 是零点, 则下述不等式

$$(\zeta(\sigma)(\sigma-1))^3 \left| \frac{\zeta(\sigma+it)}{\sigma-1} \right|^4 \left| \zeta(\sigma+2it) \right| \ge \frac{1}{\sigma-1}$$

 ϕ σ → 1⁺ 时左边是常数而右边趋于无穷, 矛盾.

2.2 素数定理

引理 2.9. 设 f(u) 是 (可积, 间断点离散)实函数.

(1) 存在 M > 0, s.t. $|f(u)| \le \frac{M}{u}$ $(\forall u \ge 1)$.

(2)
$$g(s) = \int_{1}^{+\infty} \frac{f(u)}{u^{s}} du \ (Re(s) > 0)$$
 可以延拓到 $Re(s) \ge 0$.

则积分 $\int_{1}^{+\infty} f(u)du$ 收敛.

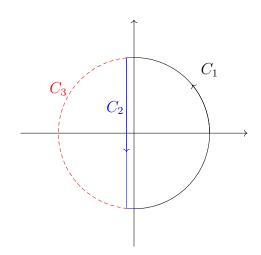
证明. 引入 $g_x(s) = \int_1^x \frac{f(u)}{u^s}$ ($\forall s$),要证结论即转为 $\lim_{x \to +\infty} g_x(0) = g(0)$. 对充分大的 R,存在 $h_R > 0$,s.t. g(s) 在 $Re(s) \geq -h_R$ 且 $|Im(s)| \leq R$ 的范围内解析. 任取正数 $h < h_R$,存在 M_R ,s.t. $|g(s)| \leq M_R$ ($\forall s \in D_R$). 其中 D_R 是由积分围道 $C(=C_1+C_2)$ 围成的闭集,虚轴右端的半圆记为 C_1 ,即

$$C_1 = \{ s \mid Re(s) \ge 0, |s| = R \}$$

 $C_2 = C - C_1$, 虚轴左边的半圆记为 C_3 , 即

$$C_3 = \{ s \mid Re(s) \le 0, |s| = R \}$$

如下图所示.



根据 Cauchy 积分公式, 我们有

$$g_x(0) - g(0) = \frac{1}{2\pi i} \int_C \frac{g_x(s) - g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1\right) ds$$

于是原积分改写为

$$\frac{1}{2\pi i} \int_C \frac{g_x(s) - g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1\right) ds = \frac{1}{2\pi i} \int_{C_1} \frac{g_x(s) - g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1\right) ds + \frac{1}{2\pi i} \int_{C_2} \frac{g_x(s) - g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1\right) ds$$

其中

$$\frac{1}{2\pi i} \int_{C_2} \frac{g_x(s) - g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1\right) ds = \frac{1}{2\pi i} \int_{C_3} \frac{g_x(s)}{s} x^s \left(\frac{s^2}{R^2} + 1\right) ds - \frac{1}{2\pi i} \int_{C_2} \frac{g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1\right) ds$$

下面我们分别考虑这些积分.

在
$$C_1$$
 上, 有 $|x^s| = x^{\sigma}$, $|\frac{1}{s}| = \frac{1}{R}$, $|\frac{s^2}{R^2} + 1| = \frac{2\sigma}{R}$. 当 $\sigma > 0$ 时

$$|g_x(s) - g(s)| = \left| \int_x^{+\infty} \frac{f(u)}{u^s} ds \right|$$

$$\leq M \left| \int_x^{+\infty} \frac{1}{u^{\sigma+1}} du \right| = \frac{M}{\sigma} x^{-\sigma}$$

于是

$$\left|\frac{1}{2\pi i} \int_{C_1} \frac{g_x(s) - g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1\right) ds\right| \le \left|\frac{1}{2\pi i} \pi R \cdot \frac{M}{\sigma} x^{-\sigma} \cdot x^{\sigma} \cdot \frac{1}{R} \cdot \frac{2\sigma}{R}\right|$$

$$\le \frac{M}{R} \quad (\sigma \ge 0, \ s \in C_1)$$

类似地有

$$\left| \frac{1}{2\pi i} \int_{C_3} \frac{g_x(s)}{s} x^s \left(\frac{s^2}{R^2} + 1 \right) ds \right| \le \frac{M}{R} \quad (\sigma \le 0, \ s \in C_3)$$

而在 C_2 上, 我们把它分为两个小弧段和直线, 依次有

$$\left| \frac{1}{2\pi i} \int_{C_2} \frac{g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1 \right) ds \right| \le \left| \frac{1}{2\pi i} \cdot 2\frac{\pi}{2} h \left(\frac{M_R}{R} x^{\sigma} \frac{2\sigma}{R} \right) \right| + \left| \frac{1}{2\pi i} \cdot \frac{M_R}{h} \cdot x^{-h} \cdot 2 \right|$$

$$\le \frac{M_R h^2}{R^2} + x^{-h} \frac{2RM_R}{\pi h}$$

综上, 我们有

$$|g_x(0) - g(0)| \le \frac{2M}{R} + \frac{M_R h^2}{R^2} + x^{-h} \frac{2RM_R}{\pi h}$$

于是对于任意的 $\varepsilon > 0$,能够(依次)取到合适的 R,h, s.t. $\exists x_0,$ 对任意的 $x > x_0,$ $|g_x(0) - g(0)| \le \varepsilon.$

定理 2.10. $\psi(x) \sim x$.

证明. 根据引理1.8和引理2.9, 要证素数定理, 只需证 $f(u) = \frac{\psi(u)-u}{u^2}$ 满足引理2.9的两个条件. 我们已经知道存在正常数 c_1, c_2 使得 $c_1x \leq \psi(x) \leq c_2x$, 这就满足了第一个条件. 对于第二个条件, Re(s) > 0 时, 我们考虑

$$\begin{split} g(s) &= \int_{1}^{+\infty} \frac{\psi(u) - u}{u^{s+2}} du = \int_{1}^{+\infty} \frac{\sum_{n \leq u} \Lambda(n)}{u^{s+2}} du - \frac{1}{s} \\ &= \sum_{n=1}^{\infty} \Lambda(n) \int_{n}^{+\infty} \frac{1}{u^{s+2}} du - \frac{1}{s} \\ &= -\frac{1}{s+1} \frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{1}{s} \end{split}$$

只用代入延拓后的 Riemann zeta 函数 (4) 即可证得其满足第二个条件.

3 算术级数中的素数分布 I

本章目的是证明如下的 Dirichlet 定理

定理 3.1 (Dirichlet). 给定 $a,q \in \mathbb{Z}^+, (a,q) = 1$. 则有无穷多个素数形如 $p \equiv a \pmod{q}$. 即

$$\{a + qk \mid k \in \mathbb{Z}^+\}$$

中有无穷多个素数.

为了证明这个定理, 我们需要做一些准备工作. 若无特殊声明, 本节提到的群均为有限 Abel 群.

3.1 有限 Abel 群的特征

群的特征是 Dedekind 研究所谓群行列式的时候发现的, 这实际上也是群表示论的开端. 感兴趣的读者仅需要高等代数和一些抽象代数的知识就可以阅读 [3], 有更强大背景的读者想必可以从 [7] 中汲取大量营养.

定义 3.2. 从群 G 到 $\mathbb{C}^{\times} = \mathbb{C} \setminus \{0\}$ 的群同态

$$\chi:G\to\mathbb{C}^{\times}$$

称为群 G 的一个特征. 所有特征构成的集合记为 G^*

注. 不难看出 G^* 非空, 因为 $[q \mapsto 1] \in G^*$

注. 若记 |G| = n, 则对任意 $q \in G$, $\chi(q)$ 都是 n 次单位根.

我们称上述恒映到 1 的特征为主特征, 记为 χ_0 . 本文中有时为了强调它作为单位元, 也记作 id_{G^*} , 引入乘法

$$\chi_1 * \chi_2 : G \to \mathbb{C}^\times$$
$$g \mapsto [\chi_1 * \chi_2(g) := \chi_1(g)\chi_2(g)]$$

于是不难验证有

引理 3.3. G* 构成有限 Abel 群.

注. 由于特征 χ 都是单位根, 它的逆可以写成 $\chi^{-1}: g \mapsto \chi^{-1}(g) = \chi(g^{-1}) = \overline{\chi(g)}$.

定理 3.4. 我们有如下群同构

$$G \cong G^*$$
.

证明. Step 1. 我们首先证明结论对循环群成立.

记
$$G = \langle g \rangle, |g| = |G| = n$$
. 于是对任意 $\chi \in G^*$,

$$\chi(g) \in \{e^{2\pi i \frac{k}{n}} \mid 0 \le k \le n - 1\}.$$

定义

$$\chi_k : G \to \mathbb{C}^*$$

$$g^j \mapsto \left[\chi_k(g^j) = e^{2\pi i \frac{kj}{n}} \right] \quad (0 \le j \le n - 1)$$

不难验证 $\chi_k \in G^*$, 更进一步 G^* 是循环群.

Step 2. 我们现在证明对有限 Abel 群 $A, B, (A \times B)^* \equiv A^* \times B^*$. 引入

$$\rho: A^* \times B^* \to (A \times B)^*$$
$$(\sigma, \tau) \mapsto [\rho(\sigma, \tau) : (a, b) \mapsto \sigma(a)\tau(b)]$$

不难验证这样定义的 $\rho(\sigma,\tau)$ 确实是 $A\times B$ 上的特征, 更进一步 ρ 是一个群同态. 要证它是同构, 只需证它既是单射又是满射.

(单射) 若对任意 $a \in A$, $b \in B$, $\rho(\sigma, \tau)(a, b) = \sigma(a)\tau(b) = 1$. 取定 $a = \mathrm{id}_A$, 则 $\forall b, \tau(b) = 1$, 于是 $\tau = \mathrm{id}_{B^*}$. 取定 $b = \mathrm{id}_B$, 则 $\forall a, \sigma(a) = 1$, 于是 $\sigma = \mathrm{id}_{A^*}$.

(满射) 对任意 $f \in (A \times B)^*$, 取 $\sigma : a \to f(a, \mathrm{id}_B) \ \forall a \in A, \tau : b \to f(\mathrm{id}_A, b) \ \forall b \in B$. 不难验证 $\sigma \in A^*, \tau \in B^*$, 且 $\rho(\sigma, \tau) = f$.

于是根据有限 Abel 群的结构定理即证.

定理 3.5 (正交关系). 设 G 为有限 Abel 群,

(1)
$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = \begin{cases} 1 & \chi = \chi_0, \\ 0 & otherwise. \end{cases}$$

(2)
$$\frac{1}{|G|} \sum_{\chi \in G^*} \chi(g) = \begin{cases} 1 & g = \mathrm{id}_G, \\ 0 & otherwise. \end{cases}$$

证明. (1) 只需考虑 $\chi \neq \chi_0$ 的情况. 此时 $\exists s \in G \text{ s.t. } \chi(s) \neq 1$, 则

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(sg)$$
$$= \chi(s) \sum_{g \in G} \chi(g)$$

于是 $(1-\chi(s))\sum_{g\in G}\chi(g)=0.$

(2) 只需考虑 $g \neq \mathrm{id}_G$ 的情况. 我们首先证明对这样的 g, 存在 $\tau \in G^*$ s.t. $\tau(g) \neq 1$. 如果不然,即对任意的 $\chi \in G^*$, $\chi(g) = 1$. χ 自然诱导从商群 $G/\langle g \rangle$ 到 \mathbb{C}^* 的同态

$$\tilde{\chi}: G/\langle g \rangle \to \mathbb{C}^{\times}$$

$$h \cdot \langle g \rangle \mapsto \chi(h)$$

于是 $|G| = |G^*| \le |(G/\langle g \rangle)^*| = |G/\langle g \rangle|$, 矛盾. 其余部分与 (1) 同理.

注. 我们也可以从另一个角度看这个定理. 对有限 Abel 群 $G, G^* \cong G$ 也是有限 Abel 群,于是我们可以考虑 G^* 的特征,它由 G 中的元素给出:

$$g:G^*\to\mathbb{C}^\times$$

$$\chi\mapsto\langle g,\chi\rangle:=\chi(g)$$

不难验证他们同样构成一个有限 Abel 群 $(G^*)^*$. 于是有 $G \cong G^* \cong (G^*)^*$. 那么定理3.5中的 (2) 就可以由 (1) 直接推出:

$$\sum_{\chi \in G^*} \chi(g) = \sum_{\chi \in G^*} \langle g, \chi \rangle.$$

这立刻给出下面两条推论.

推论 3.6. 对 $\chi_1, \chi_2 \in G^*$,

$$\frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \begin{cases} 1 & \chi_1 = \chi_2, \\ 0 & otherwise. \end{cases}$$

证明. 我们有

$$\frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_1 \chi_2^{-1}(g)$$

由定理3.5(1) 立即可得.

推论 3.7. 对 $g_1, g_2 \in G$,

$$\frac{1}{|G|} \sum_{\chi \in G^*} \chi(g_1) \overline{\chi(g_2)} = \begin{cases} 1 & g_1 = g_2, \\ 0 & otherwise. \end{cases}$$

证明. 注意到对任意特征 χ , $\chi(g)\overline{\chi(g)}=\chi(g)\chi(g^{-1})=1$, 于是

$$\frac{1}{|G|} \sum_{\chi \in G^*} \chi(g_1) \overline{\chi(g_2)} = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(g_1 g_2^{-1})$$

由定理3.5(2) 立即可得.

3.2 Dirichlet L 函数及其性质

现在我们着手把上述理论应用到 $G = (\mathbb{Z}/q\mathbb{Z})^{\times}$ 上.

定义 3.8 (Dirichlet 特征). 对 $q \in \mathbb{Z}^+$ $(q \ge 2)$, $\chi \in G^*$, $\overline{m} \in G$. 我们称

$$\chi_D(m) = \begin{cases} \chi(\overline{m}) & (m,q) = 1, \\ 0 & (m,q) > 1. \end{cases}$$

给出的函数

$$\chi_D: \mathbb{Z} \to \mathbb{C}$$

为 (mod q) 的 Dirichlet 特征.

注. 一共有 $\varphi(q)$ 个 mod q 的 Dirichlet 特征. 其中 φ 是 Euler 函数.

下面给出一些关于 Dirichlet 特征 (的由定义和正交关系立即可得) 的性质.

命题 3.9. 设 χ 是 mod q 的特征, 则 χ 是完全积性的, 即 $a,b \in \mathbb{Z}$,

$$\chi(ab) = \chi(a)\chi(b)$$

命题 3.10. 对 $a, b \in \mathbb{Z}$,

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \chi(a) \overline{\chi(b)} = \begin{cases} 1 & a \equiv b \pmod{q} \text{ } \mathbb{L} \text{ } (ab,q) = 1, \\ 0 & otherwise. \end{cases}$$

其中 $\sum_{\chi \pmod{q}}$ 表示对所有 $\mod q$ 的特征求和.

命题 3.11. 对 $a \in \mathbb{Z}$,

$$\frac{1}{\varphi(q)} \sum_{1 \le a \le q} \chi(a) = \begin{cases} 1 & \chi = (\mathrm{id}_{G^*})_D, \\ 0 & otherwise. \end{cases}$$

命题 3.12. χ 是周期为 q 的函数.

定义 3.13 (Dirichlet L-函数). 在 Re(s) > 1 时, 我们定义

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

$$= \prod_{p} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right)$$

$$= \prod_{p\nmid a} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

$$= \prod_{p\nmid a} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

 $L(s,\chi)$ 称为 Dirichlet L-函数.

称 G^* 中单位元给出的 Dirichlet 特征为 (Dirichlet) 主特征, 在无歧义的情况下仍记为 χ_0 . 即

$$\chi_0(m) = \begin{cases} 1 & (m,q) = 1, \\ 0 & (m,q) > 1. \end{cases}$$

注. 若非主特征 $\chi(n)$ 总是实数,则称为非主实特征. 非实特征称为复特征,即 $\exists n$ s.t. $\chi_n \notin \mathbb{R}$.

引理 3.14. 设 χ 是 mod q 的 Dirichlet 特征, $x \ge 1$.

(1) 若 χ 不是主特征,则

$$|\sum_{n \le x} \chi(n)| \le \varphi(q)$$

2 若 $\chi = \chi_0$, 则

$$\left|\sum_{n \le x} \chi(n) - \frac{\varphi(q)}{q} x\right| \le 2\varphi(q)$$

证明. 由于周期性, 我们可以把求和写成如下形式:

$$\sum_{n \le x} \chi(n) = \left[\frac{x}{q}\right] \sum_{1 \le a \le q} \chi(a) + R,$$

其中 $|R| \le \sum_{1 \le a \le q} |\chi(a)| \le \varphi(q)$. 于是当 $\chi \ne \chi_0$ 时, 由命题可知 $\sum_{1 \le a \le q} \chi(a) = 0$. 当 $\chi = \chi_0$ 时, $\sum_{1 \le a \le q} \chi(a) = \varphi(q)$.

命题 3.15. 对正实数 s, 当 χ 不是主特征时, $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ 收敛, 但不绝对收敛. 当 $\chi = \chi_0$ 时, $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ 不收敛.

证明. $\chi \neq \chi_0$ 时,由于 $|\sum_{n=1}^N \chi(n)| \leq \varphi(q)$,根据 Dirichlet 关于条件收敛的判据可知 s>0 时, $\sum_{n=1}^\infty \frac{\chi(n)}{n^s}$ 收敛.

命题 3.16. $L(s,\chi_0)$ 可以延拓到整个复平面, s=1 是单极点.

证明. 注意到
$$L(s,\chi_0) = \prod_{p|q} (1 - \frac{1}{p^s})\zeta(s)$$
.

命题 3.17. 当 $\chi \neq \chi_0$, Re(s) > 1 时, 有

$$L(s,\chi) = \frac{1}{s} \int_{1}^{\infty} F_{\chi}(u) u^{-s-1} du$$

其中 $F_\chi(u) = \sum_{1 \le a \le u} \chi(a)$. 并且上式给出了 $L(s,\chi)$ 在 Re(s) > 0 上的解析延拓.

证明. 由分部求和有

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{F_{\chi}(n) - F_{\chi}(n-1)}{n^s}$$

$$= \sum_{n=1}^{\infty} F_{\chi}(n) (n^{-s} - (n+1)^{-s})$$

$$= \frac{1}{s} \sum_{n=1}^{\infty} F_{\chi}(n) \int_{n}^{n+1} u^{-s-1} du$$

$$= \frac{1}{s} \sum_{n=1}^{\infty} \int_{n}^{n+1} F_{\chi}(u) u^{-s-1} du$$

$$= \frac{1}{s} \int_{1}^{+\infty} F_{\chi}(u) u^{-s-1} du.$$

根据引理 3.14. 可知上式最后的积分的收敛性.

推论 3.18. 设 $q \ge 3$, 则有 $\chi \ne \chi_0$ 时的 $\varphi(q) - 1$ 个 Dirichlet 函数中至多有一个 函数在 s = 1 处为零. 且若 $L(1,\chi) = 0$ $(\chi \ne \chi_0)$, 则 s = 1 是 $L(s,\chi)$ 的单零点.

证明. 对实数 s > 1 考察

$$\prod_{\chi(\text{mod}q)} L(s,\chi) = \prod_{\chi(\text{mod}q)} \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

$$= \exp\left(\sum_{\chi(\text{mod}q)} \sum_{p} \log\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}\right)$$

$$= \exp\left(\sum_{\chi} \sum_{p} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}\right)$$

$$= \exp\left(\sum_{\chi} \sum_{p} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}\right)$$

$$= \exp\left(\varphi(q) \sum_{k} \sum_{p^k \equiv 1 \pmod{q}} \frac{1}{kp^{ks}}\right) \ge 1.$$

我们知道 s=1 是 $L(s,\chi_0)$ 的一个单极点, 而 $\chi \neq \chi_0$ 时 $L(s,\chi)$ 在 s=1 处是解析的. 于是若有超过一个函数在 s=1 处为零则乘积为 0,与上述计算结果矛盾.

推论 3.19. 设 χ 是复特征, 则 $L(1,\chi) \neq 0$.

证明. 取 χ 的共轭函数 $\overline{\chi}$, 它也是 mod q 的 Dirichlet 特征. χ 和 $\overline{\chi}$ 是不同的函数,且 $L(1,\chi)=0 \Leftrightarrow L(1,\overline{\chi})=0$. 当实数 s>1 时有 $L(s,\overline{\chi})=\overline{L(s,\chi)}$. 取 $s\to 1^+$ 即证.

我们介绍一个非常重要的公式,并给出一些估计.

定理 3.20 (Abel 求和公式 (部分求和公式)). 对于任意 $y \in \mathbb{R}, y \geq 1$, 我们有

$$\sum_{1 \le n \le y} a(n)b(n) = \sum_{1 \le n \le y} a(n)b(y) - \int_1^y \left(\sum_{1 \le n \le t} a(n)\right)b'(t)dt$$

证明. 注意到

$$\int_{1}^{y} \left(\sum_{1 \le n \le t} a(n) \right) b'(t) dt = \sum_{1 \le n \le y} a(n) \int_{n}^{y} b'(t) dt = \sum_{1 \le n \le y} a(n) (b(y) - b(n)).$$

易见等式成立. □

我们首先给出一个在数学分析中已经知道的估计.

推论 3.21. 我们有

$$\sum_{n=1}^{y} \frac{1}{n} = \log y + \gamma + O(\frac{1}{y})$$

其中 γ 称为 Euler 常数.

证明.

$$\sum_{n=1}^{y} \frac{1}{n} = 1 + \int_{1}^{y} [t] \frac{1}{t^{2}} dt$$

$$= 1 + \int_{1}^{y} \frac{1}{t} dt - \int_{1}^{y} \{t\} \frac{1}{t^{2}} dt$$

$$= \log y + 1 - \int_{1}^{+\infty} \{t\} \frac{1}{t^{2}} dt + O(\frac{1}{y})$$

$$= \log y + \gamma + O(\frac{1}{y}).$$

其中
$$\gamma = 1 - \int_{1}^{+\infty} \{t\} \frac{1}{t^2} dt$$
.

下面给出两个在之后的证明中要用到的估计.

推论 3.22. 我们有

$$\sum_{n=1}^{y} \frac{1}{\sqrt{n}} = 2\sqrt{y} + A + O(\frac{1}{\sqrt{y}})$$

其中 A 是一个常数.

证明.

$$\begin{split} \sum_{n=1}^{y} \frac{1}{\sqrt{n}} &= y \frac{1}{\sqrt{y}} + \frac{1}{2} \int_{1}^{y} [t] t^{-\frac{3}{2}} dt \\ &= \sqrt{y} + \frac{1}{2} \int_{1}^{y} t^{-\frac{1}{2}} dt - \frac{1}{2} \int_{1}^{y} \{t\} t^{-\frac{3}{2}} dt \\ &= 2\sqrt{y} - 1 - \frac{1}{2} \int_{1}^{+\infty} \{t\} t^{-\frac{3}{2}} dt + O(y^{-\frac{1}{2}}) \\ &2\sqrt{y} + A + O(\frac{1}{\sqrt{y}}). \end{split}$$

其中 $A = -1 - \frac{1}{2} \int_{1}^{+\infty} \{t\} t^{-\frac{3}{2}} dt$.

推论 3.23. 对于非主的 $mod\ q$ 特征 χ , $\beta > 0$, $y \ge 1$ 是实数. 我们有

$$\sum_{n=1}^{y} \frac{\chi(n)}{n^{\beta}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{\beta}} + O(\frac{1}{y^{\beta}})$$

证明. 任取 $Y\in\mathbb{Z}^+$ $(y\leq Y)$, 对 $n\leq Y$, 我们取 $a(n)=\chi(n)$ $(y\leq n\leq Y)$, 其余情况取 0, $b(n)=\frac{1}{n^\beta}$. 套用 Abel 求和公式我们有

$$\sum_{y \le n \le Y} \frac{\chi(n)}{n^{\beta}} = \sum_{y \le n \le Y} \frac{\chi(n)}{y^{\beta}} - \int_{1}^{y} \sum_{y \le n \le t} \chi(n) t^{-\beta - 1} dt$$
$$\le \varphi(q) y^{-\beta} + \varphi(q) y^{-\beta}$$
$$\le 2\varphi(q) y^{-\beta}$$

此式对任意 $Y \in \mathbb{Z}^+$ $(y \leq Y)$ 都成立. 推论即证.

定理 3.24. 设 χ 是 mod q 的非主特征,则有

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

证明. 对于实数 s > 1, 取 y,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{n=1}^{y} \frac{\chi(n)}{n^s} + \sum_{n>y} \frac{\chi(n)}{n^s}$$

于是有

$$|L(s,\chi) - \sum_{n=1}^{y} \frac{\chi(n)}{n^s}| \le 2\varphi(q)y^{-s} \le 2\varphi(q)y^{-1}$$

则

$$|L(1,\chi) - \sum_{n=1}^{y} \frac{\chi(n)}{n}| \le 2\varphi(q)y^{-1}.$$

即有
$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}$$
.

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(a(n))}{a(n)^s}.$$

引理 3.25. 设 χ 是非主实特征, $y \ge 1$, 令 $D(n) = \sum_{d|n} \chi(d)$.

$$\sum_{n \le y} D(n) n^{-\frac{1}{2}} = 2L(1, \chi) y^{\frac{1}{2}} + O(1).$$

证明. 我们用 Dirichlet 双曲律 (定理) 证明这个引理.

$$\sum_{n \le y} \frac{D(n)}{\sqrt{n}} = \sum_{\substack{a,b \le y \\ ab \le y}} \frac{\chi(a)}{\sqrt{ab}}$$

$$= \sum_{a \le \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \le \frac{y}{a}} \frac{1}{\sqrt{b}} + \sum_{b \le \sqrt{y}} \frac{1}{\sqrt{b}} \sum_{a \le \frac{y}{b}} \frac{\chi(a)}{\sqrt{a}}$$

$$- \sum_{a \le \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \le \sqrt{y}} \frac{\chi(b)}{\sqrt{b}}$$

我们分别估计这三项.

$$\begin{split} \sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \leq \frac{y}{a}} \frac{1}{\sqrt{b}} &= \sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{(a)}} \left(2\sqrt{\frac{y}{a}} + A + O(\sqrt{\frac{a}{y}}) \right) \\ &= 2\sqrt{y} \left(\sum_{n=1}^{\infty} \frac{\chi(a)}{a} + O(\frac{1}{\sqrt{y}}) \right) + A \left(\sum_{n=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(y^{-\frac{1}{4}}) \right) + O(1) \\ &= 2\sqrt{y} L(1, \chi) + O(1) \\ \sum_{b \leq \sqrt{y}} \frac{1}{\sqrt{b}} \sum_{a \leq \frac{y}{b}} \frac{\chi(a)}{\sqrt{a}} &= \sum_{b \leq \sqrt{y}} \frac{1}{\sqrt{b}} \left(\sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(\sqrt{\frac{b}{y}}) \right) \\ &= \sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} \left(2y^{\frac{1}{4}} + A + O(y^{-\frac{1}{4}}) \right) + O(1) \\ &= 2y^{\frac{1}{4}} \sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(1) \\ \sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \leq \sqrt{y}} \frac{\chi(b)}{\sqrt{b}} &= \left(\sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(y^{-\frac{1}{4}}) \right) \left(2y^{\frac{1}{4}} + A + O(y^{-\frac{1}{4}}) \right) \\ &= 2y^{\frac{1}{4}} \sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(1). \end{split}$$

于是我们得到

$$\sum_{n \le y} D(n) n^{-\frac{1}{2}} = 2L(1, \chi) y^{\frac{1}{2}} + O(1).$$

定理 3.26. 设 χ 是非主实特征, 则 $L(1,\chi) \neq 0$.

证明. 设 p 是素数, $a \in \mathbb{Z}^+$, 则

$$D(p^a) = \sum_{d|p^a} \chi(d) = 1 + \chi(p) + \dots + \chi(p)^a.$$

由于 χ 是实特征, 不难得到若 n 是完全平方数, $D(n) \ge 1$, 且对任意 n, $D(n) \ge 0$. 于是

$$\sum_{n \le y} \frac{D(n)}{\sqrt{n}} \ge \sum_{m^2 \le y} \frac{D(m^2)}{\sqrt{m^2}} \ge \sum_{m \le \sqrt{y}} \frac{1}{m}.$$
 (5)

若
$$L(1,\chi)=0$$
,根据引理3.25我们有 $\sum_{n\leq y}\frac{D(n)}{\sqrt{n}}=O(1)$. 这同 (5) 矛盾.

推论 3.27. 对 $q \in \mathbb{Z}^+$ (不妨 $q \ge 3$). 由

$$\sum_{p \equiv 1 \pmod{q}} \frac{1}{p} = \infty$$

特别地, 有无穷多个素数 $p \equiv 1 \pmod{q}$.

3.3 Dirichlet 定理的证明

引理 3.28.
$$\sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} = -\frac{L'(s,\chi)}{L(s,\chi)}.$$

证明.

$$\left(\sum_{m=1}^{\infty} \frac{\Lambda(m)\chi(m)}{m^s}\right) \left(\sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}\right) = \sum_{n=1}^{\infty} \sum_{mk=n} \Lambda(m)\chi(m)\chi(k)$$

$$= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \sum_{m|n} \Lambda(m)$$

$$= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \log n$$

$$= -L'(s, \chi).$$

于是引理得证.

下面我们证明 Dirichlet 定理 (定理3.1).

证明. 由引理3.28, 有

$$\sum_{\substack{n=1\\n\equiv a(\mathrm{mod}q)}}^{\infty} \frac{\Lambda(n)}{n^s} = \frac{1}{\varphi(q)} \sum_{\chi(\mathrm{mod}q)} \overline{\chi(a)} \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}$$
$$= -\frac{1}{\varphi(q)} \frac{L'(s,\chi_0)}{L(s,\chi_0)} + \frac{1}{\varphi(q)} \sum_{\chi(\mathrm{mod}q)\atop \chi\neq\chi_0} \overline{\chi(a)}(-1) \frac{L'(s,\chi)}{L(s,\chi)}$$

下只考虑 s 为大于 1 的实数,考虑 $s \to 1^+$. 当 $\chi = \chi_0$ 时有 $\frac{1}{s-1}g(s)$,其中 g(s) 是一个在 1 的邻域内的解析函数且 $g(1) \neq 0$. 则有

$$-\frac{L'(s,\chi_0)}{L(s,\chi_0)} = -\frac{-\frac{1}{(s-1)^2}g(s) + \frac{1}{s-1}g'(s)}{\frac{1}{s-1}g(s)}$$
$$= \frac{1}{s-1} - \frac{g'(s)}{g(s)} \to +\infty \quad (s \to 1^+).$$

而对任意 $\chi \neq \chi_0$,有

$$\frac{L'(s,\chi)}{L(s,\chi)} \to \frac{L'(1,\chi)}{L(1,\chi)} \quad (s \to 1^+).$$

因此

$$\sum_{\substack{n=1\\n\equiv a(\mathrm{mod}q)}}^{\infty} \frac{\Lambda(n)}{n^s} \to +\infty \quad (s \to 1^+).$$

即

$$\sum_{\substack{n=1\\n\equiv a \pmod{a}}}^{\infty} \frac{\Lambda(n)}{n} = +\infty. \tag{6}$$

注意到

$$\sum_{p} \sum_{k>1} \frac{\log p}{p^k} = +\infty$$

而

$$\sum_{p} \sum_{k \le 2} \frac{\log p}{p^k} = \sum_{p} \log p \frac{1}{p(p-1)}$$

$$\le 2 \sum_{p} \frac{\log p}{p^2}$$

$$\le 2 \sum_{p=2}^{\infty} \frac{\log p}{n^2} \le +\infty.$$

且上式对 $p \equiv a(\text{mod}q)$ 求和也是收敛的, 于是由 (6) 可知

$$\sum_{p \equiv a \pmod{q}} \frac{\log p}{p} = +\infty.$$

可知这样的 p 有无穷多个.

算术级数中的素数分布 II

本章证明算术级数中的素数定理.

算术级数中的素数定理 4.1

我们首先引入 $\pi(y;q,a) = \sum_{p \le y} 1$. 其中记号与条件同定理3.1.

定理 4.1 (算术级数中的素数定理). 对 (a,q)=1, 有

$$\pi(y; q, a) \sim \frac{y}{\varphi(q) \log y} \quad (y \to +\infty).$$

我们首先给出同证明素数定理类似的引理.

引理 4.2. 令
$$\psi(y;q,a) = \sum_{p \leq y \atop p \equiv a \pmod{q}} \Lambda(n)$$
. 如果 $\lim_{y \to +\infty} \frac{\psi(y;q,a)}{y/\varphi(q)} = 1$,则定理 4.1.. 成立,即 $\lim_{y \to +\infty} \frac{\pi(y;q,a)}{y/\varphi(q)\log y} = 1$.

成立,即
$$\lim_{y\to +\infty} \frac{\pi(y;q,a)}{y/\varphi(q)\log y} = 1.$$

引理 4.3. 若
$$\int_1^{+\infty} rac{\psi(y;q,a)\varphi(q)-y}{y^2} dy$$
 收敛, 则 $\lim_{y o +\infty} rac{\psi(y;q,a)}{y/\varphi(q)} = 1.$

引理 4.4. $\psi(y;q,a) \leq \psi(y) = O(y)$.

上述引理以及定理的证明同素数定理的证明过程是完全平行的.

引理 4.5. 设
$$\chi \neq \chi_0$$
, $Re(s) = 1$ $(s \neq 1)$, 则 $L(s, \chi) \neq 0$

证明. 首先对于 Re(s) > 1 我们有

$$\begin{split} L(s,\chi) &= \prod_{p\nmid q} (1-\frac{\chi(p)}{p^s})^{-1} \\ &= \exp(\log(\prod_{p\nmid q} (1-\frac{\chi(p)}{p^s})^{-1})) \\ &= \exp(\sum_{p\nmid q} \sum_{m=1}^{\infty} \frac{\chi(p)^m}{mp^{sm}}) \\ &= \exp(\sum_{p\nmid q} \sum_{m=1}^{\infty} \frac{\chi(p)^m e^{-itm\log p}}{mp^{\sigma m}}) \end{split}$$

类似定理2.8, 考虑

$$L(\sigma, \chi_0)^3 L(\sigma + it, \chi)^4 L(\sigma + 2it, \chi^2)^3 = \exp(\sum_{p \nmid g} \sum_{m=1}^{\infty} \frac{3 + 4(\chi(p)e^{-it\log p})^m + (\chi(p)e^{-it\log p})^{2m}}{mp^{\sigma m}})$$

又

$$|L(\sigma, \chi_0)^3 L(\sigma + it, \chi)^4 L(\sigma + 2it, \chi^2)^3| = \exp(\sum_{p \nmid q} \sum_{m=1}^{\infty} \frac{3 + 4\cos\theta + \cos 2\theta}{mp^{\sigma m}}) \ge 1,$$

其中 $(\chi(p)e^{-it\log p})^m = e^{i\theta}, \ \theta = \theta(\chi, t, p, m) \in \mathbb{R}$. 所以当 $\sigma \to 1$ 时

$$|L(\sigma,\chi_0)| \le A \frac{1}{\sigma-1}, \ L(\sigma+2it,\chi) \to L(1+2it,\chi^2),$$

其中 A 是与 σ 无关的常数. 如果 $L(1+it,\chi)=0$, 则当 $\sigma\to 1^+$ 时, $L(\sigma+it,\chi)\le B(\sigma-1)$, 矛盾.

引理 4.6. $\int_1^{+\infty} \frac{\psi(t;q,a)\varphi(q)-t}{y^{2+s}}dt \ (Re(s)>0)$ 可以延拓成 $Re(s)\geq 0$ 上的解析函数.

证明.

Part II

代数理论

5 代数数域和代数整数环

5.1 代数数域

命题 5.1. 设 $\alpha \in \mathbb{Q}$, 若 $\alpha \notin \mathbb{Z}$, 则 α 不是代数整数.

证明. 初等数论.

命题 5.2. 设 f(x) 是 $\alpha \in \mathbb{C}$ 的极小多项式, $f(x) \in \mathbb{Q}[x]$ 是首一多项式. 则 α 是 代数整数当且仅当 $f(x) \in \mathbb{Z}[x]$

证明. 线性代数.

引理 5.3. 设 $\alpha \in \mathbb{C}$, 下列性质等价.

- (1) α 是代数整数;
- (2) 环 $\mathbb{Z}[\alpha]$ 作为加法群是有限生成的;
- (3) 存在环 $R \in \mathbb{C}$ 包含 α 作为加法群是有限生成的;
- (4) 存在有限生成的非零加法群 $A \in \mathbb{C}$ 使得 $\alpha A \subset A$.

证明. $(1) \Rightarrow (2)$. 设 α 在 \mathbb{Q} 上的极小多项式为 $f(x) \in \mathbb{Z}[x]$, 不妨设 $\deg f = n \geq 1$. 不难看出每个 α^m $m \geq 0$ 都能写成 $\alpha, \alpha^2, \ldots, \alpha^{n-1}$ 的 (整系数) 线性组合. 即 $\mathbb{Z}[\alpha]$ 由 $\alpha, \alpha^2, \ldots, \alpha^{n-1}$ 生成.

- $(2) \Rightarrow (3)$ 和 $(3) \Rightarrow (4)$ 是显然的.
- $(4) \Rightarrow (1)$. 由于 A 是有限生成的, 设 $a_1, \ldots, a_n \in A$ 生成 A. 因为 $\alpha A \subset A$, 所以我们有

$$\alpha a_i = \sum_{j=1}^n k_{ij} a_j \quad k_{ij} \in \mathbb{Z}.$$

记 $\mathbf{a} = (a_1, \dots, a_n)^T$, $B = (k_{ij})_{1 \le i, j \le n}$, 于是

$$(\alpha I - B)\boldsymbol{a} = \mathbf{0},$$

其中 I 是单位矩阵. 于是 α 是首一的 n 次多项式 $f(x)=\det(xI-B)\in\mathbb{Z}[x]$ 的根,于是 α 是代数整数.

命题 5.4. 给定代数数域 $K([K:\mathbb{Q}]<\infty)$, 代数整数对加法, 乘法封闭. 更进一步, 记 \mathcal{O}_K 为所有 K 上的代数整数构成的集合, 则 \mathcal{O}_K 是一个环.

证明. 由引理5.3立即可得.

5.2 范, 迹和判别式

定义 5.5. 设 L|K 是数域的扩张, [L:K]=n, 记 σ_1,\ldots,σ_n 是 L 的 n 个 (不同的)K-嵌入. 对 $\alpha \in L$, 定义

$$N_{L|K}(\alpha) = \prod_{i=1}^{n} \sigma_i \alpha,$$
$$T_{L|K}(\alpha) = \sum_{i=1}^{n} \sigma_i \alpha.$$

分别称为 α 关于扩张 L|K 的范与迹.

命题 5.6. (1) 对 $\alpha, \beta \in L$,

$$N_{L|K}(\alpha\beta) = N_{L|K}(\alpha)N_{L|K}(\beta),$$

$$T_{L|K}(\alpha+\beta) = T_{L|K}(\alpha) + T_{L|K}(\beta).$$

- (2) $\alpha \in K$, $N_{L|K}(\alpha) = \alpha^n$, $T_{L|K}(\alpha) = n\alpha$.
- (3) $\alpha \in L, k \in K, T_{L|K}(k\alpha) = kT_{L|K}(\alpha)$

定理 5.7. 设 $n = [L:K], \alpha \in L,$ 设 α 在 K 上的极小多项式为

$$f(x) = x^m + c_{m-1}x^{m-1} + \dots + c_1x + c_0$$

则

$$N_{L|K}(\alpha) = (-1)^n c_0^{\frac{n}{m}}, \ T_{L|K}(\alpha) = -\frac{n}{m} c_{m-1}.$$

证明. n = m 时显然.

设 $\alpha_1, \ldots, \alpha_m$ 是 f(x) 的 m 个根, 因此

$$N_{K(\alpha)|K}(\alpha) = (-1)^m c_0$$

$$T_{K(\alpha)|K}(\alpha) = -c_{m-1}$$

我们有 m 个 K-嵌入 τ_1, \ldots, τ_m , 且每个 τ_i 都能扩张成 $[L:K(\alpha)] = \frac{n}{m}$ 个嵌入 $\tau_{i,j_1 \leq j \leq \frac{n}{m}} \cdot \tau_{i,j_1 \leq i \leq m,1 \leq j \leq \frac{n}{m}}$ 是 L 上 n 个不同的 K-嵌入. 于是

$$N_{L|K}(\alpha) = \prod_{i} \prod_{j} \tau_{i,j} = \prod_{i} \tau_{i}(\alpha)^{\frac{n}{m}}$$

$$= (N_{K(\alpha)|K}(\alpha))^{\frac{n}{m}}$$

$$= ((-1)^{m} c_{0})^{\frac{n}{m}} = (-1)^{n} c_{0}^{\frac{n}{m}}.$$

类似地有 $T_{L|K}(\alpha) = -\frac{n}{m}c_{m-1}$.

注. 由此不难看出 $N_{L|K}(\alpha)$, $T_{L|K}(\alpha) \in K$.

定理 5.8. 对于有限的数域扩张 $K \subset M \subset L$, 有

$$N_{L|K}(\alpha) = N_{M|K}(N_{L|M}(\alpha)), T_{L|K}(\alpha) = T_{M|K}(T_{L|M}(\alpha)).$$

证明. 我们给一个对可分的有限域扩张都成立的证明, 事实上有限的数域扩张都是可分扩张.

固定 K 的一个代数闭包 \bar{K} , 记 $\mathrm{Hom}_K(L,\bar{K})$ 为 K-嵌入构成的集合, 它被等价关系

$$\sigma \sim \tau \iff \sigma|_M = \tau|_M$$

划分为 m := [M:K] 个等价类, 记 $\sigma_1, \ldots, \sigma_m$ 是一组代表元, 于是 $\operatorname{Hom}_K(M, \overline{K}) = \{\sigma_1|_M, \ldots, \sigma_m|_M\}$. 则

$$T_{L|K}(\alpha) = \sum_{i=1}^{m} \sum_{\sigma \sim \sigma_i} \sigma(\alpha) = \sum_{i=1}^{m} T_{\sigma(L)|\sigma(M)}(\sigma_i(\alpha))$$
$$= \sum_{i=1}^{m} \sigma_i T_{L|M}(\alpha)$$
$$= T_{M|K}(T_{L|M}(\alpha)).$$

范的情形是类似的.

注. 这个定理对不可分的域扩张也对, 证明可以参考 [8].

定义 5.9. 设 L|K 是 n 次扩张, $\sigma_1, \ldots, \sigma_n$ 是 L 上的 n 个 K-嵌入. 定义 $\alpha_1, \ldots \alpha_n \in L$ 对于扩张 L|K 的判别式为

$$d_{L|K}(\alpha_1, \dots \alpha_n) := \det(\sigma_i(\alpha_i))^2.$$

注. 判别式与 $\sigma_1, \ldots \sigma_n$ 的顺序无关.

定理 5.10. $d_{L|K}(\alpha_1, \ldots, \alpha_n) = \det(T_{L|K}(\alpha_i, \alpha_i))$.

证明. 把判别式定义展开即知.

定理 5.11. $d_{L|K}(\alpha_1, \ldots \alpha_n) \neq 0 \Leftrightarrow \alpha_1, \ldots \alpha_n$ 是 K-线性无关的.

证明. (⇒) 用反证法. 设 $\alpha_1, \ldots \alpha_n$ 是 K-线性相关的, 即存在不全为 0 的 $k_1, \ldots k_n \in K$ s.t. $k_1\alpha_1 + \cdots k_n\alpha_n = 0$. 于是对任意 $1 \le i \le n$,

$$0 = \sigma_i(k_1\alpha_1 + \dots + k_n\alpha_n) = \sigma_i(k_1)\sigma_i(\alpha_1) + \dots + \sigma_i(k_n)\sigma_i(\alpha_n)$$
$$= k_1\sigma_i(\alpha_1) + \dots + k_n\sigma_i(\alpha_n)$$

其中 σ_i $1 \le i \le n$ 是 n 个不同的 K-嵌入. 于是

$$\mathbf{0} = k_1 \begin{pmatrix} \sigma_1(\alpha_1) \\ \vdots \\ \sigma_n(\alpha_n) \end{pmatrix} + \dots + k_n \begin{pmatrix} \sigma_1(\alpha_1) \\ \vdots \\ \sigma_n(\alpha_n) \end{pmatrix}$$

因此 $d_{L|K}(\alpha_1, \ldots \alpha_n) = 0$, 与假设矛盾.

(\Leftarrow) 同样用反证法. 设 $d_{L|K}(\alpha_1, \dots \alpha_n) = 0$. 记 $v_i = (T_{L|K}(\alpha_i \alpha_1), \dots, T_{L|K}(\alpha_i \alpha_n))$. 不难看出 v_i 是 K-线性相关的. 于是有不全为零的 $k_1, \dots, k_n \in K$ 使得

$$k_1v_1+\cdots+k_nv_n=\mathbf{0}.$$

令 $\alpha = k_1\alpha_1 + \dots + k_n\alpha_n \neq 0$ 但向量 $k_1v_1 + \dots + k_nv_n$ 的第 j 个元素 $T_{L|K}(\alpha\alpha_j) = 0$. 考虑 α^{-1} , 它可以写成

$$\alpha^{-1} = k_1' \alpha_1 + \dots + k_n' \alpha_n.$$

于是 $T_{L|K}(\alpha\alpha^{-1}) = 0 = T_{L|K}(1)(=n)$, 矛盾.

定理 5.12. 设 $L = K(\alpha)$, [L:K] = n, α 在 K 上的极小多项式记为 $f(x) \in K[x]$, $\alpha(=\alpha_1), \ldots, \alpha_n$ 是 f(x) 的 n 个不同的根. 则

$$d_{L|K}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)^2$$
$$= (-1)^{\frac{n(n-1)}{2}} N_{L|K}(f'(\alpha))$$

证明. 不妨设 $n \ge 2$. n 个不同的 $L \perp K$ -嵌入 $\sigma_1, \ldots, \sigma_n$ 满足

$$\sigma_i(\alpha) = \alpha_i$$
.

则

$$d_{L|K}(1, \alpha, \dots, \alpha^{n-1}) = \det((\sigma_i(\alpha^j))_{1 \le i, j \le n})^2$$

$$= \det((\alpha_i^j)_{1 \le i, j \le n})^2$$

$$= \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)^2$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i) \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{\substack{j=1 \ j \ne i}}^{n} (\alpha_i - \alpha_j)$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i)$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\sigma_i(\alpha))$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \sigma_i(f'(\alpha))$$

$$= (-1)^{\frac{n(n-1)}{2}} N_{L|K}(f'(\alpha))$$

定义 5.13. $\alpha \in L$, 令 $d_{L|K}(\alpha) = d_{L|K}(1, \alpha, \dots, \alpha^{n-1})$, 称为 α 对扩张 L|K 的判别式.

例 5.14. 考虑分圆域 $L=\mathbb{Q}(\omega)$, $\omega=e^{2\pi i/p^m}$, 其中 p 是奇素数, $m\in\mathbb{Z}^+$. 我们知道 ω 的极小多项式为

$$f(x) = \Phi_{p^m}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1}$$
$$= x^{p^{m-1}(p-1)} + x^{p^{m-1}(p-2)} + \dots + x^{p^{m-1}} + 1.$$

多项式的次数为 $\deg f = \varphi(p^m) = p^{m-1}(p-1) =: d$. 我们有

$$p^{m-1}x^{p^{m-1}-1}f(x) + (x^{p^{m-1}-1} - 1)f'(x) = p^m x^{p^{m-1}-1}.$$

可知

$$N_{L|\mathbb{Q}}(f'(\omega)) = N_{L|\mathbb{Q}}(\frac{p^m}{w(w^{p^{m-1}})} - 1).$$

而我们有

$$N_{L|\mathbb{Q}}(p^m) = (p^m)^d$$
$$N_{L|\mathbb{Q}}(\omega) = (-1)^d$$

只需考虑

$$N_{L|\mathbb{Q}}(\omega^{p^{m-1}} - 1) = N_{L|\mathbb{Q}}(e^{2\pi i/p^m} - 1) = (-1)^d p^{d/(p-1)}.$$

整理得

$$d_{L|\mathbb{Q}}(\omega) = (-1)^{\frac{d(d-1)}{2}} p^{p^{m-1}(mp-m-1)}.$$

5.3 代数整数环

引理 5.15. 对代数数 α , 存在非零 $n \in \mathbb{Z}$, 使得 $n\alpha$ 是代数整数.

证明. 记 α 的极小多项式为

$$f(x) = a_n x^n + \dots + a_1 x + a_0.$$

于是

$$a_n^{n-1}f(x) = (a_nx)^n + \dots + a_1a_n^{n-1}(a_nx) + a_0a_n^{n-1}.$$

因此我们有首一整系数多项式

$$g(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1a_n^{n-1}x + a_0a_n^{n-1}$$

满足 $g(a_n\alpha) = 0$, 因此 $a_n\alpha$ 是代数整数.

我们首先考虑二次域的代数整数环.

定理 5.16. 设 $K = \mathbb{Q}(\sqrt{d}), d \neq 1$ 是无平方因子整数,则

(1) 当 $d \equiv 2, 3 \pmod{4}$ 时,

$$\mathcal{O}_K = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \},\$$

(2) 当 $d \equiv 1 \pmod{4}$ 时,

$$\mathcal{O}_K = \{ a + b \frac{1 + \sqrt{d}}{2} \mid a, b \in \mathbb{Z} \},$$

证明. 设 $\alpha + \beta \sqrt{d} \in \mathcal{O}_K \ (\beta \neq 0)$, 其极小多项式为

$$(x - \alpha - \beta\sqrt{d})(x - \alpha + \beta\sqrt{d}) = x^2 - 2\alpha x + \alpha^2 - \beta^2 d.$$

 $\alpha + \beta \sqrt{d}$ 是代数整数当且仅当 $2\alpha, \alpha^2 - \beta^2 d \in \mathbb{Z}$. 因此 $(2\alpha)^2 - (2\beta)^2 d \in 4\mathbb{Z}$. 特别地 $(2\beta)^2 d \in \mathbb{Z}$, 而由于 d 无平方因子, 可知 $2\beta \in \mathbb{Z}$. 且由 $(2\alpha)^2 \equiv (2\beta)^2 d \pmod{4}$ 可知 $2\alpha, 2\beta$ 奇偶性相同.

当 $d \equiv 2,3 \pmod{4}$ 时, 若 $2\alpha,2\beta$ 都是偶数, 则 $\alpha,\beta \in \mathbb{Z}$. 若 $2\alpha,2\beta$ 都是奇数, 则

$$(2\alpha)^2 \equiv 1 \pmod{4},$$
$$(2\beta)^2 d \equiv 2, 3 \pmod{4}.$$

矛盾.

当 $d\equiv 1\pmod 4$ 时, 若 $2\alpha,2\beta$ 都是偶数, 则 $\alpha,\beta\in\mathbb{Z}$. 取 $a=\alpha-\beta,b=2\beta$, 则 $\alpha+\beta\sqrt{d}=a+b\frac{1+\sqrt{d}}{2}$. 若 $2\alpha,2\beta$ 都是奇数, 则 $\alpha-\beta\in\mathbb{Z}$, 有

$$\alpha + \beta \sqrt{d} = (\alpha - \beta) + 2\beta \frac{1 + \sqrt{d}}{2}.$$

其中 $\alpha - \beta, 2\beta \in \mathbb{Z}$.

接下来我们考虑分圆域 $\mathbb{Q}(e^{2\pi i/m})$ 的代数整数环. 我们先考虑 $m=p^n$ 的简单情况.

定理 5.17. 设 $K = \mathbb{Q}(\zeta_{p^n})$, 其中 $\zeta_m = e^{2\pi i/p^n}$, p 是素数, $n \in \mathbb{Z}^+$, 则 $\mathcal{O}_K = \mathbb{Z}[e^{2\pi i/p^n}]$

证明. 记 $\omega = (\zeta_{p^n}), s = \varphi(p^n) = [K : \mathbb{Q}].$ 显然有 $\mathbb{Z}[\omega] \subset \mathcal{O}_K$, 只需证反方向的包含. 注意到 K 作为 \mathbb{Q} -向量空间有一组基 $1, \omega, \ldots, \omega^{s-1}$, 因此任意 $\alpha \in \mathcal{O}_K$, 有

$$\alpha = t_0 + t_1 \omega + \dots + t_{s-1} \omega^{s-1},$$

其中 $t_0, \ldots, t_{s-1} \in \mathbb{Q}$. 下证 $t_0, \ldots, t_{s-1} \in \mathbb{Z}$.

记 $Gal(K|\mathbb{Q}) = \{\tau_1, \ldots, \tau_s\}$. 我们有

$$\tau_i(\alpha) = t_0 + t_1 \tau_i(\omega) + \dots + t_{s-1} \tau_i(\omega^{s-1}) \ (1 \le i \le s).$$

这给出了由 s 个方程组成的线性方程组, 于是由 Cramer 法则, 可以解出

$$t_i = \frac{\gamma_j}{\delta},$$

其中 $\delta = \det(\tau_i(\omega^k)_{\substack{1 \le i \le s \\ 0 \le k \le s-1}})$, γ_j 是根据 Cramer 法则替换 $(\tau_i(\omega^k)_{\substack{1 \le i \le s \\ 0 \le k \le s-1}})$ 第 j 列 后的新方阵的行列式. 由于所有 $\tau_i(\omega^k)$ 和 $\tau_i(\alpha)$ 都是代数整数, γ_j , δ 也都是代数整数. 且

$$\delta^2 = d_K(1, \omega, \dots, \omega^{s-1}) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

从而

$$t_j d = \delta \gamma_j \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

记 $t_j d = m_j$, 我们有

$$\alpha = \frac{m_0}{d} + \frac{m_1}{d}\omega + \dots + \frac{m_{s-1}}{d}\omega^{s-1}$$

上式可变换为

$$\alpha = \frac{m_0'}{d} + \frac{m_1'}{d}(1 - \omega) + \dots + \frac{m_{s-1}'}{d}(1 - \omega)^{s-1},\tag{7}$$

我们想证 $d|m_j$ $(0 \le j \le s-1)$,这等价于证 $d|m'_j$ $(0 \le j \le s-1)$. 用反证法,已经知道 d 可以写成 $d = \pm p^l$ $(l \in \mathbb{Z}^+)$,假设 $(m'_0, \ldots, m'_{s-1}) = p^{\lambda}m'$,其中 $\lambda \le l-1, p \nmid m'$.记 $m'_j = p^{\lambda}m''_j$ $(m''_j \in \mathbb{Z})$,则 $p \nmid (m''_0, \ldots, m''_{s-1}) = m'$.我们有

$$\alpha = \frac{p^{\lambda}}{p^{l}}(m_{0}'' + m_{1}''(1 - \omega) + \dots + m_{s-1}''(1 - \omega)^{s-1})$$

于是

$$p^{l-\lambda-1}\alpha = \frac{1}{p}(m_0'' + m_1''(1-\omega) + \dots + m_{s-1}''(1-\omega)^{s-1})$$

不妨设 $p|m_i''(0 \le j \le t-1)$ 但 $p \nmid m_i''(0 \le t \le s-1)$. 于是

$$p^{l-\lambda-1}\alpha - \frac{1}{p}(m_0'' + m_1''(1-\omega) + \dots + m_{t-1}''(1-\omega)^{t-1})$$

$$= \frac{m_t''(1-\omega)^t}{p} + \dots + \frac{m_{s-1}''(1-\omega)^{s-1}}{p}$$

上式等号左边是代数整数,于是等号右边也是代数整数,记为 α' .上式化为

$$\frac{\alpha' p}{(1-\omega)^{1+t}} = \frac{m''_t}{(1-\omega)} + m''_{t+1} + \dots + m''_{s-1} (1-\omega)^{s-t-2}$$

我们有

$$N_{K|\mathbb{Q}}(1-\omega) = \prod_{\substack{k=1\\(k,p)=1}}^{m=p^n} (1-\omega^k) = p$$

由此可知 $\frac{p}{(1-\omega)^{1+t}} \in \mathbb{Z}[\omega] \subset \mathcal{O}_K$, 于是 $\frac{\alpha'p}{(1-\omega)^{1+t}} \in \mathcal{O}_K$. 从而有 $\frac{m''_t}{1-\omega} \in \mathcal{O}_K$. 于是

$$N_{K|\mathbb{Q}}(\frac{m_t''}{1-\omega}) = \frac{(m_t'')^s}{p} \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

这同 $p \nmid m_t''$ 矛盾, 从而 $p^l | m_j' \ (0 \le j \le s - 1)$.

为了计算一般的分圆域的代数整数环, 我们需要做一些准备工作.

定理 5.18. 设 $[K:\mathbb{Q}]=n$, 则 \mathcal{O}_K 是秩为 n 的自由 Abel 群.

证明. 设 $\alpha_1, \ldots, \alpha_n$ 是 K 作为 \mathbb{Q} -向量空间的一组基, 由引理5.15, 不妨设 $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. 对任意 $\gamma \in \mathcal{O}_K$,

$$\gamma = x_1 \alpha_1 + \dots + x_n \alpha_n,$$

其中 $x_1, \ldots, x_n \in \mathbb{Q}$. 记 $\sigma_1, \ldots, \sigma_n$ 是 $n \uparrow K$ 上的 \mathbb{Q} -嵌入, 则

$$\sigma_i(\gamma) = x_1 \sigma_i(\alpha_1) + \dots + x_n \sigma_i(\alpha_n).$$

类似定理5.17可以解得 $x_i = \frac{\gamma_i}{\delta}$, 其中 $\delta = \det(\sigma_i(\alpha_i))$, 且

$$\delta^2 = d = d_{K|\mathbb{Q}}(\alpha_1, \dots, \alpha_n) \in \mathbb{Q} \cap \mathcal{O}_K,$$

于是 d 是非零整数. 从而

$$x_j d = \gamma_j \delta =: m_j \in \mathbb{Z}.$$

因此

$$\mathcal{O}_K \subset \mathbb{Z} \frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z} \frac{\alpha_n}{d}$$
.

由定理A.6可知 \mathcal{O}_K 是秩不大于 n 的自由 Abel 群. 若 \mathcal{O}_K 由 β_1, β_m 整系数 线性生成,则 K 由 β_1, β_m 有理系数线性生成,从而 $m \geq n$,因此 m = n. 即 $\mathrm{rank}(\mathcal{O}_K) = n$.

定义 5.19. 设 $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$. 如果 $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$, 则称 $\omega_1, \ldots, \omega_n$ 是 \mathcal{O}_K 或 K 的一组整基.

不难看出整基不是唯一的. 事实上, 如果 $\omega_1, \ldots, \omega_n$ 是 \mathcal{O}_K 的整基, 那么 $-\omega_1, \ldots, \omega_n$ 和 $\omega_1, \ldots, \omega_{n-1}, \omega_1 + \omega_n$ 也都是 \mathcal{O}_K 的整基.

引理 5.20. 设 $[K:\mathbb{Q}]=n, \omega_1,\ldots,\omega_n$ 是 \mathcal{O}_K 的一组整基. 设 $\alpha_1,\ldots,\alpha_n\in\mathcal{O}_K$, 若有

$$(\alpha_1, \dots, \alpha_n)^T = A(\omega_1, \dots, \omega_n)^T$$

其中 $A \in \operatorname{Mat}_n(\mathbb{Z})$, 则

$$d_K(\alpha_1,\ldots,\alpha_n) = \det(A)^2 d_K(\omega_1,\ldots,\omega_n)$$

证明. 记 $A = (a_{ij})_{1 \leq i,j \leq n}$,则 $\alpha_i = \sum_{i=1}^n a_{ij}\omega_j$. 我们有

$$(\sigma_i(\alpha_j)) = (\sigma_i(\sum_{k=1}^n a_{j,k}\omega_k))$$
$$= (\sum_{k=1}^n a_{j,k}\sigma_i(\omega_k))$$
$$= (\sigma_i(\omega_k))A^T.$$

于是
$$d_K(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = \det(A)^2 d_K(\omega_1, \dots, \omega_n),$$

推论 5.21. 设 $[K:\mathbb{Q}]=n, \omega_1,\ldots,\omega_n$ 和 α_1,\ldots,α_n 是 \mathcal{O}_K 的两组整基. 则

$$d_K(\alpha_1,\ldots,\alpha_n)=d_K(\omega_1,\ldots,\omega_n)$$

证明. 两组整基的变换矩阵 A, B 满足 $AB = I_n$, 于是 $\det(A)\det(B) = 1$. 又 $A, B \in \operatorname{Mat}_n(\mathbb{Z})$, 因此 $\det(A), \det(B) \in \mathbb{Z}$. 于是 $\det(A)^2 = 1$.

定义 5.22. K 的判别式 d(K) (有时记作 d_K) 是它任意一组整基的判别式.

引理 5.23. 设 $\alpha_1,\ldots,\alpha_n\in\mathcal{O}_K$. 若

- (1) $d_K(\alpha_1,\ldots,\alpha_n)=d(K)$, $\not \equiv$
- (2) $d_K(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ 是无平方因子的非零整数.

则 $\alpha_1, \ldots, \alpha_n$ 是 K 的一组整基.

证明. 设 $\omega_1, \ldots, \omega_n$ 是一组整基. 我们有

$$(\alpha_1,\ldots,\alpha_n)^T=A(\omega_1,\ldots,\omega_n)^T,$$

其中 $A \in \operatorname{Mat}_n(\mathbb{Z})$. 则

$$d_K(\alpha_1,\ldots,\alpha_n) = \det(A)^2 d(K).$$

由 (1), $\det(A)^2 = 1$, 则 $A^{-1} \in \operatorname{Mat}_n(\mathbb{Z})$, 故 $\alpha_1, \ldots, \alpha_n$ 是 K 的一组整基.

由 (2) 同样有
$$\det(A)^2 = 1$$
.

定理 5.24. 设 K, L 是数域, 若 $[K:\mathbb{Q}] = m, [L:\mathbb{Q}] = n$ 且 $[KL:\mathbb{Q}] = mn$, 并且 (d(K), d(L)) = 1, 则

- (1) $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L := \{ \sum_{i=1}^t \alpha_i' \beta_i' \mid \alpha_i' \in \mathcal{O}_K, \beta_i' \in \mathcal{O}_L, t \in \mathbb{Z}^+ \},$
- (2) 若 $\alpha_1, \ldots, \alpha_m$ 和 β_1, \ldots, β_n 分别是 K, L 的整基,则 $\{\alpha_i \beta_j \mid 1 \le i \le m, 1 \le j \le n\}$ 是 KL 的一组整基.
- (3) $d(KL) = d(K)^n d(K)^m$.

证明. 对于 (1), $\mathcal{O}_K\mathcal{O}_L \subset \mathcal{O}_{KL}$ 是显然的, 而由 (2) 立即可得 $\mathcal{O}_{KL} \subset \mathcal{O}_K\mathcal{O}_L$.

下证 (2). 首先 $\{\alpha_i\beta_j\}_{1\leq i\leq m\atop 1\leq j\leq n}$ 是 KL 作为作为 $\mathbb Q$ -向量空间的一组基, 于是任意 $\alpha\in\mathcal O_K$ 都能写成

$$\alpha = \sum_{i,j} \frac{r_{ij}}{r} \alpha_i \beta_j,$$

其中 $r_{ij} \in \mathbb{Z}$, $r \in \mathbb{Z}^+$ 且 $(r, r_{11}, \dots, r_{mn}) = 1$. 令 σ_k 是 K 的 m 个不同的 \mathbb{Q} -嵌入. 我们可以把 σ_k 扩张到 KL 上,且有 $[KL:K] = \frac{[KL:\mathbb{Q}]}{[K:\mathbb{Q}]} = \frac{mn}{m} = n$ 种扩张的方式. 记它们为 $\sigma_k^{(1)}, \dots, \sigma_k^{(n)}$. 这 n 个嵌入中一定有一个嵌入 $\tilde{\sigma}_k$ 使得 $\tilde{\sigma}_k|_L = \mathrm{id}_L$. 于是

$$\widetilde{\sigma_k}(\alpha) = \sum_{i,j} \frac{r_{ij}}{r} \sigma_k(\alpha_i) \beta_j$$
$$= \sum_{i=1}^m x_i \sigma_k(\alpha_i)$$

其中 $x_i = \sum_{j=1}^n \frac{r_{ij}}{r} \beta_j \in L$. 仍然是利用 Cramer 法则, 记 $\delta = \det(\sigma_k(\alpha_i))$, 可以解得

$$x_i = \frac{\gamma_i}{\delta},$$

其中 γ_i 是替换相应列后的行列式,且 $\delta^2 = d_K(\alpha_1, \ldots, \alpha_m) = d(K) \in \mathbb{Z}$. 于是 $x_i d(K) = \delta \gamma_i \in \mathcal{O}_L$. 因此

$$\sum_{i=1}^{n} \frac{r_{ij}}{r} d(K)\beta_j \in \mathcal{O}_L.$$

所以 $\frac{r_{ij}}{r}d(K) \in \mathbb{Z}$, 故而 r|d(K). 同理, r|d(L). 而 (d(K),d(L))=1, 所以 r=1. 这就证明了 (2).

下证 (3). 设 $\{\sigma_k\}_{1\leq k\leq m}$ 是 K 上的 m 个 \mathbb{Q} -嵌入, $\{\tau_l\}_{1\leq l\leq n}$ 是 L 上的 n 个 \mathbb{Q} -嵌入. 前面已经证明了对于每一对 (σ_k,τ_l) 都存在唯一的 KL 上的 \mathbb{Q} -嵌入 $\pi_{k,l}$ 满足

$$\pi_{k,l}|_K = \sigma_k, \pi_{k,l}|_L = \tau_l.$$

于是 $\{\pi_{k,l}\}_{1 \le k \le m \atop 1 \le l \le n}$ 就是 KL 上全部的 mn 个 \mathbb{Q} -嵌入. 因此

$$d(KL) = \det(\pi_{k,l}(\alpha_i\beta_j))^2$$

$$= \det(\pi_{k,l}(\alpha_i)\pi_{k,l}(\beta_j))^2$$

$$= \det((\sigma_k(\alpha_i)) \otimes (\tau_l(\beta_j)))^2$$

$$= d(K)^n d(L)^m$$

其中 $(\sigma_k(\alpha_i)) \otimes (\tau_l(\beta_i))$ 是两个矩阵的 Kronecker 乘积.

定理 5.25. 设 $K=\mathbb{Q}(\zeta_m)$, 其中 $\zeta_m=e^{2\pi i/m},\ m\in\mathbb{Z}_{\geq 3}$ 且 $m\not\equiv 2\ (\mathrm{mod}\ 4)$, 则

 $(1) \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[e^{2\pi i/m}],$

(2)
$$d(K) = \frac{(-1)^{\frac{\varphi(m)}{2}} m^{\varphi(m)}}{\prod_{p|m} p^{\varphi(m)/(p-1)}}.$$

证明. 设 $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. 先证 r=2 的情形. 记

$$K_1 = \mathbb{Q}(e^{2\pi i/p_1^{n\alpha_1}}), K_2 = \mathbb{Q}(e^{2\pi i/p_2^{n\alpha_2}}).$$

则 $K = K_1K_2$

由定理5.24有

$$\mathcal{O}_{K} = \mathcal{O}_{K_{1}} \mathcal{O}_{K_{2}}$$

$$= \mathbb{Z}(e^{2\pi i/p_{1}^{\alpha_{1}}}) \mathbb{Z}(e^{2\pi i/p_{2}^{\alpha_{2}}})$$

$$= \mathbb{Z}(e^{2\pi i/(p_{1}^{\alpha_{1}}p_{2}^{\alpha_{2}}})).$$

以及

$$\begin{split} d(K) &= d(K_1)^{\varphi(p_2^{\alpha_2})} d_{K_2}^{\varphi(p_1^{\alpha_1})} \\ &= \frac{(-1)^{\frac{\varphi(m)}{2}} m^{\varphi(m)}}{\prod_{p|m} p^{\varphi(m)/(p-1)}}. \end{split}$$

一般情况由数学归纳法即得.

注. 如果定理 5.25 中的条件 $m \not\equiv 2 \pmod{4}$ 不再成立, 即若 $m \equiv 2 \pmod{4}$, 有

$$\mathbb{Q}(e^{2\pi i/m}) = \mathbb{Q}(e^{2\pi i/m'}),$$

其中 $m' = \frac{m}{2}$.

5.4 单位根

本节考虑的数域 K 都是有限扩张, 即 $[K:\mathbb{Q}] \leq \infty$.

定义 5.26. 设 K 为数域. 我们称 $u \in K$ 是 n 次单位根如果存在 $n \in \mathbb{Z}^+$ 使得 $u^n = 1$

记 W_K 为K中所有单位根构成的群.

命题 5.27. W_K 是有限群.

证明. 如果 W_K 是无限群, 则对任意 $n \in \mathbb{Z}^+$, 都存在 $m \ge n$ 使得 W_K 中含有 m 次本原单位根, 记为 ζ_m . 我们有 K

$$[K:\mathbb{Q}] \ge \varphi(m) \ge \frac{1}{2}\sqrt{m} \to \infty.$$

下面我们给一个稍显复杂但典范的处理.

证明. 设 $w \in W_K$ 是 n 次单位根. 设 $f(x) = x^m + c_{m-1} + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ 是 w 的极小多项式. 记 f 所有的根为 $w_1 = w, w_2, \ldots, w_m$. 于是 $f(x)|x^n - 1$, 因此 $w_j^n = 1$ $(1 \le j \le m)$. 于是 $|w_j| = 1$. 由根与系数关系可知 $|c_{m-j}| \le {m \choose j}$. 又 WK中元素的 \mathbb{Z} 上极小多项式次数比 n 小且系数的绝对值比 2^n 小,满足这些条件的首一整系数多项式只有有限个,因此 W_K 元素有限.

命题 5.28. W_K 是有限循环群.

证明. 设 $|W_k| = n$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. 由于 W_K 是有限 Abel 群, 我们有

$$W_K = G_1 \oplus \cdots G_r$$
.

其中 G_j 是 $p_j^{\alpha_j}$ 阶子群. 故只需证 G_j 是循环群. 如果不是,则 $G_j = \bigoplus_i H_{j,i}$, 其中 $|H_{j,i}| \leq p_j^{\alpha_j-1}$ 且是循环群. 而任意 $w \in G_j$ 都满足 $w^{p_j^{\alpha_j-1}} = 1$,则多项式 $x^{p_j^{\alpha_j-1}} = 1$ 的根至少有 $|G_j| = p_j^{\alpha_j}$ 个,矛盾.

定义 5.29. 设 $u \in \mathcal{O}_K$ 且 $u^{-1} \in \mathcal{O}_K$, 则称 $u \notin \mathcal{O}_K$ 中的单位.

 $\dot{\mathbf{L}}$. 不难看出单位群即 \mathcal{O}_K 中可逆元全体 \mathcal{O}_K^{\times} .

引理 5.30. 设 $[K:\mathbb{Q}]=n$, 设 σ_1,\cdots,σ_n 是 n 个嵌入, $u\in\mathcal{O}_K$. 则有

- $(1) \ u \in \mathcal{O}_K^{\times} \iff N_{K|\mathbb{Q}}(u) = \pm 1,$
- (2) $u \in W_K \iff |\sigma_i(u)| = 1 \ (1 \le i \le n)$

证明. (1) (⇒) 设 u 是单位,则 $N_{K|\mathbb{Q}}(u)N_{K|\mathbb{Q}}(u^{-1}) = 1$. 而 $u, u^{-1} \in \mathcal{O}_K$,故 $N_{K|\mathbb{Q}}(u), N_{K|\mathbb{Q}}(u^{-1}) \in \mathbb{Z}$. 因此 $N_{K|\mathbb{Q}}(u) = \pm 1$.

(⇐) 设 $N_{K|\mathbb{Q}}(u) = \pm 1$. 考虑多项式

$$f(x) = \prod_{i=1}^{n} (x - \sigma_i(u)) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x].$$

可知 u^{-1} 是首一整系数多项式

$$a_0 + a_0 a_{n-1} x + \dots + a_0 a_1 x^{n-1} + a_0$$

的根. 所以 $U^{-1} \in \mathcal{O}_K$.

(2) (\Rightarrow) 设 $u \in W_K$, 于是存在 m 使得 $u^m = 1$. 则

$$\sigma_i(u)^m = \sigma_i(u^m) = 1.$$

于是 $\sigma_i(u)$ 是单位根, 自然有 $|\sigma_i(u)| = 1$.

(\Leftarrow) 用反证法. 设 $|\sigma_i(u)|=1$, 但 u 不是单位根, 于是 $\{u^j\}_{j\geq 1}$ 两两不同. 显然 u^j 是多项式

$$f(x) = \prod_{i=1}^{n} (x - \sigma_i(u^j)) \in \mathbb{Z}[x]$$

的根. 故由根与系数的关系, x^{n-k} 项的系数比 $\binom{n}{k}$ 小, 故 f_j 的系数的绝对值比 2^n 小. 于是 f_j 只有有限个, 矛盾.

那么模长为1的单位是否一定是单位根呢?下面的例子给出了否定的回答.

例 5.31. 考虑多项式 $x^4 - 2x^3 - 2x - 1$, 我们有如下因式分解

$$x^4 - 2x^3 - 2x - 1 = (x^2 - x + 1 + \sqrt{3}x)(x^2 - x + 1 - \sqrt{3}x).$$

这个方程有四个根,包括两个共轭的复根 u, \bar{u} 满足 $|u| = u\bar{u} = 1$ 和两个实根 u_1, u_2 满足 $u_1u_2 = 1$. 如果 u 是单位根,则 $|u_1| = |u_2| = 1$. 这使得 $u_1.u_2 = \pm 1$,矛盾. 所以 u 不是单位根.

6 素理想分解

6.1 Dedekind 整环

定义 6.1. 设 R 是整环, 如果 R 满足: 若 $a \in \operatorname{Frac}(R)$ 是 R[x] 中首一多项式的 R 则 $a \in R$,则称 R 是整闭的.

定义 6.2. 若整环 R 是整闭的 Noether 环, 且任意非零素理想都是极大理想,则称其为 Dedekind 整环.

引理 6.3. 设 R 是 Noether 整环, $I \subset R$ 是非零理想, 则存在 R 的有限个素理想 $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ 使得 $I \supset \mathfrak{p}_1 \ldots \mathfrak{p}_n$.

证明. 用反证法. 假设存在非平凡理想 I 使得 R 不具备上述性质, 记这些理想构成的集合为 S. 由于 R 是 Noether 的, 于是 S 中存在极大元, 记为 M. 易见 M 不是素理想, 于是存在 $x,y \in R-M$ 满足 $xy \in M$. 于是 $M \subsetneq M+Rx \notin S$, $M \subsetneq M+Ry \notin S$. 于是存在素理想 $\mathfrak{p}_1,\ldots,\mathfrak{p}_n,\mathfrak{q}_1,\ldots,\mathfrak{q}_m$ 使得 $M+Rx \supset \mathfrak{p}_1,\ldots,\mathfrak{p}_n,M+Ry \supset \mathfrak{q}_1,\ldots,\mathfrak{q}_m$. 从而有

$$M \supset (M + Rx)(M + Ry) \supset \mathfrak{p}_1 \dots \mathfrak{p}_n \mathfrak{q}_1 \dots \mathfrak{q}_m$$

这同 $M \in S$ 矛盾, 于是 $S = \emptyset$.

引理 6.4. 设 R 是 Dedekind 整环, $A \subsetneq R$ 是 R 的理想, $K = \operatorname{Frac}(R)$, 则存在 $\gamma \in K$ 且 $\gamma \notin R$ 使得 $\gamma A \subset R$.

证明. 不妨设 $A \neq 0$. 取 $0 \neq a \in A$. 设 r 是最小的正整数使得存在素理想 $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ 满足 $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset (a)$. 故存在极大理想 \mathfrak{m} 使得

$$\mathfrak{m} \supset A \supset (a) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$$
.

于是存在 i 使得 $\mathfrak{p}_i \subset \mathfrak{m}$, 不妨 i=1. 于是 $\mathfrak{m}=\mathfrak{p}_1$. 又由 r 的最小性, 有 $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ 但 $b \notin (a)$. 则

$$bA \subset b\mathfrak{m} = b\mathfrak{p}_1 \subset \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset aR.$$

引理 6.5. 设 R 是 Dedekind 整环, I 是 R 的理想. 则存在 R 的非零理想 J 使得 IJ 是 R 的主理想.

证明. 不妨假设 $I \neq 0$. 取 $\alpha \in I$, $\alpha \neq 0$, 定义

$$J := \{ \beta \in R \mid \beta I \subset (\alpha) \}.$$

显然 J 是 R 的理想, 且 $IJ = JI \subset (\alpha)$. 令 $A = \frac{1}{\alpha}IJ \subset R$, 则显然有 A 也是 R 的理想.

断言. A = R.

我们用反证法证明断言. 若 A 是真理想,则由引理6.4,存在 $\gamma \notin R$ 使得 $\gamma A \subset R$. 由 $\alpha \in I$ 且 $A = \frac{1}{\alpha}IJ \supset J$,有 $\gamma J \subset \gamma A \subset R$. 即对任意 $\beta \in J$ 有 $\gamma \beta \in R$ 且

$$\gamma \beta I \subset \gamma J I \subset \gamma \alpha A \subset \alpha R = (\alpha).$$

从而有 $\gamma\beta \in J$, 于是 $\gamma J \subset J$. 设 a_1, \dots, a_n 是 J 的一组生成元. 于是

$$\gamma a_i = \sum_{j=1}^n c_{ij} a_j \ c_{ij} \in R.$$

记 $C = (c_{ij})_{1 \le i,j \le n}$,我们有 $\det(\gamma I_n - C) = 0$. 于是 γ 是 R 上的代数整数. 由于 R 是整闭的, $\gamma \in R$, 矛盾.

引理 6.6 (消去律). 设 A, B, C 都是 Dedekind 整环 R 的理想, $A \neq 0$. 若 AB = AC, 则 B = C.

证明. 由引理6.5, 存在非零理想 J 使得 $JA=(\alpha)$. 于是我们有 JAB=JAC, 则 $(\alpha)B=(\alpha)C$. 因此 B=C.

引理 6.7. 设 A, B 是 Dedekind 整环 R 的理想,则

$$A \supset B \iff \exists ideal \ C \subset R \ s.t.AC = B.$$

证明. \Leftarrow 是显然的, 下证反方向. 由引理6.5可知存在 R 中的非零理想 J 使得 $JA=(\alpha)$, 其中 $\alpha\neq 0$. 于是由 $A\subset B$ 可以推出 $C:=\frac{1}{\alpha}JB$ 是 R 的理想, 且 $AC=\frac{1}{\alpha}AJB=\frac{1}{\alpha}(\alpha)B=B$.

定理 6.8. 设 R 是一个 Dedekind 整环, $I \subset R$ 是非平凡理想, 则存在有限个素理 想 $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, 使得

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

且在不记次序的意义下唯一.

证明. **I. 存在性**. 我们用反证法. 令 S 是所有不能写成有限个素理想乘积的非平凡理想构成的集合. 于是 S 中有极大元 $M \neq R$. 取极大理想 $P \supset M$, 则由引理6.7, 存在理想 I 使得 PI = M 且 $I \not\supseteq M$. 于是 $I \notin S$. 故存在素理想 $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ 使得 $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$. 则 $M = P\mathfrak{p}_1 \cdots \mathfrak{p}_k$,矛盾.

II. 唯一性. 设 $I = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. 则 $\mathfrak{p}_1 \supset \mathfrak{q}_1 \cdots \mathfrak{q}_m$, 因此 \mathfrak{p}_1 包含某个 \mathfrak{q}_i , 不妨设包含 \mathfrak{q}_1 , 由消去律和归纳法可知该分解唯一.

注. 在 Z 上 6.8 即为算术基本定理.

于是许多初等数论的概念可以自然地建立在 Dedekind 整环上. 我们称理想间有 A 整除 B(记为 A|B),如果存在理想 C 使得 B=AC. 由引理6.7可知这等价于 $A \supset B$. 于是我们可以去定义理想的最大公因子和最小公倍"数". 设 A,B是两个非零理想,并分解为

$$A = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}, B = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r}.$$

其中 $e_i, f_i \ge 0$, 且规定理想的 0 次幂 $\mathfrak{p}_i^0 = R$. 我们可以定义

$$\gcd(A,B) := \mathfrak{p}_1^{\min(e_1,f_1)} \cdots \mathfrak{p}_r^{\min(e_r,f_r)}, \operatorname{lcm}(A,B) := \mathfrak{p}_1^{\max(e_1,f_1)} \cdots \mathfrak{p}_r^{\max(e_r,f_r)}$$

事实上. 我们有 gcd(A, B) = A + B, $lcm(A, B) = A \cap B$. 如果 A + B = R, 我们称 A, B 互素.

引理 6.9. 设 R 是 Dedekind 整环, 则 R 是 UFD 当且仅当它是 PID.

证明. 只需证明 UFD \Rightarrow PID. 设 $\mathfrak{p} \subset R$ 是任意理想. 考虑素元分解 $0 \neq x = p_1 \cdots p_r \in \mathfrak{p}$. 则每个 (p_i) 都是素理想且 $\mathfrak{p}|(x) = \prod_i (p_i)$. 于是存在 p_i 使得 $\mathfrak{p}|(p_i)$,而 (p_i) 极大,因此 $\mathfrak{p} = (p_i)$.

引理 6.10. 设 I 是 Dedekind 整环中的非零理想, 设 $0 \neq a \in I$, 则存在 $b \in I$ 使 得 I = (a, b).

证明. 不妨设 $I \neq R$. 由于 $a \in I$, I|(a). 取 J 使得 IJ = (a). 根据中国剩余定理,我们可以取到一个同 J 互素的非零理想 J' 使得 IJ' = (b). 于是

$$(a) + (b) = \gcd((a), (b)) = \gcd(IJ, IJ') = I.$$

定理 6.11. 设 $[K:\mathbb{Q}]=n$, 则 \mathcal{O}_K 是 Dedekind 整环.

证明. (1) 设 $I \in \mathcal{O}_K$ 的非零理想. I 作为加法群是自由 Abel 群 \mathcal{O}_K 的子群, 故 而 I 也是是自由 Abel 群, 所以作为理想 I 是有限生成的. 这说明 \mathcal{O}_K 是诺特环. (2) 设 $\alpha \in K$, 设它是首一多项式 $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0 \in \mathcal{O}_K[x]$ 的根. 记 $S = \mathbb{Z}[c_0, \ldots, c_{m-1}]$. S 作为加法群是有限生成的, 即有

$$S = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_s$$
.

由于 $f(\alpha) = 0$, 每个 α^i 都能写成 $1, \alpha, \dots, \alpha^{m-1}$ 的 S-线性组合. 于是

$$S[\alpha] = S + S\alpha + \dots + S\alpha^{m-1}$$

$$= \mathbb{Z}\gamma_1 + \dots + \mathbb{Z}\gamma_s + \mathbb{Z}\alpha\gamma_1 + \dots + \mathbb{Z}\alpha\gamma_s + \mathbb{Z}\alpha^{m-1}\gamma_1 + \dots + \mathbb{Z}\alpha^{m-1}\gamma_s.$$

即 $S[\alpha]$ 作为加法群是有限生成的. 于是 α 是代数整数, 所以 $\alpha \in \mathcal{O}_K$. 故 \mathcal{O}_K 是整闭的.

(3) 设 \mathfrak{p} 是非零素理想. 取 $0 \neq \alpha \in I$. 考虑 $0 \neq m = N_{K|\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_{i}(\alpha)$. 不

妨设 $\sigma_1 = \mathrm{id}_K$. 于是 $\frac{m}{\alpha} = \prod_{i=2}^n \sigma_i(\alpha) \in K$ 也是代数整数, 故 $\frac{m}{\alpha} \in \mathcal{O}_K$. 于是 $m = \alpha \cdot \frac{m}{\alpha} \in I$. 因此 $(m) \in I$. 设 w_1, \ldots, w_n 是 \mathcal{O}_K 的一组整基, 即

$$\mathcal{O}_K = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n.$$

于是

$$m\mathcal{O}_K = \mathbb{Z}mw_1 \oplus \cdots \oplus \mathbb{Z}mw_n.$$

故

$$\mathcal{O}_K/m\mathcal{O}_K \cong (\mathbb{Z}/m\mathbb{Z})^{\oplus n}.$$

由于 I 是素理想, 综上可知 \mathcal{O}_K/I 是有限整环, 故为域. 因此 I 是极大理想.

推论 6.12. 设 $[K:\mathbb{Q}]=n$, I 是 K 的非零理想, 则 I 作为加法群是秩为 n 的自由 Abel 群.

定义 6.13. 设 $I \neq 0$ 是数域 K 的非空子集. 如果存在非零元 u 使得 uI 是 \mathcal{O}_K 的理想, 则称 I 是 K 的分式理想. 记 K 的全体分式理想构成的集合为 $\mathcal{I}(K)$.

设 $A, B \in K$ 的分式理想, 引入乘法

$$AB := \{ \sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B \},$$

并且定义

$$A^{-1} := \{ x \in K \mid xA \subset \mathcal{O}_K \}.$$

不难验证 AB, A^{-1} 都是分式理想.

引理 6.14. 设 $\mathfrak{p} \subset \mathcal{O}_K$ 是非零素理想, 则

$$\mathfrak{p}^{-1} := \{ x \in K \mid x\mathfrak{p} \subset \mathcal{O}_K \}$$

是 \mathfrak{p} 的逆,即 $\mathfrak{pp}^{-1} = \mathcal{O}_K$.

证明. 不难看出 $\mathcal{O}_K \subset \mathfrak{p}^{-1}$, 故 $\mathfrak{p} \subset \mathfrak{pp}^{-1} \subset \mathcal{O}_K$. 由于 \mathfrak{p} 极大, 只能有 $\mathfrak{p} = \mathfrak{pp}^{-1}$ 或者 $\mathfrak{pp}^{-1} = \mathcal{O}_K$. 假设 $\mathfrak{p} = \mathfrak{pp}^{-1}$. 令 $\alpha_1, \ldots, \alpha_r$ 是 \mathfrak{p} 的一组生成元. 于是对任意 $x \in \mathfrak{p}^{-1}$,

$$x\alpha_i = \sum_{j=1}^r c_{ij}\alpha_j \ c_{ij} \in \mathcal{O}_K.$$

记 $C = (c_{ij})_{1 \leq i,j \leq r}$,我们有 $\det(xI_r - C) = 0$,于是 x 是 \mathcal{O}_K 上的代数整数,而由于 \mathcal{O}_K 是整闭的, $x \in \mathcal{O}_K$. 这表明 $\mathcal{O}_K = \mathfrak{p}^{-1}$. 现在选择 \mathfrak{p} 中的非零元 b,取素理想分解 $\mathfrak{p}_1 \cdots \mathfrak{p}_m = (b) \subset \mathfrak{p}$. 于是存在 i, $\mathfrak{p}_i \subset \mathfrak{p}$. 不妨设 i = 1. 于是 $\mathfrak{p}_2 \cdots \mathfrak{p}_m \subsetneq (b)$,故存在 $a \in \mathfrak{p}_2 \cdots \mathfrak{p}_m$, $a \notin (b)$. 则 $a \notin b\mathcal{O}_K$,即 $ab^{-1} \notin \mathcal{O}_K$. 而我们有 $ab^{-1}\mathfrak{p} \subset b^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_m \subset \mathcal{O}_K$,即 $ab^{-1} \in \mathfrak{p}^{-1}$,矛盾.

注. 不难看出这个证明仿效了引理 6.4 的手法. 事实上, 如果没有定理 6.8, 本证明只需稍加修改: 将证明中的素理想分解改为取最小的 m 使得 $\mathfrak{p}_1\cdots\mathfrak{p}_m\subset (b)\subset \mathfrak{p}$ 即可.

定理 6.15. $\mathcal{I}(K)$ 是交换群, 单位元为 \mathcal{O}_{K} .

证明. 只需证明对任意分式理想 $A, A^{-1} := \{x \in K \mid xA \subset \mathcal{O}_K\}$ 是 A 的逆. 素理想的情况已经由引理6.14给出. 对任意理想 $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, 它的逆为 $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$. 而由 $\mathfrak{ba} = \mathcal{O}_K$, 有 $\mathfrak{b} \subset \mathfrak{a}^{-1}$. 反过来, 对 $x \in \mathfrak{a}^{-1}$, $x\mathfrak{a} \subset \mathcal{O}_K$, 则 $x\mathfrak{ab} \subset \mathfrak{b}$, 故 $x \in \mathfrak{b}$. 于是 $\mathfrak{b} = \mathfrak{a}^{-1}$. 对任意的分式理想 A 及相应的非零元 u, $(uA)^{-1} = u^{-1}A^{-1}$, 因此 $AA^{-1} = \mathcal{O}_K$.

引理 6.16. 设 $[K:\mathbb{Q}]=n$, I 是 K 的分式理想, 则 I 作为加法群是秩为 n 的自由 Abel 群.

设 $[K:\mathbb{Q}]=n, I$ 是 \mathcal{O}_K 的理想. 设 $I=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n, \mathcal{O}_K=\mathbb{Z}w_1\oplus\cdots\oplus\mathbb{Z}w_n$, 我们有矩阵变换

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = T \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}.$$

其中 $T \in \operatorname{Mat}_n(\mathbb{Z})$.

定义 6.17. 设 $I \in \mathcal{O}_K$ 的理想. 我们称

$$N_K(I) = N_{K|\mathbb{Q}}(I) := |\det T|$$

为理想 I 的范数.

引理 6.18. 设 $A \in K$ 的非零整理想,则 $N_K(A) = |\mathcal{O}_K/A|$.

证明. 可以取 \mathcal{O}_K 的一组整基 w_1, \ldots, w_n 使得

$$\mathcal{O}_K = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n,$$

$$A = \mathbb{Z}d_1w_1 \oplus \cdots \oplus \mathbb{Z}d_nw_n.$$

于是 $N_K(A) = |d_1 \cdots d_n|$. 而

$$\mathcal{O}_K/A \cong \mathbb{Z}/d_1\mathbb{Z}\cdots \oplus \mathbb{Z}/d_n\mathbb{Z}.$$

故 $|\mathcal{O}_K/A| = |d_1 \cdots d_n|$.

推论 6.19. 对 $0 \neq \alpha \in \mathcal{O}_K$, 有 $N_K((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$.

证明. 取整基 w_1, \ldots, w_n , 有

$$\begin{pmatrix} \alpha w_1 \\ \vdots \\ \alpha w_n \end{pmatrix} = T \begin{pmatrix} w_1 \\ \vdots \\ w_n . \end{pmatrix}$$

而由定义, $N_{K|\mathbb{Q}}(\alpha) = \det T$.

定理 6.20. 设 $A, B \not\in \mathcal{O}_K$ 中的非零理想, $[K:\mathbb{Q}] = n$. 不妨设 $A = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, 其中 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ 是互不相同的素理想, $e_1, \cdots, e_r \in \mathbb{Z}_{\geq 1}$. 则

- $(1) N_K(A) = N_K(\mathfrak{p}_1)^{e_1} \cdots N_K(\mathfrak{p}_r)^{e_r},$
- (2) $N_K(AB) = N_K(A)N_K(B)$.

证明. 对 (1), 由中国剩余定理有

$$\mathcal{O}_K/A = \mathcal{O}_K/\mathfrak{p}_1^{e_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{e_r}.$$

于是

$$N_K(A) = N_K(\mathfrak{p}_1^{e_1}) \cdots N_K(\mathfrak{p}_r^{e_r}).$$

故只需证 $N_K(\mathfrak{p}^e)=N_K(\mathfrak{p})^e$, 其中 \mathfrak{p} 是素理想, $e\in\mathbb{Z}_{\geq 1}$. 由唯一分解定理我们知道 $\mathfrak{p}^m \supseteq \mathfrak{p}^{m+1}$. 取 $\alpha\in\mathfrak{p}^m\setminus\mathfrak{p}^{m+1}$ 有

$$\mathfrak{p}^m \supset (\alpha) + \mathfrak{p}^{m+1} \ncong \mathfrak{p}^{m+1}.$$

存在一个同 $\mathfrak p$ 互素的理想 B 使得 $(\alpha) = \mathfrak p^m B$, 于是 $(\alpha) + \mathfrak p^{m+1} = \mathfrak p^m (B + \mathfrak p) = \mathfrak p^m$. 这表明 $\mathfrak p^m/\mathfrak p^{m+1}$ 是由 $\alpha \mod \mathfrak p^{m+1}$ 生成的一维 $\mathcal O_K/\mathfrak p$ -向量空间. 故 $\mathcal O_K/\mathfrak p \cong \mathfrak p^m/\mathfrak p^{m+1}$. 因此

$$|\mathcal{O}_K/\mathfrak{p}^e| = |\mathcal{O}_K/\mathfrak{p}||\mathfrak{p}/\mathfrak{p}^2|\cdots|\mathfrak{p}^{e-1}/\mathfrak{p}^e| = |\mathcal{O}_K/\mathfrak{p}|^e.$$

Part III

附录 A 代数学

本附录旨在回顾正文中可能用到的代数学背景知识.

A.1 分圆多项式

本节旨在初步介绍分圆多项式并给出一些基本性质. 我们记 $\xi_n=e^{\frac{2\pi i}{n}}$.

定义 A.1. 我们称

$$\Phi_n(x) = \prod_{\substack{k=1\\(k,n)=1}}^n (x - e^{2\pi i \frac{k}{n}})$$

为 n 次分圆多项式.

注. n 次分圆多项式 (nth cyclotomic polynomial) 的 n 次来自于 n 次本原单位根 (nth primitive root), 而不是说它的次数 (degree) 是 n.

命题 A.2.
$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

证明. 首先

$$x^{n} - 1 = \prod_{k=0}^{n-1} (x - \xi_{n}^{k}) = \prod_{d \mid n} \prod_{(k,n)=d} (x - \xi_{n}^{k})$$

于是只需证明假设 (k,n)=d, 设 k=dj, 则 $\xi_n^k=\xi_n^{dj}=\xi_{\frac{n}{d}}^j$ 且 $(j,\frac{n}{d})=1$. 因此

$$\prod_{(k,n)=d} (x - \xi_n^k) = \prod_{j,\frac{n}{d}} (x - \xi_{\frac{n}{d}}^j) = \Phi_{\frac{n}{d}}(x)$$

而

$$\prod_{d|n} \Phi_{\frac{n}{d}}(x) = \prod_{d|n} \Phi_d(x)$$

推论 A.3. $\deg \Phi_n(x) = \varphi(n)$, 其中 $\varphi(n)$ 是 Euler 函数.

证明. 对命题 A.2. 式两边取次数得

$$n = \sum_{d|n} \deg \Phi_d(x)$$

应用 Möbius 变换和 Euler 函数的性质立即可得.

推论 A.4. $\Phi_n(x) \in \mathbb{Z}[x]$.

证明. 用归纳法. n=1 时显然. 设对 $\Phi_k(x)$ (1 < k < n) 命题都成立, 则对 $\Phi_n(x)$, 我们有

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{k|n\\1 \le k \le n}} \Phi_k(x)}$$

记 $f(x) = \prod_{k \mid n \atop 1 \le k \le n} \Phi_k(x)$, 我们可以做多项式的带余除法

$$x^n - 1 = f(x)q(x) + r(x)$$

其中 r(x) = 0 或 $\deg r(x) < \deg f(x)$.

则 $r(x) = f(x)(\Phi(x) - g(x))$. 若 $r(x) \neq 0$, 则 $\Phi(x) \neq g(x)$, 于是 $\deg r(x) \geq \deg f(x)$, 矛盾. 于是 r(x) = 0, $\Phi(x) = g(x) \in \mathbb{Z}[x]$ 且是首一的.

定理 A.5. $\Phi_n(x)$ 不可约且是任意 n 次本原单位根的极小多项式.

A.2 有限生成自由 Abel 群

定理 A.6. 设 (G,+) 是有限生成的自由 Abel 群, H < G 是非零子群, 则 H 也是有限生成的自由 Abel 群且 $\mathrm{rank}(H) \leq \mathrm{rank}(G)$.

这个定理在模论的框架下考虑是自然的, 若对具体的证明感兴趣可以参考欧阳毅等著《代数学 II 近世代数》.

附录 B 分析学

本附录旨在回顾正文中可能用到的分析学背景知识. 附录中的结论几乎不会给出证明, 读者可以自行参考分析学的相关著作如 [2],[3].

B.1 解析延拓

定理 B.1. 设 f,g 是在一个区域 $\Omega \subset \mathbb{C}$ 上的全纯函数, 并且在某个非空开子集 $S \subset \Omega$ 上, $f(z) = g(z) \ \forall z \in S$, 则 $f(z) = g(z) \ \forall z \in \Omega$

 $\dot{\mathbf{L}}$. 更一般地, S 可以替换成聚点在 Ω 内的 (不同点构成的)点列.

定义 B.2. 给定函数 f, F 使得它们分别在区域 Ω, Ω' 上解析, 并且 $\Omega \subset \Omega'$. 如果 $f(z) = F(z) \ \forall z \in \Omega$, 我们就称 $F \not\in f$ 到 Ω' 上的解析延拓.

如果解析延拓存在, **定理** B.1 保证了解析延拓的唯一性.

事实上, 正文中出现的大多是延拓成亚纯函数, 不难证明亚纯延拓也是唯一的.

B.2 Poisson 求和公式

Poisson 求和公式或可归于调和分析, 欲探求具体细节和一般形式的读者可查阅 [4].

定义 B.3. 设 $f: \mathbb{R} \to \mathbb{C}$ 是 L^1 函数 (即可积函数). f 的 Fourier 变换 $\hat{f}: \mathbb{R} \to \mathbb{C}$ 由

$$\hat{f}(\xi) = \int_{-\infty}^{+\infty} f(x)e^{-2\pi ix\xi}dx$$

给出, 这是一致连续的.

定义 B.4. 我们定义 Schwarz 函数空间如下

$$\mathcal{S}(\mathbb{R}) = \{ f : \mathbb{R} \to \mathbb{C} \mid f \in C^{\infty}(\mathbb{R}), |f^{(n)}(t)| = o(|t|^{c})(t \to \pm \infty) \ \forall n \in \mathbb{N}_{\geq 0}, c \in \mathbb{R} \}$$

引理 B.5. 设 $f,g \in \mathcal{S}(\mathbb{R})$. 则有

- (1) $\hat{f}, \hat{g} \in \mathcal{S}(\mathbb{R})$.
- (2) $\hat{f}(t) = f(-t)$.
- (3) 对卷积

$$(f \star g)(t) = \int_{\infty}^{\infty} f(t - u)g(u)du$$

有

$$\widehat{f \star g}(s) = \widehat{f}(s)\widehat{g}(s).$$

定理 B.6 (Poisson 求和公式). 若 $f \in \mathcal{S}(\mathbb{R})$, 则

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

附录 C "初等"方法

本附录将介绍一些只用到数学分析的方法, 主要内容都是关于均阶估计的.

C.1 Dirichlet 除数问题

考虑除数函数 $d(n) = \sum_{m|n} 1$.

$$\sum_{n \le x} d(n) = \sum_{n \le x} \sum_{m|n} 1$$

$$\stackrel{(n=mq)}{=} \sum_{\substack{m,q \\ mq \le x}} 1 = \sum_{m \le x} \sum_{q \le \frac{x}{m}} 1$$

$$= \sum_{m \le x} \left[\frac{x}{m} \right] = \sum_{m \le x} \left(\frac{x}{m} - \left\{ \frac{x}{m} \right\} \right)$$

$$= x \sum_{m \le x} \frac{1}{m} - \sum_{m \le x} \left\{ \frac{x}{m} \right\}$$

注意到

$$\sum_{m \le x} \frac{1}{m} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

其中 γ 是 Euler 常数.

于是

$$\sum_{n \le x} d(n) = x \log x + O(x).$$

为了改进上述结果, 观察上述对 $mq \le x$ 的求和, 我们给出它的几何描述, 即第一象限的双曲线同坐标轴之间的区域有多少整点. 这启发我们考虑如下等式

$$\sum_{n \le x} d(n) = 2 \sum_{m \le x} \left[\frac{x}{m} \right] - \left[\sqrt{x} \right]^2$$

$$= 2\left(x(\log \sqrt{x} + \gamma + O(\frac{1}{\sqrt{x}})) - \sum_{m \le \sqrt{x}} \left\{ \frac{x}{m} \right\} \right) - (\sqrt{x} - \left\{ \sqrt{x} \right\})^2$$

$$= x \log x + (2\gamma - 1)x + O(\sqrt{x}).$$

注. 比较上述结果, 我们不难得出

$$\sum_{n \le x} \left\{ \frac{x}{n} \right\} = (1 - \gamma)x + O(\sqrt{x}).$$

上面的办法可以推广到一般的数论函数即为所谓 Dirichlet 双曲律,

定理 C.1 (Dirichlet 双曲律). 设 f,g 是两个数论函数, 其部分和函数分别记为 F,G. 于是对任意的 1 < y < x 有

$$\sum_{md \leq x} f(m)g(d) = \sum_{d \leq y} g(d)F(x/d) + \sum_{m \leq x/y} f(m)G(x/m) - F(x/y)G(y).$$

证明是显然的.

此外,从上面的过程中我们可以总结一套通行的做法,考虑一般的数论函数 $f: \mathbb{N} \to \mathbb{C}$,

$$\sum_{n \le x} \sum_{d|n} f(d) \xrightarrow{\underline{(n=dq)}} \sum_{d \le x} f(d) \left[\frac{x}{d} \right]$$

$$= \sum_{d \le x} f(d) \frac{x}{d} - \sum_{d \le x} f(d) \left\{ \frac{x}{d} \right\}$$

$$= x \sum_{d \le x} \frac{f(d)}{d} + O(\sum_{d \le x} |f(d)|).$$

C.2 Chebyshev 估计

本节的主要结果是下面的定理:

定理 C.2 (Chebyshev). 对于 x > 2, 我们有

- (1) $\psi(x) \approx x$,
- (2) $\varphi(x) \simeq x$,
- (3) $\pi(x) \simeq \frac{x}{\log x}$.

证明. 首先证明存在正常数 c_1, c_2 使得

$$c_1 x \le \psi(x) \le c_2 x. \tag{8}$$

我们考虑

$$T(x) := \sum_{n \le x} \log n = \sum_{n \le x} \sum_{d|n} \Lambda(d)$$

$$\xrightarrow{\underline{(n = dq)}} \sum_{\substack{d,q \\ dq \le x}} \Lambda(d) = \sum_{d \le x} \sum_{q \le \frac{x}{d}} \Lambda(d)$$

$$= \sum_{n \le x} \psi(\frac{x}{n}) = \sum_{n = 1}^{\infty} \psi(\frac{x}{n})$$

不难看出 $T(x) = \sum_{n \le x} \log n = x \log x - x + O(\log x)$. 回忆对于单调递减趋于 0 的数列 $\{a_n\}$,有

$$a_1 - a_2 \le \sum_{n=1}^{\infty} (-1)^{n-1} a_n \le a_1 - a_2 + a_3$$

我们将其应用到 $\psi(\frac{x}{n})$ 上. 首先

$$\sum_{n=1}^{\infty} (-1)^{n-1} \psi(\frac{x}{n}) = \sum_{n=1}^{\infty} \psi(\frac{x}{n}) - 2 \sum_{n=1}^{\infty} \psi(\frac{x}{2n}) = T(x) - 2T(\frac{x}{2}),$$

于是

$$\psi(x) - \psi(\frac{x}{2}) \le T(x) - 2T(\frac{x}{2}) \le \psi(x) - \psi(\frac{x}{2}) + \psi(\frac{x}{3}).$$

我们有一组不等式

$$\psi(\frac{x}{2^k}) - \psi(\frac{x}{2^{k+1}}) \le \frac{x}{2^k} \log 2 + O(\log \frac{x}{2^k}) \quad (k = 1, 2, 3, \dots)$$

把它们加起来可得

$$\psi(x) \le (2\log 2)x + O((\log x)^2).$$

另一边,我们有

$$\psi(x) \ge \psi(x) - \psi(\frac{x}{2}) \ge T(x) - 2T(\frac{x}{2}) - \psi(\frac{x}{3})$$
$$\ge \frac{\log 2}{3}x + O(\log x)$$

其余部分效仿定理 1.6. 即可.

注. Chebyshev 利用更精细的办法, 得到 (5) 中的常数大致分别为 $c_1 = 0.92..., c_2 = 1.10....$

现在我们可以证明 Bertrand 假设, 即下述定理

定理 C.3 (Bertrand). 对任意 $n \in \mathbb{Z}^+$, (n, 2n] 至少包含一个素数.

附录 D π 是无理数

命题 D.1. π 是无理数

证明. 用反证法. 假设 $\pi = \frac{a}{b}, \ a, b \in \mathbb{Z}^+$. 引入

$$f(x) = f_n(x) = \frac{x^n (a - bx)^n}{n!} \ n \in \mathbb{Z}^+$$

不难看出 $f(0) = f(\pi) = 0$, $f(x) = f(\pi - x)$.

断言. 对每一个 $j\in\mathbb{Z}^+,$ $f^{(j)}(0)\in\mathbb{Z}.$ 下面我们证明断言. 我们可以将 f(x)的分子部分写成

$$x^n(a-bx)^n = c_n x^n + \dots + c_{2n} x^{2n}$$

其中 $c_n, \ldots, c_{2n} \in \mathbb{Z}$.

当 j < n 时, $f^{(j)}(0) = 0 \in \mathbb{Z}$.

当 $j \ge n(不妨 n \le 2n)$ 时, 考虑 $(x^j)^{(j)} = j!$, 有

$$\left(\frac{c_j x^j}{n!}\right)^{(j)} = \frac{c_j j!}{n!} \in \mathbb{Z}$$

因此断言成立. 同理我们有 $\forall j \in \mathbb{Z}^+, f^{(j)}(\pi) \in \mathbb{Z}$.

下引入

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) + \dots + (-1)^n f^{(2n)}(x)$$
$$= \sum_{j=0}^n (-1)^j f^{(2j)}(x).$$

约定 $f^{(0)}(x) = f(x)$. 于是 $f(x) = F(x) + F^{(2)}(x)$. 观察到

$$(F'(x)\sin x - F(x)\cos x)' = F''(x)\sin x + F(x)\sin x$$
$$= f(x)\sin x.$$

于是

$$\int_0^{\pi} f(x) \sin x = \left(F'(x) \sin x - F(x) \cos x \right) \Big|_0^{\pi}$$
$$= F(\pi) + F(0) \in \mathbb{Z}^+$$

而当 $0 < x < \pi$ 时, $f(x) \sin x > 0$. 于是有

$$1 \le \int_0^{\pi} f(x) \sin x \le \frac{\pi^{n+1} a^n}{n!} \to 0 \quad (n \to \infty)$$

矛盾.

参考文献

- [1] 冯克勤. 代数数论入门.
- [2] G. 特伦鲍姆. 解析与概率数论导引. 陈华一译
- [3] 朱富海. 有限群表示论
- [4] Serge Lvovski. Principles of Complex Analysis.
- [5] Elias M.Stein. Complex Analysis.
- [6] Loukas Grafakos. Classical Fourier Analysis. GTM249.
- [7] J-P Serre. Linear Representations of Finite Groups. GTM42.
- [8] J.Neukirch. Algebraic Number Theory.