Hilbert 符号

邱才颙

2023 年 1 月 22 日

1

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p | \exists y \in \mathbb{Z}_p, xy = 1\}$$

$$\mathbb{Q}_p^\times = \{x \in \mathbb{Q}_p | \exists y \in \mathbb{Q}_p, xy = 1\}$$

注意，$\mathbb{Q}_p^\times = \mathbb{Q}_p - \{0\}$，但是 $\mathbb{Z}_p^\times \neq \mathbb{Z}_p - \{0\}$。

我们的第一个任务是，分析 $\mathbb{Q}_p^\times$ 的结构。首先我们要知道，p 进数域 $\mathbb{Q}_p$ 和 $\mathbb{R}$ 一样，都是有理数 $\mathbb{Q}$ 的一种完备化，因此我们先看看 $\mathbb{R}^\times$ 的乘法结构，看看是否能够有所启发：

定理 1.1
任何非零实数 $x \in \mathbb{R}^\times$ 都可以写成

$$x = \epsilon(x)|x|$$

其中 $\epsilon(x) \in \{\pm 1\}$，而对于后一部分 $|x| \in \mathbb{R}_{>0}$，我们有公式

$$\ln|xy| = \ln|x| + \ln|y|$$

这个定理有许多可以解读的地方：

- 我们可以定义映射 $\epsilon : \mathbb{R}^\times \to \{\pm 1\}$，这个映射可以用来判断一个非零实数是不是平方元素，这个映射是乘法群同态
- $\{\pm 1\}$ 这个集合，恰好是 $\mathbb{R}$ 中的所有单位根，也就是说 $\mu(\mathbb{R}) = \{\pm 1\}$
- ϵ 的核（kernel）就是 $\mathbb{R}_{>0}$

- ln 给出了 $\mathbb{R}_{>0}$ 到 $(\mathbb{R},+)$ 的同构
- 平方元（正实数）的附近的元素也是平方元（正实数）

我们在之前已经知道，任何 $x \in \mathbb{Q}_p^\times$ 都可以写成

$$x = u(x)p^{v_p(x)}$$

其中 $u(x) \in \mathbb{Z}_p^\times$ 被 x 唯一确定，所以 p 进数的乘法结构的关键，就是乘法群 $\mathbb{Z}_p^\times$ 的结构。

对于 $\mathbb{Z}_p^\times$ 的结构，从 $\mu(\mathbb{R})$ 得到启发，首先我们来研究单位根：

引理 1.2
设 $p \neq 2$，那么方程

$$X^{p-1} = 1$$

在 $\mathbb{Z}_p$ 中有 $p-1$ 个解。

证明. 考虑多项式 $f(X) = X^{p-1} - 1$，对于 $k = 1, 2, \ldots, p-1$，我们知道 $f(k)$ 是 p 的倍数（费马小定理），换言之，$|f(k)|_p \leq \frac{1}{p}$。而 $f'(k) = (p-1)k^{p-2}$ 和 p 互素，因此 $|f'(k)|_p = 1$，Hensel 引理可以使用，因此每个 k 都可以提升为一个精确解。而 $f(X) = 0$ 即便在域 $\mathbb{Q}_p$ 中也最多有 $p-1$ 个不同的根，证毕。 □

如果我们选择 k 为 $\mathbb{Z}/p\mathbb{Z}$ 的原根，那么 k 的提升 $\zeta \in \mathbb{Z}_p^\times$ 具有性质

$$\{x \in \mathbb{Q}_p : x^{p-1} = 1\} = \{\zeta^i : i = 1, 2, \ldots, p-1\} = \mu_{p-1}(\mathbb{Z}_p^\times)$$

并且 ζ^i 模 p 的结果取遍 $1, 2, \ldots, p-1$，或者说：

$$\mu_{p-1}(\mathbb{Z}_p^\times) \subset \mathbb{Z}_p^\times \xrightarrow{\varepsilon_1} (\mathbb{Z}/p\mathbb{Z})^\times$$

是同构，ε_1（作为乘同态）的核为 $1 + p\mathbb{Z}_p$。

引理 1.3
设 $p = 2$，那么方程

$$X^2 = 1$$

在 $\mathbb{Z}_2$ 中有两个解，即 ± 1。

这里的一个技术性问题是，$\{\pm 1\} \to (\mathbb{Z}/2\mathbb{Z})^\times$ 并不是同构，实际上要使用 $\{\pm 1\} \xrightarrow{\varepsilon_2} (\mathbb{Z}/4\mathbb{Z})^\times$，而 ε_2（作为乘同态）的核为 $1 + 4\mathbb{Z}_2$。

定理 1.4
设 $x \in \mathbb{Z}_p^\times$，那么

- 若 $p \neq 2$，x 可以写成 $x = \theta y$，其中 $\theta \in \mu_{p-1}(\mathbb{Q}_p)$ 而 $y \in 1 + p\mathbb{Z}_p$，这个分解是唯一的
- 若 $p = 2$，x 可以写成 $x = \theta y$，其中 $\theta \in \mu_2(\mathbb{Q}_2)$ 而 $y \in 1 + 4\mathbb{Z}_2$，这个分解是唯一的

这时候，我们就会猜想，是否有一种神奇的对数函数，使得 $1 + p\mathbb{Z}_p$ 作为乘法群，同构于加法群 $\mathbb{Z}_p$，而 $1 + 4\mathbb{Z}_2$ 作为乘法群，同构于 $\mathbb{Z}_2$ 呢?

答案是：是的。（使用 $f(x) = \ln(1 + x)$ 的 Taylor 级数）

2 总结

- 若 $p \neq 2$，那么 $0 \neq x \in \mathbb{Q}_p$ 可以写成

$$x = p^n y$$

而 $y \in \mathbb{Z}_p^\times$ 又可以写成 $y = \theta z$，其中 $\theta \in \mu_{p-1}(\mathbb{Q}_p)$ 而 $z \in 1 + p\mathbb{Z}_p$。

- x 是 $\mathbb{Q}_p$ 中的平方元当且仅当（I）n 是偶数，（II）θ 是本原单位根的偶数次方，（III）$\log z$ 是 $\mathbb{Z}_p$ 中某个元素的两倍
- 上面的（II）可以用 Legendre 符号来计算
- 上面的（III）恒成立，不需要考虑
- 若 $p = 2$，那么 $0 \neq x \in \mathbb{Q}_2$ 可以写成

$$x = 2^n y$$

而 $y \in \mathbb{Z}_2^\times$ 又可以写成 $y = \theta z$，其中 $\theta \in \mu_2(\mathbb{Q}_2)$ 而 $z \in 1 + 4\mathbb{Z}_2$。

- x 是 $\mathbb{Q}_2$ 中的平方元当且仅当（I）n 是偶数，（II）θ 是 -1 的偶数次方（III）存在 $w \in \mathbb{Z}_2$ 使得 $z = (1 + 4w)^2 = 1 + 8w + 16w^2$
- （III）告诉我们 $z \in 1 + 8\mathbb{Z}_2$，Hensel 引理说明这是充要的（留作习题）

上面的 $\theta \in \mu(\mathbb{Q}_p)$ 叫做 y 的 Teichmüller，$z = \frac{y}{\theta}$ 叫做 y 的 diamond

再总结：提出 p 的幂之后，mod p 或者 mod 8

3 例题

3.1

证明 $X^2+1=0$ 在 $\mathbb{Q}_p$ 中有解，当且仅当 $p\equiv 1 \bmod 4$

证明. 若 $p\neq 2$，那么 -1 可以写成 $p^0\times(-1)$，故只需要 $\left(\frac{-1}{p}\right)=1$

若 $p=2$，那么 -1 可以写成 $2^0\times(-1)$，但是 -1 不满足模 8 余 1 □

3.2

证明 $X^2+2=0$ 在 $\mathbb{Q}_p$ 中有解，当且仅当 $p\equiv 1,3 \bmod 8$

证明. 若 $p=2$，那么 -2 可以写成 $2^1\times(-1)$，由于这里出现了 2 的奇数次幂，故 p 不能是 2，下考虑 $p\neq 2$，我们知道只需要

$$\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=1$$

只需回忆并查表：

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & p\equiv 1 \bmod 4\\ -1, & p\equiv 3 \bmod 4\end{cases}\quad \left(\frac{2}{p}\right)=\begin{cases}1, & p\equiv 1,7 \bmod 8\\ -1, & p\equiv 3,5 \bmod 8\end{cases}$$

□

3.3 课后习题

对于什么样的 p，$X^2+6=0$ 在 $\mathbb{Q}_p$ 中有解?

4