Hilbert 符号

邱才颙

2023 年 1 月 25 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，$\{\pm1\}\to(\mathbb{Z}/2\mathbb{Z})^\times$ 并不是同构，实际上要使用 $\{\pm1\}\xrightarrow{\varepsilon_2}(\mathbb{Z}/4\mathbb{Z})^\times$，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 Hilbert 符号

从现在开始，我们用 $\mathbb{Q}_\infty$ 代表 $\mathbb{R}$，我们记 $V=\{\infty,2,3,5,7,\dots\}$

对于 $v\in V$，定义 $\mathbb{Q}_v^\times=\mathbb{Q}_v-\{0\}$，定义平方元构成的全体为

$$(\mathbb{Q}_v^\times)^2=\{x\in\mathbb{Q}_v^\times:\exists y\in\mathbb{Q}_v^\times, x=y^2\}$$

例如 $(\mathbb{Q}_\infty^\times)^2=\mathbb{R}_{>0}$。我们定义 Hilbert 符号：若 $a,b\in\mathbb{Q}_v^\times$

$$(a,b)_v=\begin{cases}1, & \text{方程}aX^2+bY^2=Z^2\text{ 存在一组}X,Y,Z\text{ 不全为零的解}\\ -1, & \text{方程}aX^2+bY^2=Z^2\text{ 的解只有}(0,0,0)\end{cases}$$

例 4.1
对于 $v=\infty$ 的情况，$(a,b)_\infty=-1$ 当且仅当 $a,b<0$

Hilbert 符号有许多显然的性质，可以用来简化计算:

- 对称性：$(a,b)_v=(b,a)_v$
- $(a,c^2)_v=1$，因为可以考虑 $X=0,Y=1,Z=c$
- $(a,-a)_v=1$，因为可以考虑 $X=Y=1,Z=0$
- $(a,1-a)_v=1$，因为可以考虑 $X=Y=Z=1$

定理 4.2
若 $(a,b)_v=1$，那么 $(aa',b)_v=(a',b)_v$

证明. 略 $\square$

引理 4.3
若 $u\in\mathbb{Z}_p^\times$,且 $(p,u)_p=1$,那么存在 $X\in\mathbb{Z}_p,Y,Z\in\mathbb{Z}_p^\times$ 使得 $pX^2+uY^2=Z^2$

证明. 方程 $pX^2+uY^2=Z^2$ 是齐次的，因此若其在 $\mathbb{Q}_p$ 中有非平凡解，那么就在 $\mathbb{Z}_p$ 中有解，并且 $v_p(X),v_p(Y),v_p(Z)$ 的最小值是 0。

显然 $v_p(Z^2-uY^2)=v_p(pX^2)\geq 1$。

若 $v_p(Z)>0,v_p(Y)=0$，那么 $v_p(Z^2-uY^2)=0$，矛盾

若 $v_p(Y)>0,v_p(Z)=0$，那么 $v_p(Z^2-uY^2)=0$，矛盾

若 $v_p(Y),v_p(Z)>0$，那么 $v_p(pX^2)=v_p(Z^2-uY^2)\geq 2$，这又和题目中 $v_p(X),v_p(Y),v_p(Z)$ 的最小值是 0 的假设矛盾了。综上所述，仅有的可能性是 $v_p(Y)=v_p(Z)=0$。 $\square$

定理 4.4 (定理 A)
假设 $p\neq 2$ 为素数，$u\in\mathbb{Z}_p^\times$，那么 $(p,u)_p=\left(\frac{u}{p}\right)$

证明. 我们考虑 u 是否是 $\mathbb{Z}_p^\times$ 中的平方元:

若 u 是 $\mathbb{Z}_p^\times$ 中的平方元，那么我们知道 $(\frac{u}{p})=1$，并且 $(p,u)=1$，此时两者相等。

若 u 不是 $\mathbb{Z}_p^\times$ 中的平方元，那么我们知道 $(\frac{u}{p})=-1$，我们还需要证明方程 $pX^2+uY^2=Z^2$ 在 $\mathbb{Q}_p$ 中无平凡解，假设有，根据引理 4.3，我们可以找到一组解 (X,Y,Z) 使得 $v_p(X)\geq 0,v_p(Y)=v_p(Z)=0$，将方程模 p，得到 $uY^2\equiv Z^2 \bmod p$，矛盾 $\square$

定理 4.5 (定理 B)
假设 $p \neq 2$ 为素数，$u, v \in \mathbb{Z}_p^\times$，那么 $(u, v)_p = 1$

证明. 首先将方程模 p，考虑有限域 $\mathbb{F}_p$ 上的方程

$$uX^2 + vY^2 = Z^2$$

这个方程组的次数和为 2，变量为 3，符合 Chevalley-Warning 定理的适用条件，从而解的数量是 p 的倍数，特别地，它拥有一组非平凡解 (x_0, y_0, z_0)，把这些量看作整数，而整数又是 p 进数

换言之，x_0, y_0, z_0 之中至少有一个数不是 p 的倍数，我们就把这个变量看作主元，上面的多项式关于这个主元的导数，赋值一定是 $p^0 = 1$，因此 Hensel 引理适用，我们可以将这个主元从近似解提升到精确解 □

定理 4.6 (定理 C)
假设 $p \neq 2$ 为素数，$u, v \in \mathbb{Z}_p^\times$，那么 $(pu, pv)_p = \left(\frac{-uv}{p}\right)$

证明. 我们知道 $(pu, -pu)_p = (u, -uv)_p = 1$，从而

$$(pu, pv)_p = (pu, (-pu)pv)_p = (pu, -uv)_p = (p, -uv)_p$$

然后使用定理 A □

例 4.7
Diophantus 在《算术》中写道 $15x^2 - 36 = y^2$ 没有有理数解，请替他证明

证明. 假设此方程有解，那么方程

$$15X^2 + (-1)Y^2 = Z^2$$

有非平凡的 3-adic 数解，也就是说 $(15, -1)_3 = 1$

但是计算可得 $(3^1 \times 5, -1)_3 = (3, -1)_3(5, -1)_3 = \left(\frac{-1}{3}\right) = -1$ □

5 Hilbert 符号，续，$p = 2$

6 Hilbert 互反律

定理 6.1 (Hilbert 互反律)
若 a, b 是非零有理数，那么 $(a,b)_v$ 只对有限个 $v \in V$ 取 -1，并且实际上取偶数次 -1，也就是说

$$\prod_{v \in V}(a,b)_v = 1$$

Hilbert 互反律可以用来解释，二次互反律中为什么

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

我们来计算 $(p,q)_v$，显然当 v 不取 $2, p, q$ 的时候，$(p,q)_v = 1$，因此我们知道 $(p,q)_2(p,q)_p(p,q)_q = 1$，这个式子就是二次互反律。

Hilbert 的叙述中，素数 2 不再看起来像一个障碍或者特殊情况。并且这里的 a, b 可以取的值也不再有 Legendre 符号中的种种限制。并且 Hilbert 的叙述中，实数 $\mathbb{Q}_\infty$ 的情况被考虑了，且和所有的 p 进数 $\mathbb{Q}_p$ 平等地出现。我们可以合理地认为，这种叙述更加本质。

Hilbert 互反律不仅仅是二次互反律的一种新的叙述方法,实际上 Hilbert 互反律不是一个互反律，而是一族互反律：无数个互反律。

它可以推广到任意的数域上，我们无法详细说明这一点，但是让我们继续研究 Hilbert 符号的一些事实：我们假设 $b \in \mathbb{Q}_p^\times$ 不是平方元，那么我们总是可以构造一个更大的域 $L \supset \mathbb{Q}_p$ 如下：

$$L = \{(x,y) : x, y \in \mathbb{Q}_p\}$$

其上的加法和乘法的定义分别为

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$(x_1, y_1)(x_2, y_2) = (x_1x_2 + by_1y_2, x_1y_2 + x_2y_1)$$

实际上这里 $\beta = (0, 1)$ 就起到了 $\sqrt{b}$ 的作用。任何 L 中的元素都可以写成 $x + y\beta$，其中 $x, y \in \mathbb{Q}_p$。我们也写 $L = \mathbb{Q}_p(\sqrt{b})$ 是二次扩张。

将元素乘以 $x + y\beta$ 是从 L 到 L 的 $\mathbb{Q}_p$-线性映射，我们可以考虑这个线性映射的行列式 $N_b(x + y\beta) = x^2 - by^2$，那么 N_b 是从 $L - \{0\}$ 到 $\mathbb{Q}_p^\times$ 的乘法群同态，这个群同态的像 $\mathrm{Im}N_b$ 中的元素可以解读为

$$\mathrm{Im}N_b = \{a \in \mathbb{Q}_p^\times : (a,b)_p = 1\}$$

到目前为止，我们仅仅是把 Hilbert 符号的定义重写了一遍，这里的 N_b 被叫做域扩张 $L/\mathbb{Q}_p$ 的范，若 $a \in \mathbb{Q}_p$ 落在 N_b 的值域内我们就说 a 是扩展 $L/\mathbb{Q}_p$ 的范元素。我们知道：

"a 是平方元，当且仅当它是 $\mathbb{Q}_p$ 的所有二次（循环）扩张的范元素"

类似的结论可以推广到 n 次根，这里的域 $\mathbb{Q}_p$ 可以换成局部域，在推广的时候，Hilbert 符号的定义就要用到 $K^\times/(K^\times)^n \simeq \mathrm{Gal}_K^{K(\sqrt[n]{K})}$

对于局部域的 Abelian 扩张 L/K，我们有 $\mathrm{Gal}_K^L \simeq K^\times/N_K^L(L^\times)$，因此 $K^\times$ 的结构可以反映 K^{ab}/K 的结构，参见：Artin 互反律，局部类域论