

数论基础

Lectured by Prof. Zhao Lili

Adaus

2022 年 5 月 7 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

I	解析理论	1
1	素数分布 (初等证明)	1
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	8
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	16
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	30
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	32
5.1	代数数域	32
5.2	范, 迹和判别式	34
5.3	代数整数环	38
III		47

附录	47
A 代数学	47
A.1 分圆多项式	47
A.2 有限生成自由 Abel 群	49
B 分析学	50
B.1 解析延拓	50
B.2 Poisson 求和公式	50
C “初等” 方法	52
C.1 Dirichlet 除数问题	52
C.2 Chebyshev 估计	53
D π 是无理数	56

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.

证明. 用反证法. □

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,

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

$$= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \quad (2)$$

而

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

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

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

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,

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

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

$$a(\bmod b) := \{n \in \mathbb{Z} \mid n \equiv a(\bmod b)\}$$

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 $A = \emptyset$, 要么 $\forall a \in A, \exists b \in \mathbb{Z}^+$, s.t. $a(\bmod b) \subset A$.

验证这是一个拓扑是容易的.

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

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, $\forall a \in \bigcup_\lambda A_\lambda, \exists b \in \mathbb{Z}^+$, s.t. $a(\bmod b) \subset \bigcup_\lambda A_\lambda$.

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. $a(\bmod b) \subset A_1 \cap A_2$.

易见 $a \in \mathbb{Z}, b \in \mathbb{Z}^+$, $a(\bmod b) \in \tau$.

对任意 $n \neq \pm 1$ ($n \in \mathbb{Z}$), 都存在素数 p , s.t. $p \mid n$, i.e. $n \in 0(\bmod p)$, 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

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

故

$$\bigcap_p (\mathbb{Z} \setminus 0(\bmod p)) = \bigcap_p (1(\bmod p) \cup \cdots \cup (p-1)(\bmod p))$$

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

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

取 t 为充分大的正整数, 记 $a = tq p_1 \dots p_m$. 考虑 $\Phi_q(tp p_1 \dots p_m)$ 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. \square

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 $\Lambda : \mathbb{Z}^+ \rightarrow \mathbb{R}$

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

(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

$$\begin{aligned} \pi(x) &= \sum_{n \leq x} \mathbf{1}_{\mathbb{P}}(n) \\ &= \sum_{p \leq x} 1 \end{aligned}$$

其中 $\mathbf{1}_{\mathbb{P}}$ 是素数集合的特征函数.

(3) 在 $\pi(x)$ 的和式中考虑一个权重

$$\begin{aligned} \theta(x) &= \sum_{n \leq x} \mathbf{1}_{\mathbb{P}}(n) \log n \\ &= \sum_{p \leq x} \log p \end{aligned}$$

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

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

证明. 由命题1.4, 我们有

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

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

□

至此, 我们粗略的看看下列两个无穷级数的乘积.

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

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. $(2 \Leftrightarrow 3)$:

$$\begin{aligned}
 0 \leq \psi(x) - \theta(x) &= \sum_{\substack{k \geq 2 \\ p^k \leq x}} \log p \\
 &\leq \sum_{\substack{k \geq 2 \\ p^k \leq x}} \log x \\
 &\leq \sum_{p \leq \sqrt{x}} \log p \sum_{2 \leq k \leq \frac{\log x}{\log p}} 1 \\
 &\leq \sqrt{x} \log x
 \end{aligned}$$

于是 $\frac{\psi(x)}{x} - \frac{\theta(x)}{x} \rightarrow 0 \ (x \rightarrow +\infty)$

$(1 \Leftrightarrow 2)$ 只需看下列两个不等式:

对任意正数 $\epsilon > 0$

$$\begin{aligned}
 \theta(x) &\leq \pi(x) \log x \\
 \theta(x) &\geq \sum_{x^{1-\epsilon} \leq p \leq x} \log x^{1-\epsilon} = (1-\epsilon)(\pi(x) + O(x^{1-\epsilon})) \log x
 \end{aligned}$$

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 $\operatorname{Re}(s) < 0$ 的范围内所有的零点是 $-2, -4, \dots$, 即所有负偶数, 且它们是单零点.

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

注. *Riemann* 猜想 \Rightarrow 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

$$\psi(x_n) \geq c_1 x_n$$

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

$$\psi(y_n) \leq c_2 y_n$$

若第一种情况成立, 则

$$\begin{aligned} \int_{x_n}^{c_1 x_n} \frac{\psi(x) - x}{x^2} dx &\geq \int_{x_n}^{c_1 x_n} \frac{c_1 x_n - x}{x^2} dx \\ &= c_1 - 1 - \log c_1 > 0 \end{aligned}$$

这同假设矛盾. 类似地, 若第二种情况成立, 则

$$\begin{aligned} \int_{c_2 y_n}^{y_n} \frac{\psi(x) - x}{x^2} dx &\leq \int_{c_2 y_n}^{y_n} \frac{c_2 y_n - x}{x^2} dx \\ &= -c_2 + 1 + \log c_2 < 0 \end{aligned}$$

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 $\operatorname{Re}(s) > 1$ 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

$$\begin{aligned} |\zeta(s)| &= \left| \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \right| \\ &= \prod_p \left| \left(1 - \frac{1}{p^s}\right)^{-1} \right| \\ &\geq \prod_p \left(1 + \frac{1}{p^\sigma}\right)^{-1} \\ &\geq \prod_p \left(1 - \frac{1}{p^\sigma}\right) \\ &\geq \left(\prod_p \left(1 - \frac{1}{p^\sigma}\right)^{-1} \right)^{-1} \\ &\geq \frac{1}{\zeta(\sigma)} \in \mathbb{R}^+ \end{aligned}$$

即 $\zeta(s) \neq 0$. □

注. 现在回过头看第一节的结果, 我们有当 $\operatorname{Re}(s) > 1$ 时,

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

定理 2.2. 当 $\operatorname{Re}(s) > 1$ 时, 我们有

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{+\infty} \{x\} x^{-s-1} dx \quad (4)$$

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

证明. 当 $Re(s) > 2$ 时, 我们有

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

继续计算有

$$\begin{aligned}
 \zeta(s) &= \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s}) \\
 &= s \sum_{n=1}^{\infty} n \int_n^{n+1} x^{-s-1} dx \\
 &= s \sum_{n=1}^{\infty} \int_n^{n+1} [x] x^{-s-1} dx \\
 &= s \sum_{n=1}^{\infty} \int_n^{n+1} (x - \{x\}) x^{-s-1} dx \\
 &= s \sum_{n=1}^{\infty} \int_n^{n+1} x^{-s} dx - s \sum_{n=1}^{\infty} \int_n^{n+1} \{x\} x^{-s-1} dx \\
 &= \frac{s}{s-1} - s \int_1^{+\infty} \{x\} x^{-s-1} dx
 \end{aligned}$$

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. \square

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 $s = 0, -1, -2, \dots$, 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 $\theta(x) = \sum_{n=-\infty}^{+\infty} e^{-n^2 x \pi} (= 1 + 2 \sum_{n=1}^{\infty} e^{-n^2 x \pi})$.

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

证明. 考虑 Poisson 公式有

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

□

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.

$$\begin{aligned}
\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \int_0^{+\infty} x^{\frac{s}{2}-1} e^{-x} dx \sum_{n=1}^{\infty} \frac{1}{n^s} \\
&= \sum_{n=1}^{\infty} \frac{1}{n^s} \int_0^{+\infty} x^{\frac{s}{2}-1} e^{-x} dx \\
&\stackrel{(x=\pi n^2 y)}{=} \sum_{n=1}^{\infty} \frac{1}{n^s} \int_0^{+\infty} \pi^{\frac{s}{2}-1} n^{s-2} y^{\frac{s}{2}-1} e^{-\pi n^2 y} \pi n^2 dy \\
&= \pi^{\frac{s}{2}} \sum_{n=1}^{\infty} \int_0^{+\infty} y^{\frac{s}{2}-1} e^{-\pi n^2 y} dy \\
&= \pi^{\frac{s}{2}} \int_0^{+\infty} y^{\frac{s}{2}-1} \sum_{n=1}^{\infty} e^{-\pi n^2 y} dy \\
&= \pi^{\frac{s}{2}} \int_0^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy
\end{aligned}$$

将积分拆开如下

$$\begin{aligned}
\pi^{\frac{s}{2}} \int_0^{\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy &= \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_0^1 y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy \\
&\stackrel{(y=\frac{1}{x})}{=} \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_1^{+\infty} x^{-\frac{s}{2}-1} \frac{\theta(\frac{1}{x}) - 1}{2} dx \\
&= \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_1^{+\infty} x^{-\frac{s}{2}-1} \frac{\sqrt{x}\theta(x) - 1}{2} dx \\
&= \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_1^{+\infty} x^{-\frac{s}{2}-1} \frac{\sqrt{x}(\theta(x) - 1) + \sqrt{x} - 1}{2} dx \\
&= \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_1^{+\infty} x^{-\frac{s}{2}-\frac{1}{2}} \frac{\theta(x) - 1}{2} dx - \pi^{\frac{s}{2}} \frac{1}{s(1-s)}.
\end{aligned}$$

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

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 $\zeta(0) \neq 0$, $\zeta(-2) = \zeta(-4) = \dots = 0$ 是单零点 (有时称作平凡零点).

推论 2.7. $\operatorname{Re}(s) < 0$ 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 $s = \sigma + it$.

$$\begin{aligned}\zeta(\sigma + it) &= \prod_p \left(1 - \frac{1}{p^{\sigma+it}}\right) \\ &= \exp\left(\log \prod_p \left(1 - \frac{1}{p^{\sigma+it}}\right)\right) \\ &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{m(\sigma+it)}}\right) \\ &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{\cos(\log p)mt - i \sin(\log p)mt}{mp^{m\sigma}}\right).\end{aligned}$$

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

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

于是

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

倘若对某个 t , $1 + it$ 是零点, 则下述不等式

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

令 $\sigma \rightarrow 1^+$ 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. $|f(u)| \leq \frac{M}{u}$ ($\forall u \geq 1$).

(2) $g(s) = \int_1^{+\infty} \frac{f(u)}{u^s} du$ ($Re(s) > 0$) 可以延拓到 $Re(s) \geq 0$.

则积分 $\int_1^{+\infty} f(u) du$ 收敛.

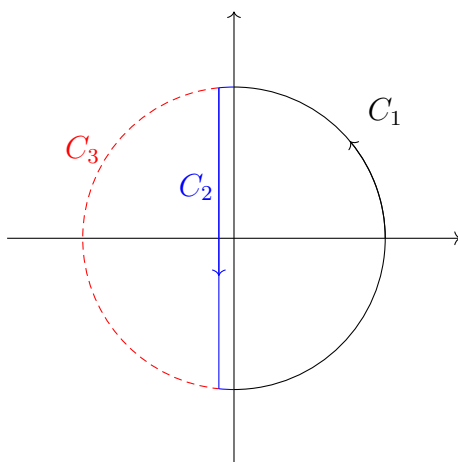
证明. 引入 $g_x(s) = \int_1^x \frac{f(u)}{u^s} du$ ($\forall s$), 要证结论即转为 $\lim_{x \rightarrow +\infty} g_x(0) = g(0)$. 对充分大的 R , 存在 $h_R > 0$, s.t. $g(s)$ 在 $Re(s) \geq -h_R$ 且 $|Im(s)| \leq R$ 的范围内解析. 任取正数 $h < h_R$, 存在 M_R , s.t. $|g(s)| \leq M_R$ ($\forall s \in D_R$). 其中 D_R 是由积分围道 $C(= C_1 + C_2)$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

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

$C_2 = C - C_1$, 虚轴左边的半圆记为 C_3 , 即

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

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

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

其中

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

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

$$\begin{aligned} |g_x(s) - g(s)| &= \left| \int_x^{+\infty} \frac{f(u)}{u^s} du \right| \\ &\leq M \left| \int_x^{+\infty} \frac{1}{u^{\sigma+1}} du \right| = \frac{M}{\sigma} x^{-\sigma} \end{aligned}$$

于是

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{C_1} \frac{g_x(s) - g(s)}{s} x^s \left(\frac{s^2}{R^2} + 1 \right) ds \right| &\leq \left| \frac{1}{2\pi i} \pi R \cdot \frac{M}{\sigma} x^{-\sigma} \cdot x^\sigma \cdot \frac{1}{R} \cdot \frac{2\sigma}{R} \right| \\ &\leq \frac{M}{R} \quad (\sigma \geq 0, s \in C_1) \end{aligned}$$

类似地有

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

而在 C_2 上, 我们把它分为两个小弧段和直线, 依次有

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

综上, 我们有

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

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 $x > x_0$, $|g_x(0) - g(0)| \leq \varepsilon$. \square

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 $c_1 x \leq \psi(x) \leq c_2 x$, 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

$$\begin{aligned} g(s) &= \int_1^{+\infty} \frac{\psi(u) - u}{u^{s+2}} du = \int_1^{+\infty} \frac{\sum_{n \leq u} \Lambda(n)}{u^{s+2}} du - \frac{1}{s} \\ &= \sum_{n=1}^{\infty} \Lambda(n) \int_n^{+\infty} \frac{1}{u^{s+2}} du - \frac{1}{s} \\ &= -\frac{1}{s+1} \frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{1}{s} \end{aligned}$$

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. \square

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

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

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 $[g \mapsto 1] \in G^*$

注. 若记 $|G| = n$, 则对任意 $g \in G$, $\chi(g)$ 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

$$\chi_1 * \chi_2 : G \rightarrow \mathbb{C}^\times$$

$$g \mapsto [\chi_1 * \chi_2(g) := \chi_1(g)\chi_2(g)]$$

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 $\chi \in G^*$,

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

定义

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

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

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

$$\rho : A^* \times B^* \rightarrow (A \times B)^*$$

$$(\sigma, \tau) \mapsto [\rho(\sigma, \tau) : (a, b) \mapsto \sigma(a)\tau(b)]$$

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 $a = \text{id}_A$, 则 $\forall b, \tau(b) = 1$, 于是 $\tau = \text{id}_{B^*}$. 取定 $b = \text{id}_B$, 则 $\forall a, \sigma(a) = 1$, 于是 $\sigma = \text{id}_{A^*}$.

(满射) 对任意 $f \in (A \times B)^*$, 取 $\sigma : a \rightarrow f(a, \text{id}_B) \quad \forall a \in A, \tau : b \rightarrow f(\text{id}_A, b) \quad \forall b \in B$. 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,

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

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

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

$$\begin{aligned} \sum_{g \in G} \chi(g) &= \sum_{g \in G} \chi(sg) \\ &= \chi(s) \sum_{g \in G} \chi(g) \end{aligned}$$

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

(2) 只需考虑 $g \neq \text{id}_G$ 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

$$\begin{aligned} \tilde{\chi} : G/\langle g \rangle &\rightarrow \mathbb{C}^\times \\ h \cdot \langle g \rangle &\mapsto \chi(h) \end{aligned}$$

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

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:

$$\begin{aligned} g : G^* &\rightarrow \mathbb{C}^\times \\ \chi &\mapsto \langle g, \chi \rangle := \chi(g) \end{aligned}$$

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 $\chi_1, \chi_2 \in G^*$,

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

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 $g_1, g_2 \in G$,

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

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 $q \in \mathbb{Z}^+$ ($q \geq 2$), $\chi \in G^*$, $\overline{m} \in G$. 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

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

为 $(\text{mod } q)$ 的 Dirichlet 特征.

注. 一共有 $\varphi(q)$ 个 $\text{mod } q$ 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 $\text{mod } q$ 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 $a, b \in \mathbb{Z}$,

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

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

命题 3.11. 对 $a \in \mathbb{Z}$,

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

命题 3.12. χ 是周期为 q 的函数.

定义 3.13 (Dirichlet L-函数). 在 $\text{Re}(s) > 1$ 时, 我们定义

$$\begin{aligned} L(s, \chi) &:= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \\ &= \prod_p \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \dots \right) \\ &= \prod_p \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} \\ &= \prod_{p \nmid q} \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} \end{aligned}$$

$L(s, \chi)$ 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, $x \geq 1$.

(1) 若 χ 不是主特征, 则

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

2 若 $\chi = \chi_0$, 则

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

证明. 由于周期性, 我们可以把求和写成如下形式:

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

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

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 $\chi \neq \chi_0$, $\operatorname{Re}(s) > 1$ 时, 有

$$L(s, \chi) = \frac{1}{s} \int_1^\infty F_\chi(u) u^{-s-1} du$$

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

证明. 由分部求和有

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} &= \sum_{n=1}^{\infty} \frac{F_\chi(n) - F_\chi(n-1)}{n^s} \\ &= \sum_{n=1}^{\infty} F_\chi(n) (n^{-s} - (n+1)^{-s}) \\ &= \frac{1}{s} \sum_{n=1}^{\infty} F_\chi(n) \int_n^{n+1} u^{-s-1} du \\ &= \frac{1}{s} \sum_{n=1}^{\infty} \int_n^{n+1} F_\chi(u) u^{-s-1} du \\ &= \frac{1}{s} \int_1^{+\infty} F_\chi(u) u^{-s-1} du. \end{aligned}$$

根据引理 3.14. 可知上式最后的积分的收敛性. □

推论 3.18. 设 $q \geq 3$, 则有 $\chi \neq \chi_0$ 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 $L(1, \chi) = 0$ ($\chi \neq \chi_0$), 则 $s = 1$ 是 $L(s, \chi)$ 的单零点.

证明. 对实数 $s > 1$ 考察

$$\begin{aligned}
 \prod_{\chi(\bmod q)} L(s, \chi) &= \prod_{\chi(\bmod q)} \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \\
 &= \exp \left(\sum_{\chi(\bmod q)} \sum_p \log \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \right) \\
 &= \exp \left(\sum_{\chi} \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} \right) \\
 &= \exp \left(\sum_{\chi} \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} \right) \\
 &= \exp \left(\varphi(q) \sum_k \sum_{p^k \equiv 1(\bmod q)} \frac{1}{kp^{ks}} \right) \geq 1.
 \end{aligned}$$

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 $\bar{\chi}$, 它也是 $\bmod q$ 的 Dirichlet 特征. χ 和 $\bar{\chi}$ 是不同的函数, 且 $L(1, \chi) = 0 \Leftrightarrow L(1, \bar{\chi}) = 0$. 当实数 $s > 1$ 时有 $L(s, \bar{\chi}) = \overline{L(s, \chi)}$. 取 $s \rightarrow 1^+$ 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

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

证明. 注意到

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

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

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

其中 γ 称为 *Euler* 常数.

证明.

$$\begin{aligned} \sum_{n=1}^y \frac{1}{n} &= 1 + \int_1^y [t] \frac{1}{t^2} dt \\ &= 1 + \int_1^y \frac{1}{t} dt - \int_1^y \{t\} \frac{1}{t^2} dt \\ &= \log y + 1 - \int_1^{+\infty} \{t\} \frac{1}{t^2} dt + O\left(\frac{1}{y}\right) \\ &= \log y + \gamma + O\left(\frac{1}{y}\right). \end{aligned}$$

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

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

其中 A 是一个常数.

证明.

$$\begin{aligned} \sum_{n=1}^y \frac{1}{\sqrt{n}} &= y \frac{1}{\sqrt{y}} + \frac{1}{2} \int_1^y [t] t^{-\frac{3}{2}} dt \\ &= \sqrt{y} + \frac{1}{2} \int_1^y t^{-\frac{1}{2}} dt - \frac{1}{2} \int_1^y \{t\} t^{-\frac{3}{2}} dt \\ &= 2\sqrt{y} - 1 - \frac{1}{2} \int_1^{+\infty} \{t\} t^{-\frac{3}{2}} dt + O(y^{-\frac{1}{2}}) \\ &= 2\sqrt{y} + A + O\left(\frac{1}{\sqrt{y}}\right). \end{aligned}$$

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 $\bmod q$ 特征 χ , $\beta > 0$, $y \geq 1$ 是实数. 我们有

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

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

$$\begin{aligned} \sum_{y \leq n \leq Y} \frac{\chi(n)}{n^\beta} &= \sum_{y \leq n \leq Y} \frac{\chi(n)}{y^\beta} - \int_1^y \sum_{y \leq n \leq t} \chi(n) t^{-\beta-1} dt \\ &\leq \varphi(q) y^{-\beta} + \varphi(q) y^{-\beta} \\ &\leq 2\varphi(q) y^{-\beta} \end{aligned}$$

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 $\bmod q$ 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

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

则

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

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

□

注. 设 $\{a(n)\}_n$ 是 \mathbb{Z}^+ 的一个重排. 于是当 $Re(s) > 1$ 时有

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

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

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

证明. 我们用 Dirichlet 双曲律 (定理) 证明这个引理.

$$\begin{aligned} \sum_{n \leq y} \frac{D(n)}{\sqrt{n}} &= \sum_{\substack{a, b \leq y \\ ab \leq y}} \frac{\chi(a)}{\sqrt{ab}} \\ &= \sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \leq \frac{y}{a}} \frac{1}{\sqrt{b}} + \sum_{b \leq \sqrt{y}} \frac{1}{\sqrt{b}} \sum_{a \leq \frac{y}{b}} \frac{\chi(a)}{\sqrt{a}} \\ &\quad - \sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \leq \sqrt{y}} \frac{\chi(b)}{\sqrt{b}} \end{aligned}$$

我们分别估计这三项.

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

于是我们得到

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

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

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

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

于是

$$\sum_{n \leq y} \frac{D(n)}{\sqrt{n}} \geq \sum_{m^2 \leq y} \frac{D(m^2)}{\sqrt{m^2}} \geq \sum_{m \leq \sqrt{y}} \frac{1}{m}. \quad (5)$$

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. \square

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

$$\begin{aligned} \left(\sum_{m=1}^{\infty} \frac{\Lambda(m)\chi(m)}{m^s} \right) \left(\sum_{k=1}^{\infty} \frac{\chi(k)}{k^s} \right) &= \sum_{n=1}^{\infty} \sum_{mk=n} \Lambda(m)\chi(m)\chi(k) \\ &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \sum_{m|n} \Lambda(m) \\ &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \log n \\ &= -L'(s, \chi). \end{aligned}$$

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

$$\begin{aligned} \sum_{\substack{n=1 \\ n \equiv a \pmod{q}}}^{\infty} \frac{\Lambda(n)}{n^s} &= \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \overline{\chi(a)} \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} \\ &= -\frac{1}{\varphi(q)} \frac{L'(s, \chi_0)}{L(s, \chi_0)} + \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \overline{\chi(a)} (-1) \frac{L'(s, \chi)}{L(s, \chi)} \end{aligned}$$

下只考虑 s 为大于 1 的实数, 考虑 $s \rightarrow 1^+$. 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

$$\begin{aligned} -\frac{L'(s, \chi_0)}{L(s, \chi_0)} &= -\frac{-\frac{1}{(s-1)^2}g(s) + \frac{1}{s-1}g'(s)}{\frac{1}{s-1}g(s)} \\ &= \frac{1}{s-1} - \frac{g'(s)}{g(s)} \rightarrow +\infty \quad (s \rightarrow 1^+). \end{aligned}$$

而对任意 $\chi \neq \chi_0$, 有

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

因此

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

即

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

注意到

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

而

$$\begin{aligned} \sum_p \sum_{k \leq 2} \frac{\log p}{p^k} &= \sum_p \log p \frac{1}{p(p-1)} \\ &\leq 2 \sum_p \frac{\log p}{p^2} \\ &\leq 2 \sum_{n=2}^{\infty} \frac{\log n}{n^2} \leq +\infty. \end{aligned}$$

且上式对 $p \equiv a \pmod{q}$ 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. □

4 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.

4.1 算术级数中的素数定理

我们首先引入 $\pi(y; q, a) = \sum_{\substack{p \leq y \\ p \equiv a \pmod{q}}} 1$. 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

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

我们首先给出同证明素数定理类似的引理.

引理 4.2. 令 $\psi(y; q, a) = \sum_{\substack{p \leq y \\ p \equiv a \pmod{q}}} \Lambda(n)$. 如果 $\lim_{y \rightarrow +\infty} \frac{\psi(y; q, a)}{y/\varphi(q)} = 1$, 则**定理 4.1.**

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

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

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 $\chi \neq \chi_0$, $\operatorname{Re}(s) = 1$ ($s \neq 1$), 则 $L(s, \chi) \neq 0$

证明. 首先对于 $\operatorname{Re}(s) > 1$ 我们有

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

类似定理2.8, 考虑

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

又

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

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

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

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

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

证明. \square

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 $\alpha, \alpha^2, \dots, \alpha^{n-1}$ 的 (整系数) 线性组合. 即 $\mathbb{Z}[\alpha]$ 由 $\alpha, \alpha^2, \dots, \alpha^{n-1}$ 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 $a_1, \dots, a_n \in A$ 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 $\mathbf{a} = (a_1, \dots, a_n)^T$, $B = (k_{ij})_{1 \leq i, j \leq n}$, 于是

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

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 $\sigma_1, \dots, \sigma_n$ 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

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

证明. $n = m$ 时显然.

设 $\alpha_1, \dots, \alpha_m$ 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, \dots, τ_m , 且每个 τ_i 都能扩张成 $[L : K(\alpha)] = \frac{n}{m}$ 个嵌入 $\tau_{i,j} |_{1 \leq j \leq \frac{n}{m}}$. $\tau_{i,j} |_{1 \leq i \leq m, 1 \leq j \leq \frac{n}{m}}$ 是 L 上 n 个不同的 K -嵌入. 于是

$$\begin{aligned} N_{L|K}(\alpha) &= \prod_i \prod_j \tau_{i,j} = \prod_i \tau_i(\alpha)^{\frac{n}{m}} \\ &= (N_{K(\alpha)|K}(\alpha))^{\frac{n}{m}} \\ &= ((-1)^m c_0)^{\frac{n}{m}} = (-1)^n c_0^{\frac{n}{m}}. \end{aligned}$$

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 $\text{Hom}_K(L, \bar{K})$ 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 $\sigma_1, \dots, \sigma_m$ 是一组代表元, 于是 $\text{Hom}_K(M, \bar{K}) = \{\sigma_1|_M, \dots, \sigma_m|_M\}$. 则

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

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

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

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

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

证明. 把判别式定义展开即知. □

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

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

$$\begin{aligned} 0 &= \sigma_i(k_1 \alpha_1 + \dots + k_n \alpha_n) = \sigma_i(k_1) \sigma_i(\alpha_1) + \dots + \sigma_i(k_n) \sigma_i(\alpha_n) \\ &= k_1 \sigma_i(\alpha_1) + \dots + k_n \sigma_i(\alpha_n) \end{aligned}$$

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

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

因此 $d_{L|K}(\alpha_1, \dots, \alpha_n) = 0$, 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

$$k_1 v_1 + \dots + k_n v_n = \mathbf{0}.$$

令 $\alpha = k_1 \alpha_1 + \dots + k_n \alpha_n \neq 0$ 但向量 $k_1 v_1 + \dots + k_n v_n$ 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 $f(x) \in K[x]$, $\alpha(=\alpha_1), \dots, \alpha_n$ 是 $f(x)$ 的 n 个不同的根. 则

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

证明. 不妨设 $n \geq 2$. n 个不同的 L 上 K -嵌入 $\sigma_1, \dots, \sigma_n$ 满足

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

则

$$\begin{aligned} d_{L|K}(1, \alpha, \dots, \alpha^{n-1}) &= \det((\sigma_i(\alpha^j))_{1 \leq i, j \leq n})^2 \\ &= \det((\alpha_i^j)_{1 \leq i, j \leq n})^2 \\ &= \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i) \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (\alpha_i - \alpha_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(\alpha_i) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(\sigma_i(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n \sigma_i(f'(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} N_{L|K}(f'(\alpha)) \end{aligned}$$

□

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

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

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

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

而我们有

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

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

$$a_n^{n-1} f(x) = (a_n x)^n + \dots + a_1 a_n^{n-1} (a_n x) + a_0 a_n^{n-1}.$$

因此我们有首一整系数多项式

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

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 $1, \omega, \dots, \omega^{s-1}$, 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 $t_0, \dots, t_{s-1} \in \mathbb{Q}$. 下证 $t_0, \dots, t_{s-1} \in \mathbb{Z}$.

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

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

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 $\delta = \det(\tau_i(\omega^k)_{\substack{1 \leq i \leq s \\ 0 \leq k \leq s-1}})$, γ_j 是根据 Cramer 法则替换 $(\tau_i(\omega^k)_{\substack{1 \leq i \leq s \\ 0 \leq k \leq s-1}})$ 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

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

上式可变换为

$$\alpha = \frac{m'_0}{d} + \frac{m'_1}{d}(1-\omega) + \cdots + \frac{m'_{s-1}}{d}(1-\omega)^{s-1}, \quad (7)$$

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

$$\alpha = \frac{p^\lambda}{p^l} (m''_0 + m''_1(1-\omega) + \cdots + m''_{s-1}(1-\omega)^{s-1})$$

于是

$$p^{l-\lambda-1}\alpha = \frac{1}{p} (m''_0 + m''_1(1-\omega) + \cdots + m''_{s-1}(1-\omega)^{s-1})$$

不妨设 $p|m''_j$ ($0 \leq j \leq t-1$) 但 $p \nmid m''_t$ ($0 \leq t \leq s-1$). 于是

$$\begin{aligned} p^{l-\lambda-1}\alpha - \frac{1}{p} (m''_0 + m''_1(1-\omega) + \cdots + m''_{t-1}(1-\omega)^{t-1}) \\ = \frac{m''_t(1-\omega)^t}{p} + \cdots + \frac{m''_{s-1}(1-\omega)^{s-1}}{p} \end{aligned}$$

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

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

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

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

这同 $p \nmid m''_t$ 矛盾, 从而 $p^l|m'_j$ ($0 \leq j \leq s-1$). □

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

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

其中 $x_1, \dots, x_n \in \mathbb{Q}$. 记 $\sigma_1, \dots, \sigma_n$ 是 n 个 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 $x_j = \frac{\gamma_j}{\delta}$, 其中 $\delta = \det(\sigma_i(\alpha_j))$, 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

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

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 $\text{rank}(\mathcal{O}_K) = n$. \square

定义 5.19. 设 $\omega_1, \dots, \omega_n \in \mathcal{O}_K$. 如果 $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_n$, 则称 $\omega_1, \dots, \omega_n$ 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 $\omega_1, \dots, \omega_n$ 是 \mathcal{O}_K 的整基, 那么 $-\omega_1, \dots, \omega_n$ 和 $\omega_1, \dots, \omega_{n-1}, \omega_1 + \omega_n$ 也都是 \mathcal{O}_K 的整基.

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

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

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

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

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

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

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 $[K : \mathbb{Q}] = n$, $\omega_1, \dots, \omega_n$ 和 $\alpha_1, \dots, \alpha_n$ 是 \mathcal{O}_K 的两组整基. 则

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

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 $A, B \in \text{Mat}_n(\mathbb{Z})$, 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 $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$. 若

- (1) $d_K(\alpha_1, \dots, \alpha_n) = d(K)$, 或
- (2) $d_K(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$ 是无平方因子的非零整数.

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

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

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

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

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

由 (1), $\det(A)^2 = 1$, 则 $A^{-1} \in \text{Mat}_n(\mathbb{Z})$, 故 $\alpha_1, \dots, \alpha_n$ 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

$$(1) \quad \mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L := \left\{ \sum_{i=1}^t \alpha'_i \beta'_i \mid \alpha'_i \in \mathcal{O}_K, \beta'_i \in \mathcal{O}_L, t \in \mathbb{Z}^+ \right\},$$

(2) 若 $\alpha_1, \dots, \alpha_m$ 和 β_1, \dots, β_n 分别是 K, L 的整基, 则 $\{\alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ 是 KL 的一组整基.

$$(3) \quad d(KL) = d(K)^n d(L)^m.$$

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 $\{\alpha_i \beta_j\}_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ 是 KL 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 $\tilde{\sigma}_k|_L = \text{id}_L$. 于是

$$\begin{aligned} \tilde{\sigma}_k(\alpha) &= \sum_{i,j} \frac{r_{ij}}{r} \sigma_k(\alpha_i) \beta_j \\ &= \sum_{i=1}^m x_i \sigma_k(\alpha_i) \end{aligned}$$

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 $\delta^2 = d_K(\alpha_1, \dots, \alpha_m) = d(K) \in \mathbb{Z}$. 于是 $x_i d(K) = \delta \gamma_i \in \mathcal{O}_L$. 因此

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

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

$$\begin{aligned} d(KL) &= \det(\pi_{k,l}(\alpha_i \beta_j))^2 \\ &= \det(\pi_{k,l}(\alpha_i) \pi_{k,l}(\beta_j))^2 \\ &= \det((\sigma_k(\alpha_i)) \otimes (\tau_l(\beta_j)))^2 \\ &= d(K)^n d(L)^m \end{aligned}$$

其中 $(\sigma_k(\alpha_i)) \otimes (\tau_l(\beta_j))$ 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 $m \not\equiv 2 \pmod{4}$, 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 $K = K_1 K_2$

由定理5.24有

$$\begin{aligned}\mathcal{O}_K &= \mathcal{O}_{K_1} \mathcal{O}_{K_2} \\ &= \mathbb{Z}(e^{2\pi i/p_1^{\alpha_1}}) \mathbb{Z}(e^{2\pi i/p_2^{\alpha_2}}) \\ &= \mathbb{Z}(e^{2\pi i/(p_1^{\alpha_1} p_2^{\alpha_2})}).\end{aligned}$$

以及

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

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 $m' = \frac{m}{2}$.

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

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

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. \square

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

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

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

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

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. \square

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 $\text{rank}(H) \leq \text{rank}(G)$.

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 $f(z) = g(z) \forall z \in \Omega$

注. 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 是 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 $f: \mathbb{R} \rightarrow \mathbb{C}$ 是 L^1 函数 (即可积函数). f 的 Fourier 变换 $\hat{f}: \mathbb{R} \rightarrow \mathbb{C}$ 由

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

给出. 这是一致连续的.

定义 B.4. 我们定义 Schwarz 函数空间如下

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

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) $\hat{\hat{f}}(t) = f(-t)$.

(3) 对卷积

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

有

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

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

$$\begin{aligned} \sum_{n \leq x} d(n) &= \sum_{n \leq x} \sum_{m|n} 1 \\ &\stackrel{(n=mq)}{=} \sum_{\substack{m, q \\ mq \leq x}} 1 = \sum_{m \leq x} \sum_{q \leq \frac{x}{m}} 1 \\ &= \sum_{m \leq x} \left[\frac{x}{m} \right] = \sum_{m \leq x} \left(\frac{x}{m} - \left\{ \frac{x}{m} \right\} \right) \\ &= x \sum_{m \leq x} \frac{1}{m} - \sum_{m \leq x} \left\{ \frac{x}{m} \right\} \end{aligned}$$

注意到

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

其中 γ 是 Euler 常数.

于是

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

为了改进上述结果, 观察上述对 $mq \leq x$ 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

$$\begin{aligned} \sum_{n \leq x} d(n) &= 2 \sum_{m \leq x} \left[\frac{x}{m} \right] - [\sqrt{x}]^2 \\ &= 2(x(\log \sqrt{x} + \gamma + O(\frac{1}{\sqrt{x}})) - \sum_{m \leq \sqrt{x}} \left\{ \frac{x}{m} \right\}) - (\sqrt{x} - \{\sqrt{x}\})^2 \\ &= x \log x + (2\gamma - 1)x + O(\sqrt{x}). \end{aligned}$$

注. 比较上述结果, 我们不难得出

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

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 $1 \leq y \leq x$ 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 $f: \mathbb{N} \rightarrow \mathbb{C}$,

$$\begin{aligned} \sum_{n \leq x} \sum_{d|n} f(d) &\stackrel{(n=dq)}{=} \sum_{d \leq x} f(d) \left[\frac{x}{d} \right] \\ &= \sum_{d \leq x} f(d) \frac{x}{d} - \sum_{d \leq x} f(d) \left\{ \frac{x}{d} \right\} \\ &= x \sum_{d \leq x} \frac{f(d)}{d} + O\left(\sum_{d \leq x} |f(d)|\right). \end{aligned}$$

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

证明. 首先证明存在正常数 c_1, c_2 使得

$$c_1 x \leq \psi(x) \leq c_2 x. \quad (8)$$

我们考虑

$$\begin{aligned} T(x) &:= \sum_{n \leq x} \log n = \sum_{n \leq x} \sum_{d|n} \Lambda(d) \\ &\stackrel{(n=dq)}{=} \sum_{\substack{d, q \\ dq \leq x}} \Lambda(d) = \sum_{d \leq x} \sum_{q \leq \frac{x}{d}} \Lambda(d) \\ &= \sum_{n \leq x} \psi\left(\frac{x}{n}\right) = \sum_{n=1}^{\infty} \psi\left(\frac{x}{n}\right) \end{aligned}$$

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

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

我们将其应用到 $\psi(\frac{x}{n})$ 上. 首先

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

于是

$$\psi(x) - \psi\left(\frac{x}{2}\right) \leq T(x) - 2T\left(\frac{x}{2}\right) \leq \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right).$$

我们有一组不等式

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

把它们加起来可得

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

另一边, 我们有

$$\begin{aligned} \psi(x) &\geq \psi(x) - \psi\left(\frac{x}{2}\right) \geq T(x) - 2T\left(\frac{x}{2}\right) - \psi\left(\frac{x}{3}\right) \\ &\geq \frac{\log 2}{3}x + O(\log x) \end{aligned}$$

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 $c_1 = 0.92\dots, c_2 = 1.10\dots$.

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

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

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

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

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

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

当 $j \geq n$ (不妨 $n \leq 2n$) 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

$$\begin{aligned} F(x) &= f(x) - f^{(2)}(x) + f^{(4)}(x) + \cdots + (-1)^n f^{(2n)}(x) \\ &= \sum_{j=0}^n (-1)^j f^{(2j)}(x). \end{aligned}$$

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

$$\begin{aligned} (F'(x) \sin x - F(x) \cos x)' &= F''(x) \sin x + F(x) \sin x \\ &= f(x) \sin x. \end{aligned}$$

于是

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

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

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

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.