数论基础

Lectured by Prof. Zhao Lilu

Adaus

2022 年 6 月 13 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

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,

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

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

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,

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

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 $(\mathbb{Z}, \tau)$ 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 $\forall a \in A, \exists b \in \mathbb{Z}^+$, s.t. $a(\text{mod } b) \subset A$.

验证这是一个拓扑是容易的.

根据定义, $\varnothing \in \tau$, $\mathbb{Z} = 0(\text{mod } 1) \in \tau$.

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. $a(\text{mod } b) \subset \bigcup_\lambda A_\lambda$.

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. $a(\text{mod } b) \subset A_1 \cap A_2$.

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

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

因此

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

而

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

故

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

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 $p_1, \ldots, p_m \equiv 1 (\text{mod } q)$

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

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

则

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

因此, 代入 a 有

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

而 $a^k \equiv 1 (\text{mod } p)$, 于是

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

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 $p \equiv 1 (\text{mod } q)$. 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 $\Lambda : \mathbb{Z}^+ \to \mathbb{R}$

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

(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

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

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

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

(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

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

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

至此, 我们粗略的看看下列两个无穷级数的乘积.

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

这几乎得到了 $\sum_{n=1}^{\infty} \dfrac{\Lambda(n)}{n^s}$ 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) $\pi(x) \sim \dfrac{x}{\log x}$

(2) $\theta(x) \sim x$

(3) $\psi(x) \sim x$

证明. $(2 \Leftrightarrow 3)$:

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

于是 $\dfrac{\psi(x)}{x} - \dfrac{\theta(x)}{x} \to 0\ (x \to +\infty)$

$(1 \Leftrightarrow 2)$ 只需看下列两个不等式:

对任意正数 $\epsilon > 0$

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

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 $Re(s) < 0$ 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 $\Rightarrow$ 素数定理.

$\zeta(1+it) \ne 0\ \forall t \in \mathbb{R}\ \Rightarrow$ 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

$$\psi(x_n)\geq c_1x_n$$

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

$$\psi(y_n)\leq c_2y_n$$

若第一种情况成立, 则

$$\begin{aligned}\int_{x_n}^{c_1x_n}\frac{\psi(x)-x}{x^2}dx &\geq \int_{x_n}^{c_1x_n}\frac{c_1x_n-x}{x^2}dx\\ &= c_1-1-\log c_1>0\end{aligned}$$

这同假设矛盾. 类似地, 若第二种情况成立, 则

$$\begin{aligned}\int_{c_2y_n}^{y_n}\frac{\psi(x)-x}{x^2}dx &\leq \int_{c_2y_n}^{y_n}\frac{c_2y_n-x}{x^2}dx\\ &= -c_2+1+\log c_2<0\end{aligned}$$

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 $Re(s) > 1$ 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

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

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

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

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 $\dfrac{s}{s-1} - s\displaystyle\int_1^{+\infty} \{x\}x^{-s-1}dx$ 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

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

□

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.

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

将积分拆开如下

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

上面证明了 $Re(s) > 2$ 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 $s = \sigma + it$.

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

于是

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

考察

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

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

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

令 $\sigma \to 1^+$ 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.* $|f(u)| \leq \dfrac{M}{u} \quad (\forall u \geq 1)$.

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

则积分 $\displaystyle\int_1^{+\infty} f(u)du$ 收敛.

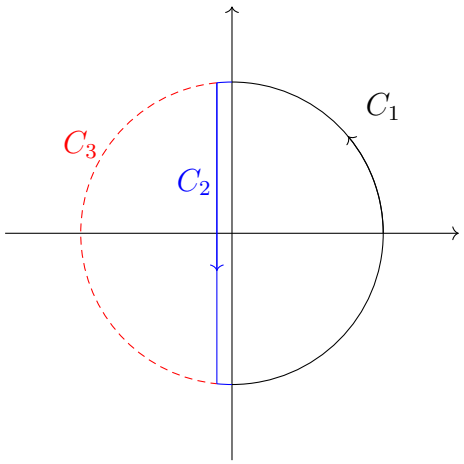
证明. 引入 $g_x(s) = \displaystyle\int_1^{x} \frac{f(u)}{u^s} \quad (\forall s)$, 要证结论即转为 $\lim\limits_{x\to+\infty} g_x(0) = g(0)$. 对充分大的 R, 存在 $h_R > 0$, s.t. $g(s)$ 在 $Re(s) \geq -h_R$ 且 $|Im(s)| \leq R$ 的范围内解析. 任取正数 $h < h_R$, 存在 M_R, s.t. $|g(s)| \leq M_R \quad (\forall s \in D_R)$. 其中 D_R 是由积分围道 $C(= C_1 + C_2)$ 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

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

其中

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

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

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

于是

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

类似地有

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

而在 C_2 上, 我们把它分为两个小弧段和直线, 依次有

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

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

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. □

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 $p \equiv a(mod\ q)$. 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 $[g \mapsto 1] \in G^*$*

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

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

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

$$\begin{aligned} \chi_k : G &\to \mathbb{C}^* \\ g^j &\mapsto [\chi_k(g^j) = e^{2\pi i \frac{kj}{n}}] \quad (0 \leq j \leq n-1) \end{aligned}$$

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

$$\begin{aligned} \rho : A^* \times B^* &\to (A \times B)^* \\ (\sigma, \tau) &\mapsto [\rho(\sigma, \tau) : (a, b) \mapsto \sigma(a)\tau(b)] \end{aligned}$$

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

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

证明. (1) 只需考虑 $\chi\neq\chi_0$ 的情况. 此时 $\exists s\in G$ 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 $(1-\chi(s))\displaystyle\sum_{g\in G}\chi(g)=0$.

(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

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

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

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:

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

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

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

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

$$\frac{1}{|G|}\sum_{\chi\in G^*}\chi(g_1)\overline{\chi(g_2)} = \frac{1}{|G|}\sum_{\chi\in G^*}\chi(g_1g_2^{-1})$$

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

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

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 $\forall a, b \in \mathbb{Z}$,

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

命题 3.10. 对 $a, b \in \mathbb{Z}$,

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

其中 $\sum_{\chi(\mathrm{mod}\ q)}$ 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

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

$L(s, \chi)$ 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 $\chi\neq\chi_0$, $Re(s)>1$ 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 $Re(s)>0$ 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

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

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 $\overline{\chi}$, 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*

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

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*

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

其中 γ 称为 Euler 常数.

证明.

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

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

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

其中 A 是一个常数.

证明.

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

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

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

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

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

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 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

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

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.

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

于是我们得到

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

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, $D(n)\ge 1$, 且对任意 n, $D(n)\ge 0$. 于是

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

若 $L(1,\chi)=0$, 根据引理3.25我们有 $\sum_{n\le y}\frac{D(n)}{\sqrt{n}}=O(1)$. 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. $\displaystyle\sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} = -\frac{L'(s,\chi)}{L(s,\chi)}$.

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 $s \to 1^+$. 当 $\chi = \chi_0$ 时有 $\dfrac{1}{s-1}g(s)$, 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

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

而对任意 $\chi \neq \chi_0$, 有

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

因此

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

即

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

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

$$\sum_{p \equiv a(\mathrm{mod}q)} \frac{\log p}{p} = +\infty.$$

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 $\pi(y;q,a)=\sum\limits_{\substack{p\le y\\ p\equiv a(\mathrm{mod}q}} 1$. 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

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

我们首先给出同证明素数定理类似的引理.

引理 4.2. 令 $\psi(y;q,a)=\sum\limits_{\substack{p\le y\\ p\equiv a(\mathrm{mod}q}}\Lambda(n)$. 如果 $\lim\limits_{y\to+\infty}\dfrac{\psi(y;q,a)}{y/\varphi(q)}=1$, 则**定理 *4.1.***.

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

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

引理 4.4. $\psi(y;q,a)\le\psi(y)=O(y)$.

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 $\chi\neq\chi_0$, $Re(s)=1$ $(s\neq1)$, 则 $L(s,\chi)\neq0$

证明. 首先对于 $Re(s)>1$ 我们有

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

类似定理2.8, 考虑

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

又

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

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

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

其中 A 是与 σ 无关的常数. 如果 $L(1+it,\chi)=0$, 则当 $\sigma\to 1^+$ 时, $L(\sigma+it,\chi)\leq B(\sigma-1)$, 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) ⇒ (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) ⇒ (3) 和 (3) ⇒ (4) 是显然的.

(4) ⇒ (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 $\boldsymbol{a} = (a_1, \cdots, a_n)^T$, $B = (k_{ij})_{1 \le i,j \le n}$, 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 $\sigma_1,\ldots,\sigma_n$ 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

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

则

$$N_{L|K}(\alpha)=(-1)^nc_0^{\frac{n}{m}},\ T_{L|K}(\alpha)=-\frac{n}{m}c_{m-1}.$$

证明. $n=m$ 时显然.

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

$$N_{K(\alpha)|K}(\alpha)=(-1)^mc_0$$
$$T_{K(\alpha)|K}(\alpha)=-c_{m-1}$$

我们有 m 个 K-嵌入 $\tau_1, \ldots, \tau_m$, 且每个 τ_i 都能扩张成 $[L : K(\alpha)] = \frac{n}{m}$ 个嵌入 $\tau_{i,j1\leq j\leq \frac{n}{m}}$. $\tau_{i,j1\leq i\leq m,1\leq j\leq \frac{n}{m}}$ 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 $\mathrm{Hom}_K(L, \bar{K})$ 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 $\mathrm{Hom}_K(M, \bar{K}) = \{\sigma_1|_M, \ldots, \sigma_m|_M\}$. 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, $\sigma_1, \ldots, \sigma_n$ 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

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

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

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

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. ($\Rightarrow$) 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 $1 \leq i \leq n$,

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

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

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

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

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

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

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

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

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

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

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

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

则

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

□

定义 5.13. $\alpha \in L$, 令 $d_{L|K}(\alpha) = d_{L|K}(1, \alpha, \ldots, \alpha^{n-1})$, 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

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

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

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

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

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

只需考虑

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

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. 记零化 α 的多项式为

$$f(x)=a_nx^n+\cdots+a_1x+a_0.$$

于是

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

因此我们有首一整系数多项式

$$g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 a_n^{n-1} x + a_0 a_n^{n-1}$$

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

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

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

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

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

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

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

从而

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

记 $t_jd = m_j$, 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

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

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

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

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 $p|m''_j$ $(0 \le j \le t-1)$ 但 $p \nmid m''_t$ $(0 \le t \le s-1)$. 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

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

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 $\alpha_1,\dots,\alpha_n$ 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 $\gamma\in\mathcal{O}_K$,

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

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

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

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

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

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 $\operatorname{rank}(\mathcal{O}_K)=n$. □

定义 5.19. 设 $\omega_1,\dots,\omega_n\in\mathcal{O}_K$. 如果 $\mathcal{O}_K=\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n$, 则称 $\omega_1,\dots,\omega_n$ 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 $A \in \mathrm{Mat}_n(\mathbb{Z})$, 则

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

证明. 记 $A = (a_{ij})_{1 \le i,j \le n}$, 则 $\alpha_i = \sum_{i=1}^n a_{ij}\omega_j$. 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 $d_K(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = \det(A)^2 d_K(\omega_1, \ldots, \omega_n)$, □

推论 5.21. 设 $[K : \mathbb{Q}] = n$, $\omega_1, \ldots, \omega_n$ 和 $\alpha_1, \ldots, \alpha_n$ 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 $A, B \in \mathrm{Mat}_n(\mathbb{Z})$, 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) $d_K(\alpha_1, \ldots, \alpha_n) = d(K)$, 或

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

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

由 (1), $\det(A)^2 = 1$, 则 $A^{-1} \in \mathrm{Mat}_n(\mathbb{Z})$, 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 $\beta_1, \ldots, \beta_n$ 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 $\{\alpha_i \beta_j\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ 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 $(r, r_{11}, \ldots, r_{mn}) = 1$. 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 $\sigma_k^{(1)}, \ldots, \sigma_k^{(n)}$. 这 n 个嵌入中一定有一个嵌入 $\widetilde{\sigma_k}$ 使得 $\widetilde{\sigma_k}|_L = \mathrm{id}_L$. 于是

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

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 $\delta^2 = d_K(\alpha_1, \ldots, \alpha_m) = d(K) \in \mathbb{Z}$. 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 $\{\sigma_k\}_{1\le k\le m}$ 是 K 上的 m 个 $\mathbb{Q}$-嵌入, $\{\tau_l\}_{1\le l\le n}$ 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 $\{\pi_{k,l}\}_{\substack{1\le k\le m\\ 1\le l\le n}}$ 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 $\zeta_m = e^{2\pi i/m}$, $m \in \mathbb{Z}_{\ge 3}$ 且 $m \not\equiv 2 \pmod 4$, 则

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

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

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

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

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

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 $m \geq n$ 使得 W_K 中含有 m 次本原单位根, 记为 ζ_m. 我们有 K

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

□

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 $w_j^n = 1$ $(1 \leq j \leq m)$. 于是 $|w_j| = 1$. 由根与系数关系可知 $|c_{m-j}| \leq \binom{m}{j}$. 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 是 $\mathcal{O}_K$ 中的单位.*

注. *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 $\sigma_1, \cdots, \sigma_n$ 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) $u \in W_K \iff |\sigma_i(u)| = 1$ $(1 \leq i \leq n)$

证明. (1) $(\Rightarrow)$ 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 $N_{K|\mathbb{Q}}(u) = \pm 1$.

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

$$f(x) = \prod_{i=1}^{n} (x - \sigma_i(u)) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

可知 u^{-1} 是首一整系数多项式

$$a_0 + a_0a_{n-1}x + \cdots + a_0a_1x^{n-1} + a_0$$

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 $a \in \mathrm{Frac}(R)$ 是 $R[x]$ 中首一多项式的根, 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

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

这同 $M \in S$ 矛盾, 于是 $S = \varnothing$. □

引理 6.4. *设 R 是 Dedekind 整环, $A \subsetneq R$ 是 R 的理想, $K = \mathrm{Frac}(R)$, 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 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ 满足 $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a)$. 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

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

即 $a^{-1}bA \subset R$. □

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

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

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

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

记 $C = (c_{ij})_{1\leq i,j\leq n}$, 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 $I \supsetneq M$. 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 $\mathfrak{q}_j$, 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 $\mathbb{Z}$ 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 $e_i, f_i \geq 0$, 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 $\gcd(A, B) = A + B$, $\operatorname{lcm}(A, B) = A \cap B$. 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

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

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

证明. (1) 设 I 是 $\mathcal{O}_K$ 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 $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0 \in \mathcal{O}_K[x]$ 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 $1, \alpha, \ldots, \alpha^{m-1}$ 的 S-线性组合. 于是

$$\begin{aligned} S[\alpha] &= S + S\alpha + \cdots + S\alpha^{m-1} \\ &= \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_s + \mathbb{Z}\alpha\gamma_1 + \cdots + \mathbb{Z}\alpha\gamma_s + \mathbb{Z}\alpha^{m-1}\gamma_1 + \cdots + \mathbb{Z}\alpha^{m-1}\gamma_s. \end{aligned}$$

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 $\dfrac{m}{\alpha} = \prod\limits_{i=2}^{n} \sigma_i(\alpha) \in K$ 也是代数整数, 故 $\dfrac{m}{\alpha} \in \mathcal{O}_K$. 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.*

6.2 分式理想

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 是 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 $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

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

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

记 $C = (c_{ij})_{1 \le i,j \le r}$, 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 $\mathfrak{b}\mathfrak{a} = \mathcal{O}_K$, 有 $\mathfrak{b} \subset \mathfrak{a}^{-1}$. 反过来, 对 $x \in \mathfrak{a}^{-1}$, $x\mathfrak{a} \subset \mathcal{O}_K$, 则 $x\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$, 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 $T \in \mathrm{Mat}_n(\mathbb{Z})$.

定义 6.17. 设 I 是 $\mathcal{O}_K$ 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 是 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

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

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

定理 6.19. 设 A, B 是 $\mathcal{O}_K$ 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) $N_K(AB) = N_K(A)N_K(B)$.

(3) 设 $A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$. 则

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

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

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 $\mathfrak{p}^m \supsetneq \mathfrak{p}^{m+1}$. 取 $\alpha \in \mathfrak{p}^m \setminus \mathfrak{p}^{m+1}$ 有

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

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 $\alpha \bmod \mathfrak{p}^{m+1}$ 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

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

(2) 由 (1) 立即可得.

(3) 记 $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ 是 n 个不同的 $\mathbb{Q}$-嵌入. 设 $\omega_1, \ldots, \omega_n$ 是 $\mathcal{O}_K$ 的一组整基. 于是有 $M = (b_{ij})_{1 \leq i,j \leq n}$ 使得

$$\alpha_j = \sum_{k=1}^{n} b_{jk}\omega_k.$$

于是有

$$\begin{aligned}\sigma_i(\alpha_j) &= \sum_{k=1}^{n} \sigma_i(b_{jk})\sigma_i(\omega_k) \\ &= \sum_{k=1}^{n} b_{jk}\sigma_i(\omega_k).\end{aligned}$$

因此 $(\sigma_i(\alpha_j)) = (\sigma_i(\omega_k))(b_{jk}) = (\sigma_i(\omega_k))M^T$. 所以

$$d_K(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i(\alpha_j)))^2 = \det((\sigma_i(\omega_k)))^2 \det(M)^2 = N_K(A)^2 d(K).$$

(4) 我们知道 $(\alpha)=\mathbb{Z}\alpha\omega_1\oplus\cdots\oplus\mathbb{Z}\alpha\omega_n$.

$$\begin{aligned} d_K(\alpha\omega_1,\ldots,\alpha\omega_n) &= \det((\sigma_i(\alpha\omega_i)))^2 \\ &= \det((\sigma_i(\alpha)\sigma_i(\omega_j)))^2 \\ &= (\prod_{i=1}^{n}\sigma_i(\alpha))^2\det(\sigma_i(\omega_j))^2 \\ &= N_{K|\mathbb{Q}}(\alpha)^2 d(K). \end{aligned}$$

而由 (3) 有 $N_K(A)^2d(K)=d_K(\alpha\omega_1,\ldots,\alpha\omega_n)$. □

下面我们把理想的范数推广到分式理想中.

定义 6.20. 设 $I=AB^{-1}$ 是 K 中的分式理想, 其中 A,B 是理想. 定义 I 的范数为

$$N_K(I)=N_K(A)N_K(B)^{-1}.$$

于是上述定理可以完全平行地推广到分式理想中, 陈述如下.

定理 6.21. 设 A,B 是 $\mathcal{O}_K$ 中的分式理想, $[K:\mathbb{Q}]=n$. 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) $N_K(AB)=N_K(A)N_K(B)$.

(3) 设 $A=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$. 则

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

(4) 对 $0\neq\alpha\in K$, 定义主分式理想 $(\alpha):=\{\alpha x\mid x\in\mathcal{O}_K\}=\alpha\mathcal{O}_K$. 有

$$N_K((\alpha))=|N_{K|\mathbb{Q}}(\alpha)|.$$

引理 6.22. (1) 设 A 是数域 K 的理想, 则 $N_K(A) \in A$.

(2) 对每个正整数 g, 只有有限个理想 $A \subset \mathcal{O}_K$ 使得 $N_K(A) = g$.

证明. (1) 若 $N_K(A) = g$, 则任意 $x \in \mathcal{O}_K/A$ 的阶数 $n|g$. 于是 $g \cdot x \in A$, 特别地, $g \cdot 1 \in A$.

(2) 设理想 $A \subset \mathcal{O}_K$ 满足 $N_K(A) = g \in \mathbb{Z}_{\geq 0}$. 则由 (1) 可知 $(g) \subset A$. 于是 $A|(g)$. 而由素理想分解可知 (g) 只有有限个因子, 故而 A 的选择有限. □

7 理想类群

7.1 格

定义 7.1. 设 $X \subset \mathbb{R}^n$ 是非零子空间, $\dim X = m$. 若存在 X 的一组基 $\alpha_1, \ldots, \alpha_m$ 使得 X 的一个子群为

$$H = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m.$$

则称 H 为 X 的一个格.

定义 7.2. 设 $H \subset \mathbb{R}^n$ 是加法子群. 如果对任意 $M > 0$, $H \cap [-M, M]^n$ 都是有限集合, 则称 H 是 $\mathbb{R}^n$ 的离散子群.

引理 7.3. 设 $H \subset \mathbb{R}^n$ 是一个非零加法子群. 则 H 是 $\mathbb{R}^n$ 的离散子群当且仅当它是某个非零子空间 X 的格.

下面我们定义格的体积. 设 H 是 $\mathbb{R}^n$ 中的格, 且

$$H = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n,$$

其中 $\alpha_1, \ldots, \alpha_n$ 是 $\mathbb{R}^n$ 的一组基. 定义

$$P = P(\alpha_1, \ldots, \alpha_n) := \{\sum_{i=1}^{n} t_i\alpha_i \mid 0 \le t_i < 1\}.$$

格 H 的体积定义为 $V(H) = \mu(P)$, 其中 μ 是 $\mathbb{R}^n$ 上的 Lebesgue 测度.

引理 7.4. 设 H 是 $\mathbb{R}^n$ 中的格, $B \subset \mathbb{R}^n$ 是可测集, 则

(1) 若 $\mu(B) \ge V(H)$, 则存在 $x, y \in B$, $x \ne y$, 使得 $x - y \in H$.

(2) 若 B 是关于原点对称的凸集, 并且 $\mu(B) > 2^n V(H)$, 则 $B \cap H$ 中有非零向量.

证明. (1) 考虑 H 的一组基的平行多面体 P, 我们有

$$B = \bigcup_{h\in H}((h+P)\cap B).$$

于是

$$\begin{aligned}\mu(B) &= \sum_{h\in H}\mu((h+P)\cap B)\\ &= \sum_{h\in H}\mu(P\cap(B-h).\end{aligned}$$

如果对于 H 中任意两个不同的元素 $h_1 \neq h_2$,

$$(P\cap(B-h_1))\cap(P\cap(B-h_2)) = \varnothing.$$

则

$$\mu(B) = \mu(\cup_{h\in H}(P\cap(B-h)) \leq \mu(P).$$

矛盾. 于是存在 $x \in (P\cap(B-h_1))\cap(P\cap(B-h_2))$. $x+h_1, x+h_2$ 即为所求. □

7.2 类群

所有主分式理想构成的子群记为 $\mathcal{P}(K)$.

定义 7.5. *商群 $C(K) := \mathcal{I}(K)/\mathcal{P}(K)$ 称为 K 的理想类群, $|C(K)|$ 称为 K 的理想类数.*

对 K 的 n 个不同的 $\mathbb{Q}$-嵌入 $\sigma_i : K \to \mathbb{C}$ $(1 \leq i \leq n)$, 如果对任意 $x \in K$, $\sigma_i(x) \in \mathbb{R}$, 则称 σ_i 为实嵌入. 不是实嵌入的嵌入称为复嵌入, 不难看出复嵌入的共轭仍是复嵌入. 我们记实嵌入的个数为 r_1, 复嵌入的个数为 r_2 对. 于是 $r_1 + 2r_2 = n$.

引理 7.6. *设 $I \subset \mathcal{O}_K$ 是非零整理想.*

$\rho : \mathcal{O}_K \to \mathbb{R}^n$

$$x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \mathrm{Re}(\sigma_{r_1+1}(x)), \mathrm{Im}(\sigma_{r_1+1}(x)), \ldots, \mathrm{Re}(\sigma_{r_1+r_2}(x)), \mathrm{Im}(\sigma_{r_1+r_2}(x))).$$

则 $\rho(I)$ 是 $\mathbb{R}^n$ 中的格, 且有

$$V(\rho(I)) = 2^{-r_2} N_K(I) |d_K|^{1/2}$$

证明. 对 $I = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_K$. $\rho(I) = \mathbb{Z}\rho(\alpha_1) \oplus \cdots \oplus \mathbb{Z}\rho(\alpha_n) \subset \mathbb{R}^n$. 取 $\mathbb{R}^n$ 中的标准基 $\{e_i\}_{1 \le i \le n}$, 则 $\rho(\alpha_i) = \sum_{j=1}^n x_{ij} e_j$, 我们有

$$V(\rho(I)) = |\det(x_{ij})| = \left| \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_1)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \cdots \\ \sigma_1(\alpha_2) & \cdots & \sigma_r(\alpha_2) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_2)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_2)) & \cdots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \cdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_n)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) & \cdots \end{pmatrix} \right|.$$

于是

$$|d(\alpha_1, \cdots, \alpha_n)|^{1/2} = |-2i|^{r_2} V(\rho(I)). \qquad \square$$

引理 7.7. (1) 设 $I \subset \mathcal{O}_K$ 是非零整理想. 则存在非零元 $x \in I$ 使得

$$|N_{K|\mathbb{Q}}(x)| \le T_K N_K(I),$$

其中 T_K 是只与 K 有关的常数.

(2) 设 A 是 K 中的分式理想, 则存在一个与 A 等价的理想 I 使得

$$|N_K(I)| \le T_K.$$

证明. (1) 对 $t > 0$, 引入

$$B_t := \{(y_1, \ldots, y_n) \in \mathbb{R}^n \mid |y_1|, \ldots, |y_{r_1}| \le t, (y_{r_1+1} + y_{r_1+2})^{1/2}, \ldots, (y_{r_1+2r_2-1} + y_{r_1+2r_2})^{1/2} \le t\}.$$

则 $\mu(B_t) = \mu(B_1) t^n$. 我们选取合适的 t 使得 $\mu(B_t) = 2^{n+1} V(\rho(I))$. 则由引理7.4可知 $B_t \cap \rho(I)$ 中有非零向量, 即存在非零元 $x \in I$ 使得 $\rho(x) \in B_t$. 于是

$$\begin{aligned} |N_{K|\mathbb{Q}}(x)| = |\prod_{i=1}^n \sigma_i(n)| &\le (\frac{1}{n} \sum_{i=1}^n |\sigma_i(x)|)^n \\ &\le (\frac{1}{n}(r_1 + 2r_2)t)^n = t^n \\ &= \frac{2^{n+1}}{\mu(B_1)} 2^{-r_2} |d(K)|^{1/2} N_K(I). \end{aligned}$$

(2) 对 A 的逆 A^{-1}, 存在 $u \in \mathcal{O}_K$ 使得 uA^{-1} 是理想. 则有

$$(u^{-1}I)^{-1} = uI^{-1},$$

因此 I 和 $u_{-1}I$ 等价, 不妨设 A^{-1} 是理想. 则存在非零元 $x \in A^{-1}$ 使得

$$|N_{K|\mathbb{Q}}(x)| \leq T_K N_K(A^{-1}).$$

令 $I = xA = (x)A$, 由于 $xA \subset A^{-1}A = \mathcal{O}_K$, 故 I 是 $\mathcal{O}_K$ 中理想. 于是

$$|N_K(I)| = |N_{K|\mathbb{Q}}(x)N_K(A)| \leq T_K. \qquad \square$$

定理 7.8. *$C(K)$ 是有限群. 即类数 $h(K) := |C(K)|$ 有限.*

证明. $h(K) \leq \#\{A \text{ 是理想} \mid N_K(A) \leq T_K\}$. 由引理6.22即证. $\square$

一般我们希望 T_K 越小越好. 例如, 若 $1 \leq T_K < 2$, 则立即得出 $h(K) = 1$.

7.3 Dirichlet 单位定理

引入映射

$$\begin{aligned} l : \mathcal{O}_K^\times &\to \mathbb{R}^{r_1+r_2} \\ x &\mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x)|, 2\log|\sigma_{r_1+1}(x)|, \ldots, 2\log|\sigma_{r_1+r_2}(x)|). \end{aligned}$$

不难看出这是从乘法群 $\mathcal{O}_K^\times$ 到加法群 $\mathbb{R}^{r_1+r_2}$ 的同态. 注意到 $\ker(l) = W_K$. 我们用 $l^{(k)}(x)$ 表示 $l(x)$ 的第 k 个分量. 则

$$\sum_{k=1}^{r_1+r_2} l^{(k)}(x) = \log(\prod_{i=1}^{n} \sigma_i(x)) = \log|N_{K|\mathbb{Q}}(x)|.$$

于是

$$\mathcal{O}_K/W_K \cong \mathrm{im}(l) \subset \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \mid \sum_{i=1}^{r_1+r_2} x_i = 0\}.$$

引理 7.9. *存在与 K 有关的常数 T'_K. 固定 $1 \le k \le r_1 + r_2$. 对任意非零元 $\alpha \in \mathcal{O}_K$, 都存在非零元 $\beta \in \mathcal{O}_K$ 使得*

$$l^{(j)}(\beta) < l^{(j)}(\alpha) \ \ \forall j \neq k,$$

并且 $|N_{K|\mathbb{Q}}(\beta)| \le T'_K$.

证明. 不妨令 $k = 1$. 设

$$B := \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid |x_i| \le c_i \ (1 \le i \le r_1), \ x_{r_1+1}^2 + x_{r_1+2}^2 \le c_{r_1+1}, \cdots .\}.$$

则 $\mu(B) = 2^{r_1} c_1 \cdots c_r \pi^{r_2} c_{r_1+1} \cdots c_{r_1+r_2}$. $\mu(B) = 2^n V_{\rho(\mathcal{O}_K)}$ 时, 由引理7.4, $B \cap \rho(\mathcal{O}_K)$ 中有非零向量. 于是存在非零元 $\beta \in \mathcal{O}_K$ 使得 $\rho(\beta) \in B$. 这样, 我们取

$$\begin{aligned} c_1 &= \frac{2^n V(\rho(\mathcal{O}_K))}{2^{r_1} c_2 \cdots c_r \pi^{r_2} c_{r_1+1} \cdots c_{r_1+r_2}} \\ c_i &= \frac{1}{2} e^{l^{(i)}(\alpha)} \ \ (2 \le i \le r_1) \\ c_j &= \frac{1}{2} e^{\frac{1}{2} l^{(j)}(\alpha)} \ \ (r_1 + 1 \le i \le r_1 + r_2) \end{aligned}$$

即可. $T'_K = \dfrac{2^n V(\rho(\mathcal{O}_K))}{2^{r_1} \pi^{r_2}}$. □

推论 7.10. *对任意 k $(1 \le k \le r_1 + r_2)$, 都存在 $u_k \in \mathcal{O}_K^\times$ 使得*

$$l^{(i)}(u_k) < 0 \ (\forall i \neq k), \ l^{(k)}(u_k) > 0.$$

证明. 对任意非零元 $\alpha_1 \in \mathcal{O}_K$, 根据引理7.9可以求出一列非零元 $\alpha_2, \alpha_3, \dots$ 满足对任意 j

$$l^{(i)}(\alpha_{j+1}) < l^{(i)}(\alpha_j) \ \ (\forall i \neq k),$$

并且 $N_{K|\mathbb{Q}}((\alpha_j)) = |N_{K|\mathbb{Q}}(\alpha_j)| \le T'_K$. 于是存在 $j' > j$ 使得 $(\alpha_j) = (\alpha_{j'})$. 故而存在 $u_k \in \mathcal{O}_K^\times$ 使得 $\alpha_{j'} = u_k \alpha_j$. 于是

$$l(\alpha_{j'}) = l(u_k) + l(\alpha_j).$$

于是对任意 $i \neq k$, $l(u_k) = l^{(i)}(\alpha_{j'}) - l^{(i)}(\alpha_j) < 0$. 而 $l^{(k)}(u_k) > 0$. □

最后我们给一个线性代数的引理.

引理 7.11. *设 A 是 m 阶实方阵, 每行元素和为 0, 且只有主对角线上的元素为正, 则*

$$rk(A) = m - 1.$$

证明. 用反证法. 设 $A = (\mathbf{a}_1, \cdots, \mathbf{a}_m)$, 其中 $\mathbf{a}_i$ 是列向量. 不妨设前 $m-1$ 个列向量是线性相关的, 则有不全为 0 的系数使得其和为 0. 不妨设 $t_k = 1$ 而其余 $|t_i| \leq 1$, 则第 k 行有

$$0 = \sum_{j=1}^{m} a_{kj} < \sum_{j=1}^{m-1} a_{kj} \leq \sum_{j=1}^{m-1} t_j a_{kj} = 0.$$

矛盾. □

现在我们可以证明 Dirichlet 单位定理.

定理 7.12 (Dirichlet 单位定理)**.** *$\mathcal{O}_K^\times = W_K \times V_K$. 其中 V_K 是秩为 $r_1 + r_2 - 1$ 的自由 Abel 群.*

证明. 对 $M > 0$, 取 $l(x) \in l(\mathcal{O}_K^\times)$ 满足

$$|\sigma_i(x)| \leq e^M \quad (1 \leq i \leq n).$$

考虑

$$f(y) = \prod_{i=1}^{n} (y - \sigma_i(x)) = y^n + c_{n-1}y^{n-1} + \cdots + c_1 y + c_0 \in \mathbb{Z}[x].$$

诸 c_i 满足 $c_i \leq 2^n e^{nM}$. 这样的多项式只有有点多个, 从而所选的 $l(x)$ 只有有限多个. 即 $l(\mathcal{O}_K^\times) \cap [-M, M]^{r_1+r_2}$ 是有限集. 这说明 $l(\mathcal{O}_K^\times)$ 是 $\mathbb{R}^{r_1+r_2}$ 的离散子群. 由定义可知 $l(\mathcal{O}_K^\times)$ 是秩不大于 $r_1 + r_2 - 1$ 的自由 Abel 群. 而推论7.10中找的向量 $l(u_k)$ $(1 \leq k \leq r_1 + r_2)$ 构成了一个 $r_1 + r_2$ 阶的方阵, 它满足引理7.11的条件, 于是我们找到了 $r_1 + r_2 - 1$ 个线性无关的向量. 即 $rk(l(\mathcal{O}_K^\times)) = r_1 + r_2 - 1$. □

7.4 Fermat 猜想的 Kummer 定理

现在我们考察分圆域 $K = \mathbb{Q}(\omega)$, $\omega = e^{2\pi i\frac{1}{p}}$, $p \geq 3$ 是素数, $[K : \mathbb{Q}] = p - 1$, K 的类数记为 h_p. 我们知道 $\mathcal{O}_K = \mathbb{Z}[\omega]$, 从 $1, \omega, \ldots, \omega^{p-1}$ 中任意选取 $p-2$ 个都能构成 $\mathcal{O}_K$ 的一组整基.

由于

$$\prod_{j=1}^{p-1}(1-\omega^j) = p,$$

我们把它放到理想里看就得到了

$$\prod_{j=1}^{p-1}(1-\omega^j)\mathcal{O}_K = p\mathcal{O}_K,$$

每个 $(1-\omega^j)\mathcal{O}_K$ 的范数都是 p, 故而是素理想. 而

$$1-\omega^j = (1-\omega)(1+\omega+\cdots+\omega^{j-1}).$$

并且我们可以取 j' 使得 $jj' \equiv 1 \pmod{p}$, 则

$$1-\omega = 1-\omega^{jj'}.$$

于是有

$$p\mathcal{O}_K = B^{p-1},$$

其中 $B = (1-\omega)\mathcal{O}_K$.

引理 7.13. *设 $x, y \in \mathbb{Z}_{\geq 0}$ 并且 $p \nmid xy(x+y)$, x, y 互素. 则*

$$(x+\omega^j y) \quad 0 \leq j \leq p-1$$

两两互素.

证明. 我们用反证法. 设有 $0 \leq j_1 < j_2 \leq p-1$ 及素理想 I 满足

$$I|(x+\omega^{j_1}y),\ I|(x+\omega^{j_2}y).$$

于是

$$I \ni \omega^{j_2}y - \omega^{j_1}y = \omega^{j_1}y(\omega^{j_2-j_1}y - 1) = \omega^{j_1}y(\omega-1)(\omega^{j_2-j_1-1}y + \cdots + 1).$$

所以 $y(\omega) - 1 \in I$, 同理 $x(\omega) - 1 \in I$, 因此 $\omega - 1 \in I$. 于是 $I|(\omega-1)\mathcal{O}_K = B$, 进而有 $I = B$. 而

$$(x+y) - (x + \omega^{j_1}y) \in B.$$

于是 $x + y \in B \cap \mathbb{Z} = p\mathbb{Z}$, 矛盾. □

引理 7.14. *对分圆域 $K = \mathbb{Q}(\omega)$, $\omega = e^{2\pi i\frac{1}{p}}$, $p \geq 3$ 是素数, 任意 $u \in \mathcal{O}_K^\times$ 都可以写成单位根和实单位的乘积.*

证明. 考虑 Galois 群 $G = \mathrm{Gal}(K|\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_{p-1}\}$. 对任意 $\sigma \in G$,

$$|\sigma(\frac{u}{\bar{u}})| = |\frac{\sigma(u)}{\sigma(\bar{u})}| = |\frac{\sigma(u)}{\overline{\sigma(u)}}| = 1.$$

于是由引理5.30, $\frac{u}{\bar{u}}$ 是单位根. 则 $\frac{u}{\bar{u}} = \pm\omega^{2a}$ $(0 \leq a \leq p-1)$.

若 $\frac{u}{\bar{u}} = \omega^{2a}$, 则

$$u\omega^{-a} = \bar{u}\omega^a = \overline{u\omega^{-a}} \in \mathbb{R}.$$

u 即表为单位根 ω^a 和实单位 $\bar{u}\omega^a$ 的乘积.

若 $\frac{u}{\bar{u}} = -\omega^{2a}$, 则

$$u\omega^{-a} = -\bar{u}\omega^a.$$

而取整基 $\omega, \ldots, \omega^{p-1}$, 可以把 $u\omega^{-a} \in \mathcal{O}_K$ 表为

$$u\omega^{-a} = c_1\omega + \cdots + c_{p-1}\omega^{p-1}.$$

于是

$$-\bar{u}\omega^a = -\overline{u\omega^{-a}} = -c_1\bar{\omega} - \cdots - c_{p-1}\bar{\omega^{p-1}}.$$

则

$$u\omega^{-a} = c_1(\omega - \omega^{-1}) + c_2(\omega^2 - \omega^{-2}) + \cdots \in B.$$

而 $u\omega^{-a}$ 是单位, 故此种情况不会发生. □

现在我们可以证明 Kummer 关于 Fermat 猜想的工作. 在证明中我们将看到此前我们学过的知识将得到充分的运用, 事实上这也反映了 Fermat 猜想在代数数论理论的发展中起到的支柱作用.

定理 7.15 (Kummer)**.** *设 $p \geq 5$ 是素数. 若 $p \nmid h_p$, 则不存在 $x, y, z \in \mathbb{Z}$ 满足*

$$x^p + y^p = z^p$$

并且 $p \nmid xyz$.

证明. 用反证法. 不妨设 x, y, z 两两互素. $p|x-y$ 和 $p|x+z$ 不能同时成立, 我们不妨假设 $p \nmid x - y$. 用反证法, 假设存在 $x, y, z \in \mathbb{Z}$ 满足

$$x^p + y^p = z^p$$

并且 $p \nmid xyz$. 则在分圆域 $K = \mathbb{Q}(\omega)$, $\omega = e^{2\pi i \frac{1}{p}}$ 中可以写成

$$x^p + y^p = \prod_{j=0}^{p-1} x + \omega^j y = z^p \in \mathcal{O}_K.$$

于是作为 $\mathcal{O}_K$ 中的理想有

$$(x^p + y^p) = \prod_{j=0}^{p-1} (x + \omega^j y) = (z)^p = B_1^{e_1 p} \cdots B_r^{e_r p}.$$

其中我们取了素理想分解 $(z) = B_1^{e_1} \cdots B_r^{e_r}$. 而由于 $(x + \omega^j y)$ 两两互素, 故存在 $\mathcal{O}_K$ 的理想 A 使得

$$(x + \omega y) = A^p.$$

于是在理想类群 $C(K)$ 中 A 所在的等价类 $[A]^p = e_{C(K)}$. 而理想类群的阶 h_p 不被 p 整除, 所以 $[A] = e_{C(K)}$. 即 A 是主理想, 记 $A = (\alpha)$. 则 $(x + \omega y) = (\alpha)^p = (\alpha^p)$, 于是存在 $u \in \mathcal{O}_K^\times$ 使得 $x + \omega y = u\alpha^p$, 而由引理7.14, $u = u_0 \omega^j$, 其中 $u_0 \in \mathcal{O}_K \cap \mathbb{R}$, $0 \leq j \leq p-1$, 则

$$x + \omega y = u_0 \omega^j \alpha^p.$$

断言. 存在 $b \in \mathbb{Z}$ 使得 $\alpha^p \equiv b \pmod{p}$.

取整基 $1, \omega, \ldots, \omega^{p-2}$,

$$\alpha = c_0 + c_1\omega + \cdots + c_{p-2}\omega^{p-2},$$

于是

$$\alpha^p \equiv c_0^p + (c_1\omega)^p + \cdots + (c_{p-2}\omega^{p-2})^p \pmod{p}.$$

这就证明了断言.

于是

$$x + \omega y \equiv \omega^j u_0 b \pmod{p}$$
$$x + \bar{\omega} y \equiv \bar{\omega}^j u_0 b \pmod{p}.$$

则有

$$\omega^{-j}(x + \omega y) \equiv \omega^j (x + \omega^{-1} y) \pmod{p}.$$

即存在 $\beta \in \mathcal{O}_K = \mathbb{Z}[\omega]$ 使得

$$x + \omega y - \omega^{2j-1} y - \omega^{2j} x = p\beta.$$

若 $1, \omega, \omega^{2j-1}, \omega^{2j}$ 互不相同, 则 $p|x$ 且 $p|y$, 矛盾.

若 $1 = \omega^{2j-1}$, 则 $p|x - y$, 矛盾.

若 $1 = \omega^{2j}$, 则 $p|y$, 矛盾.

若 $\omega = \omega^{2j-1}$, 则 $p|x$, 矛盾. □

Part III

组合数论

8 指数和

问题. 设 p 是素数, $a \in \mathbb{Z}$. 考虑同余方程 $x^2+y^3+z^4 \equiv a \pmod p$. 我们想知道这个方程是否有解, 如果有, 那么有几个解.

为了解决这个问题, 我们考虑所谓的指数和 (Gauss 和)

$$S(p,a)=\sum_{x=0}^{p-1} e^{2\pi i\frac{ax^2}{p}}.$$

下记 M_p 表示同余方程 $x^{k_1}+y^{k_2}+z^{k_3} \equiv b \pmod p$ 的解的个数 $(1 \le x,y,z \le p-1)$. 于是有

$$\begin{aligned} M_p &= \frac{1}{p}\sum_{x,y,z}\sum_{0\le a\le p-1} e^{2\pi i\frac{(x^{k_1}+y^{k_2}+z^{k_3}-b)a}{p}} \\ &= \frac{1}{p}\sum_{0\le a\le p-1}(\sum_x e^{2\pi i\frac{ax^{k_1}}{p}})(\sum_y e^{2\pi i\frac{ay^{k_2}}{p}})(\sum_z e^{2\pi i\frac{az^{k_3}}{p}})e^{-2\pi i\frac{ab}{p}} \\ &= p^2+\frac{1}{p}\sum_{1\le a\le p-1}(\sum_x e^{2\pi i\frac{ax^{k_1}}{p}})(\sum_y e^{2\pi i\frac{ay^{k_2}}{p}})(\sum_z e^{2\pi i\frac{az^{k_3}}{p}})e^{-2\pi i\frac{ab}{p}}. \end{aligned}$$

引理 8.1. $p \ge 3$ 且 $(a,p)=1$ 时

$$S(p,a)=\left(\frac{a}{p}\right)\varepsilon_p\frac{1}{p^2},$$

其中 $\varepsilon_p=\begin{cases} 1 & p\equiv 1\ (mod\ 4), \\ i & p\equiv 3\ (mod\ 4). \end{cases}$

引理 8.2. $|S(p,a)|=\sqrt{p}$

证明. 作平方

$$\begin{aligned}|S(p,a)|^2 &= |\sum_{x=0}^{p-1} e^{2\pi i\frac{ax^2}{p}}|^2 \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e^{2\pi i\frac{a(x^2-y^2)}{p}}.\end{aligned}$$

取线性变换 $\begin{cases} u = x+y \\ v = x-y \end{cases}$, 则有

$$\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e^{2\pi i\frac{a(x^2-y^2)}{p}} = \sum_{u=0}^{p-1}\sum_{v=0}^{p-1} e^{2\pi i\frac{auv}{p}} = p. \qquad \square$$

于是当 $k_1 = k_2 = k_3 = 2$ 时, $|M_p - p^2| \le \frac{p^{3/2}(p-1)}{p}$. 因此

$$M_p \ge p^2 - \sqrt{p}(p-1) \ge 1,$$

即此时同余方程有解.

引理 8.3. $S(p,a) = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right) e^{2\pi i\frac{ax}{p}} = \left(\frac{a}{p}\right)\varepsilon_p\frac{1}{p^2}$.

由此我们可以给出 M_p 的精确公式

$$\begin{aligned}M_p &= p^2 + \frac{1}{p}\sum_{1\le a\le p-1}\left(\frac{a}{p}\right)\varepsilon_p^3 p^{3/2} e^{-2\pi i\frac{ab}{p}} \\ &= p^2 + \varepsilon_p^3 p^{1/2}\sum_{1\le a\le p-1}\left(\frac{a}{p}\right) e^{-2\pi i\frac{ab}{p}} \\ &= p^2 + \left(\frac{-b}{p}\right)p.\end{aligned}$$

下面我们考虑一般的指数和

$$S_k(p,a) = \sum_{0\le x\le p-1} e^{2\pi i\frac{ax^k}{p}}$$

其中 p 是素数, $(a,p) = 1$.

令 $H = \{y \in G \mid \exists x \in G \ s.t. \ x^k = y\}$. 考虑不同的 $y_1, y_2 \in H$, 有 $x_1^k = y_1, x_2^k = y_2$, 于是

$$y_2 = x_1^k (x_2^{-1})^k y_1,$$

可以看出对不同的 $y \in H$, 方程 $x^k = y$ 解的个数是一样的, 记为 r. 则 $r = \dfrac{|G|}{|H|} = |G/H|$. 于是有

$$S_k(p, a) = 1 + r \sum_{y \in H} e^{2\pi i \frac{ay}{p}}.$$

引理 8.4. $|\sum\limits_{y \in G} e^{2\pi i \frac{y}{p}} \chi(y)| = \sqrt{p}$.

证明. 作平方

$$\begin{aligned}
|\sum_{y \in G} e^{2\pi i \frac{y}{p}} \chi(y)|^2 &= \sum_{y_1 \in G} \sum_{y_2 \in G} \chi(y_1) e^{2\pi i \frac{y_1}{p}} \overline{\chi(y_2)} e^{2\pi i \frac{-y_2}{p}} \\
&\xlongequal{(y_1 = \pi y_2 c)} \sum_{y_2 c \in G} \sum_{c \in G} \chi(y_2)\chi(c) e^{2\pi i \frac{y_1}{p}} \overline{\chi(y_2)} e^{2\pi i \frac{-y_2}{p}} \\
&= \sum_{y_2 c \in G} \sum_{c \in G} \chi(c) e^{2\pi i \frac{y_2 c - y_2}{p}} \\
&= \sum_{c \in G} \chi_c \sum_{y_2 \in G} e^{2\pi i \frac{y_2 c - y_2}{p}} \\
&= p - 1 + \sum_{\substack{c \in G \\ c \neq 1}} (-\chi_c) \\
&= p - 1 + 1 = p.
\end{aligned}$$

开平方引理即证. □

由特征的正交关系有

$$\sum_{\substack{\chi (\mathrm{mod}\ p) \\ \chi^k = \chi_0}} \chi(y) = \begin{cases} r' & y \in H, \\ 0 & y \notin H. \end{cases}$$

其中 $r' = \#\{\chi \mid \chi^k = \chi_0\} = r$. 则

$$\begin{aligned} S_k(p,a) &= 1 + \sum_{y\in G} e^{2\pi i \frac{ay}{p}} \sum_{\chi^k=\chi_0} \chi(y) \\ &= 1 + \sum_{y\in G} e^{2\pi i \frac{ay}{p}} \sum_{\substack{\chi^k=\chi_0 \\ \chi\neq\chi_0}} \chi(y) + \sum_{y\in G} e^{2\pi i \frac{ay}{p}} \chi_0(y) \\ &= \sum_{\substack{\chi^k=\chi_0 \\ \chi\neq\chi_0}} \overline{\chi(a)} \sum_{y\in G} e^{2\pi i \frac{ay}{p}} \chi(y)\chi(a) \\ &= \sum_{\substack{\chi^k=\chi_0 \\ \chi\neq\chi_0}} \overline{\chi(a)} \sum_{y\in G} e^{2\pi i \frac{y}{p}} \chi(y). \end{aligned}$$

由引理8.4, 我们有

$$|S_k(p,a)| \leq (r-1)\sqrt{p} \leq (k-1)\sqrt{p}.$$

现在用 M_p 表示同余方程 $x^2 + y^3 + z^4 \equiv b \pmod{p}$ $(p \geq 5)$ 解的个数, 此时

$$|M_p - p^2| \leq 6p^{3/2}.$$

于是当 $p \geq 37$ 时, $M_p \geq 1$, 即同余方程有解.

9 Combinatorial Nullstellensatz

本节主要关注的是如下问题

问题. p 素数. $\varnothing \neq A, B \subset \mathbb{Z}/p\mathbb{Z}$, 引入集合

$$A + B = \{a + b \mid a \in A, b \in B\}$$
$$A \mathbin{\widehat{+}} B = \{a + b \mid a \in A, b \in B, a \neq b\}.$$

我们关心上述集合的大小.

我们将用所谓的多项式方法去给出上述集合的一个下界 (Cauchy-Davenport 定理). 这个证明同这个定理最先的证明不同. 下面我们介绍 N.Alon 著名的 Combinatorial Nullstellensatz, 并用它来证明上述定理.

定理 9.1 (Combinatorial Nullstellensatz)**.** $n \geq 1$. $f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$. $x_1^{d_1} \cdots x_n^{d_n}$ *在* f *中的系数不为 0, 并且* $\deg f = d_1 + \cdots + d_n$. *若对*

$$\varnothing \neq S_1, \ldots, S_n \subset \mathbb{F}$$

有 $|S_i| \geq d_i + 1$ $(\forall i)$, *则存在* $s_i \in S_i$ $(\forall i)$ *使得*

$$f(s_1, \ldots, s_n) \neq 0.$$

证明. 不妨设 $|S_j| = d_j + 1$. 对 $d > d_j$, 考虑分解

$$x_j^d = q(x_j) \prod_{s \in S_j} (x_j - s) + r(x_j).$$

则要么 $\deg(r) \leq d$ 要么 $r \equiv 0$. 记 $h_j(x_j) = \prod_{s \in S_j} (x_j - s)$. 则我们可以将 f 表示为

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) + R(x_1, \ldots, x_n).$$

其中 $R(x_1, \ldots, x_n)$ 是 $h_j(x_j)$ 的单项式的和式, 于是 $\forall s_i \in S_i$ $(1 \leq i \leq n)$, $R(s_1, \ldots, s_n) = 0$. 并且可以知道 $x_1^{d_1} \cdots x_n^{d_n}$ 在 f 中的系数即为其在 g 中的系数. 于是 $g(x_1, \ldots, x_n)$ 可以写成

$$g(x_1, \ldots, x_n) = x_1^{d_1} g_{d_1}(x_2, \ldots, x_n) + \cdots + x_1 g_1(x_2, \ldots, x_n) + g_0(x_2, \ldots, x_n).$$

下用归纳法, 存在 $s_2 \in S_2, \ldots, s_n \in S_n$ 使得 $g_{d_1}(s_2, \ldots, s_n) \neq 0$. 则对 x 的多项式 $g(x_1, s_2, \ldots, s_n)$ 存在 $s_1 \in S_1$ 使得 $g(s_1, s_2, \ldots, s_n) \neq 0$. □

定理 9.2 (Cauchy-Davenport)**.** *p 素数. $\varnothing \neq A, B \subset \mathbb{Z}/p\mathbb{Z}$.*

$$|A + B| \geq \min(|A| + |B| - 1, p)$$

证明. 对第一个不等式, 只要证当 $|A| + |B| - 1 \leq p$ 时, $|A + B| \geq |A| + |B| - 1$. 记 $|A| = k, |B| = l$. 用反证法, 假设 $|A + B| \leq k + l + -2$. 考虑多项式

$$f(x, y) = (\prod_{c \in A+B} (x + y - c))(x + y)^{k+l-2-|A+B|} \in \mathbb{F}_p[x, y].$$

则 $\deg(f) = k + l - 2$. 而 $x^{k-1}y^{l-1}$ 在 f 中的系数即为其在 $(x + y)^{k+l-2}$ 中的系数, 即为 $\binom{k+l-2}{k-1} \cdot 1_{\mathbb{F}_p} \neq 0_{\mathbb{F}_p}$. 于是由定理9.1知道存在 $a_0 \in A, b_0 \in B$ 使得 $f(a_0, b_0) \neq 0$, 矛盾. □

定理 9.3 (Alon-Nathanson-Ruzsa)**.** *p 素数. $\varnothing \neq A, B \subset \mathbb{Z}/p\mathbb{Z}$.*

$$|A \mathbin{\widehat{+}} B| \geq \min(|A| + |B| - 3, p).$$

证明. 只需将多项式改为

$$f(x, y) = (\prod_{c \in A+B} (x + y - c))(x + y)^{k+l-2-|A \mathbin{\widehat{+}} B|} \in \mathbb{F}_p[x, y].$$

即可类似地证明. □

定理 9.4. *设 q 是奇数, $\{a_1, \ldots, a_n\} \subset \mathbb{Z}/q\mathbb{Z}$ 和 $\{b_1, \ldots, b_n\} \subset \mathbb{Z}/q\mathbb{Z}$. 则存在 $\tau \in \mathfrak{S}_n$ 使得*

$$a_1 + b_{\tau(1)}, \cdots, a_n + b_{\tau_n}$$

两两不同.

证明. 考虑嵌入

$$\rho : \mathbb{Z}/q\mathbb{Z} \to \{e^{2\pi i \frac{j}{q}}\}.$$

记 $\alpha_j = \rho(a_j)$, $\beta_j = \rho(b_j)$. 于是只需要证存在 τ 使得

$$\alpha_1\beta_{\tau(1)}, \cdots, \alpha_n\beta_{\tau_n}$$

两两不同. 考虑多项式

$$f(x_1, \ldots, x_n) = \prod_{1\le i<j\le n} (\alpha_j x_j - \alpha_i x_i) \prod_{1\le i<j\le n} (x_j - x_i).$$

$\deg(f) = n(n-1)$. 取 $S_1 = \cdots = S_n = B = \{\beta_1, \cdots, \beta_n\}$, $d_1 = \cdots = d_n = n-1$. 于是只用证明 $x_1^{n-1}\cdots x_n^{n-1}$ 在 f 中的系数不为 0, 这时存在 $s_1, \ldots, s_n \in B$ 使得 $f(s_1, \ldots, s_n) \neq 0$. 注意到 f 是两个 Vandermonde 行列式的积, 我们将行列式直接展开

$$f = (\sum_{\sigma\in\mathfrak{S}_n} \varepsilon_\sigma \prod_{i=1}^n (\alpha_i x_i)^{\sigma(i)-1})(\sum_{\tau\in\mathfrak{S}_n} \varepsilon_\tau \prod_{j=1}^n (x_j)^{\tau(j)-1}).$$

这里 $\sigma(j) - 1 + \tau(j) - 1 = n-1$. 于是 $x_1^{n-1}\cdots x_n^{n-1}$ 的系数为

$$\sum_{\sigma\in\mathfrak{S}_n} \varepsilon_\sigma\varepsilon_\tau \prod_{i=1}^n (\alpha_i x_i)^{\sigma(i)-1} = \sum_{\sigma\in\mathfrak{S}_n} \prod_{i=1}^n \alpha_i^{\sigma(i)-1}.$$

若

$$\sum_{\sigma\in\mathfrak{S}_n} \prod_{i=1}^n \alpha_i^{\sigma(i)-1} = \prod_{1\le i<j\le n} (\alpha_j - \alpha_i) + 2\sum_{\substack{\sigma\in\mathfrak{S}_n \\ \varepsilon_\sigma=-1}} \prod_{i=1}^n \alpha_i^{\sigma(i)-1} = 0,$$

则

$$\prod_{1\le i<j\le n} (\alpha_j - \alpha_i) = -2\sum_{\substack{\sigma\in\mathfrak{S}_n \\ \varepsilon_\sigma=-1}} \prod_{i=1}^n \alpha_i^{\sigma(i)-1}.$$

而右式取范数为偶数, 左式取范数为奇数, 矛盾. 故而 $x_1^{n-1}\cdots x_n^{n-1}$ 在 f 中的系数不为 0. □

注. 嵌入到特征为 2 的有限域 $\mathbb{F}_{2^{\varphi(q)}}$ 上即可避开范数的计算.

Part IV

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. □

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

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

记 $f(x) = \prod\limits_{\substack{k|n \\ 1<k<n}} \Phi_k(x)$, 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. □

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

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

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

给出. 这是一致连续的.

定义 B.4. *我们定义 Schwarz 函数空间如下*

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

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

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

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

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

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

注. 比较上述结果, 我们不难得出

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

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 $1\le y\le x$ 有

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

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 $f:\mathbb{N}\to\mathbb{C}$,

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

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

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

我们考虑

$$\begin{aligned} T(x) := \sum_{n\le x} \log n &= \sum_{n\le x}\sum_{d\mid n} \Lambda(d) \\ &\overset{(n=dq)}{=\!=\!=} \sum_{\substack{d,q\\ dq\le x}} \Lambda(d) = \sum_{d\le x}\sum_{q\le \frac{x}{d}} \Lambda(d) \\ &= \sum_{n\le} \psi(\frac{x}{n}) = \sum_{n=1}^{\infty} \psi(\frac{x}{n}) \end{aligned}$$

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

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

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

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

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

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

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

当 $j \geq n$(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

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

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.

[9] N.Alon Combinatorial Nullstellensatz. Combinatorics, Probability and Computing, 1999, 8(1-2): 7-29.