目录

第一章　p 进数基础

1.1　绝对赋值与超度量空间

1.1.1　导言

什么？...9999=-1?? $\sum_{k=1}^{\infty} 5^{k-1} = -\frac{1}{4}$?? 所有的三角形都是等腰三角形？每一个开球都是闭集?? 有理数集 $\mathbb{Q}$ 完备化得到的可以不是 $\mathbb{R}$??

这些看似非常反直觉的结论，在本篇文章的主角——p-adic 数（p 进数）的背景下都是成立的，现在我们正式走入 p 进数的世界 ~

1.1.2　p 进赋值与域上的绝对赋值

定义 1.1. 对于给定的素数 p，在 $\mathbb{Q}$ 上定义范数 $\|\cdot\|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ ，对任意的 $x \in \mathbb{Q}\backslash\{0\}$ ，有

$$\|x\|_p = p^{-v_p(x)}.$$

这里的 $v_p(x)$ 指的是整数 x 的素因子分解时 p 的幂次，并延拓至有理数：对于 $x = \frac{a}{b}(a, b \in \mathbb{Z})$ 有 $v_p(x) = v_p(a) - v_p(b)$ 。同时约定 $\|0\|_p = 0$ ，称上述范数为 p 进赋值。

直观上讲，对固定的 p ，$\|x\|_p$ 越小意味着其被 p 整除的次数越高。根据定义，我们能够感觉到如上定义的范数和数论中的一些性质应该是密切相关的，我们将在之后的文章里阐述这一点（目前还得做一些准备工作）。现在我们考虑该范数的一些性质：

$$(1)\|x\|_p = 0 \iff x = 0$$

$$(2)\|x\|_p\|y\|_p = \|xy\|_p$$

$$(3)\|x + y\|_p \leq \max\{\|x\|_p, \|y\|_p\}$$

这里 (1)(2) 都是自然的，性质 (3) 可以通过初等数论里的一个简单结论 $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$ 得出。这是一个比一般的三角不等式更强的结论，在这样的范数下，两个数之和的 “长度” 不会超过这两个数中 “长度” 更大的那个。在这样的度量空间中，会出现许多与我们平常习惯的绝对值度量完全不同的性质。

此外，若 $v_p(x) \neq v_p(y)$ ，则 $v_p(x+y) = \min\{v_p(x) + v_p(y)\}$ ，从而我们可以加上第 (4) 条性质：

$$(4)若\|x\|_p \neq \|y\|_p, 则\|x+y\|_p = \max\{\|x\|_p, \|y\|_p\}$$

事实上，前三条性质蕴含了 (4)，我们后面将在更一般的情形下证明这一点。

接下来我们可以解答导言中的前两个等式了。这两个等式左边都可以看作无穷求和，故可以通过求部分和再取极限的方式定义，我们断言在刚刚定义的范数 $\|\cdot\|$ 的意义下，左边确实可以收敛至右边。例如取 $p = 5$ ，考虑级数 $\sum_{k=1}^{\infty} 5^{k-1}$ ，其部分和定义为

$$S_N = \sum_{k=1}^{N} 5^{k-1} = \frac{1-5^N}{1-5} = \frac{5^N - 1}{4}$$

从而

$$\|S_N - (-\frac{1}{4})\|_5 = \|\frac{5^N}{4}\|_5 = 5^{-N}$$

这说明对任意的 $\epsilon > 0$ ，存在 $N_0 > -\log_5 \epsilon$ ，使得 $N > N_0$ 时有

$$\|S_N - (-\frac{1}{4})\|_5 = 5^{-N} < \epsilon$$

由极限的定义，我们可以说级数 $\sum_{k=1}^{\infty} 5^{k-1}$ 在 $\|\cdot\|_\infty$ 范数意义下收敛至 $-\frac{1}{4}$ ！至于在这种范数下的级数的性质和收敛的意义，我们将在之后的文章中深入研究。

接下来我们考虑将 p 进赋值推广至更一般的情形。

定义 1.2. 设 $\mathbf{k}$ 是任意的一个域（这里为什么要强调是域？因为后面我们将要以代数的视角去研究），称 $\mathbf{k}$ 上的一个函数

$$|\cdot| : \mathbf{k} \to \mathbb{R}_{\geq 0}$$

为绝对赋值的，如果其满足以下条件：

(1) 对任意的 $x \in \mathbf{k}$ ， $|x| = 0 \iff x = 0$

(2) 对任意的 $x, y \in \mathbf{k}$ ， $|xy| = |x||y|$

(3) 对任意的 $x, y \in \mathbf{k}$ ， $|x+y| \leq |x| + |y|$

若进一步地，该绝对赋值满足 $|z+y| \leq \max\{|z|, |y|\}$ ，则称其是一个非阿基米德赋值。可以看出这对应着 p 进赋值中的强三角不等式（也叫超度量不等式），也是一条比 (3) 更强的性质。若一个绝对赋值仅仅满足前三条而不满足强三角不等式，则称其为阿基米德赋值（我们日常所习惯的绝对值计算就属于这种情形）。

至于这里的定义为什么和阿基米德有关，我们可以回忆起实数理论中的阿基米德性质：对于任意的 $z, y \in \mathbb{R}$ ，存在正整数 n ，使得 $|nz| > |y|$ 。直观来讲就是一个数是可

以 “越加越大” 的。然而可以看出这个性质在满足超度量不等式的绝对赋值里是不成立的，因为这里的数 “越加越小”。在这种赋值里，很多性质都和我们平常所习惯的绝对值完全不同，一些性质甚至会违反直觉、颠覆认知。不过在熟悉这种赋值的过程中，我们会逐渐感到它们的精妙之处。

我们接着考察非阿基米德赋值的一些性质。

命题 1.1. 对于域 $\mathbf{k}$ 上的一个绝对赋值，则以下几条性质是等价的：

(1) 对任意的 $z, y \in \mathbf{k}$ ， $|z+y| \leq \max\{|z|, |y|\}$

(2) 对于任意的正整数 n ， $|n \cdot 1| \leq 1$ （这里的 $n \cdot 1$ 指的是 n 个乘法单位 1 相加）

(3) 对于任意的 $z \in \mathbf{k}$ ， $|z+1| \leq \max\{|z|, 1\}$

(4) 若 $|z| \neq |y|$ ，则 $|z+y| = \max\{|z|, |y|\}$

证明. (1) $\Rightarrow$ (2) 是显然的；

(2) $\Rightarrow$ (3)： 对任意的正整数 m ，和 $z \in \mathbf{k}$ ，我们有

$$|z+1|^m = |(z+1)^m| = \left|\sum_{k=0}^{m} \binom{m}{k} z^k\right| \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |z|^k = \sum_{k=0}^{m} |\binom{m}{k} \cdot 1||z|^k \leq \sum_{k=0}^{m} |z|^k$$

若 $|z| > 1$ ，则 $\sum_{k=0}^{m} |z|^k \leq (m+1)|z|^m$ ；若 $|z| \leq 1$ ，则 $\sum_{k=0}^{m} |z|^k \leq m+1$ ，从而

$$|z+1|^m \leq \sum_{k=0}^{m} |z|^k \leq (m+1)\max\{1, |z|^m\}$$

两边同时开 m 次方有 $|z+1| \leq \sqrt[m]{m+1}\max\{1, |z|\}$ ，再令 $m \to \infty$ 即得

$$|z+1| \leq \max\{|z|, 1\}$$

这便证明了 (3)。

(3) $\Rightarrow$ (4)： 不妨设 $|z| > |y|$ ，则

$$|z+y| = |z|\left|1 + \frac{y}{z}\right| \leq |z| \max\left\{1, \left|\frac{y}{z}\right|\right\} = \max\{|z|, |y|\} = |z|$$

另一方面，由于 $z = (z+y) - y$ ，故

$$|z| = |(z+y) - y| = |z+y|\left|1 - \frac{y}{z+y}\right| \leq |z+y| \max\left\{1, \left|\frac{y}{z+y}\right|\right\} = \max\{|z+y|, |y|\}$$

又因为 $|z| > |y|$ ，所以 $|z| \leq |z+y|$ ，进而我们得到了 $|z+y| = |z|$ ，这就证明了 (4)。

(4) $\Rightarrow$ (1)： 若 $|z| \neq |y|$ ，则 $|z+y| = \max\{|z|, |y|\} \leq \max\{|z|, |y|\}$ ；若 $|z| = |y|$ ，我们用反证法，假设 $|z+y| > |z|$ ，则 $|z+y| > |-z|$ ，故由 (4) 的性质

$$|y| = |(z+y) + (-z)| = |z+y|$$

这和 $|z| = |y| < |z+y|$ 矛盾！从而 $|z+y| \leq |z|$ ，即 $|z+y| \leq \max\{|z|, |y|\}$ 。这便证明了 (1)。

综上所述，命题得证。 □

这说明只要上述四条性质任意一条得到证明，便可以说该赋值是非阿基米德的，且剩下三条性质也成立。

同时我们可以在 $\mathbf{k}$ 上定义度量 $d(x,y)=|x-y|$ 。若绝对赋值是非阿基米德的，我们称配备了该度量的空间为超度量空间（$(\mathbf{k},d)$ ）。在超度量空间中，有一个比较神奇的性质是：

命题 1.2. 在超度量空间中，所有的三角形都是等腰三角形。即对任意的 $x,y,z\in\mathbf{k}$

$$d(x,y),\ d(y,z),\ d(z,x)$$

这三个值至少有两个相等。

证明. 若 $d(x,y)=d(y,z)$ ，则命题自动成立；若 $d(x,y)\neq d(y,z)$ ，则

$$d(x,z)=|(x-y)+(y-z)|=\max\{d(x,y),d(y,z)\}$$

综上所述命题成立。 □

1.1.3 超度量空间上的拓扑性质

在超度量空间上，我们可以定义度量诱导的拓扑，这里的拓扑结构和 $\mathbb{R}$ 上的标准拓扑有非常大的区别。

定义 1.3. 在度量空间 $(\mathbf{k},d)$ 上，我们按如下方式定义开球和闭球：

$$B(a,r)=\{x\in\mathbf{k}:d(x,a)<r\},\qquad \overline{B}(a,r)=\{x\in\mathbf{k}:d(x,a)\leq r\}$$

称集合 $U\subset\mathbf{k}$ 为 $\mathbf{k}$ 上的开集，如果对任意的 $z\in U$ ，存在 $\epsilon>0$ ，使得 $B(x,\epsilon)\subset U$（这其实是我们熟知的定义）。若集合 $F\subset\mathbf{k}$ 在 $\mathbf{k}$ 上的补集为开集，则称 F 为 $\mathbf{k}$ 上的闭集。

在 $\mathbb{R}$ 上的标准拓扑中，我们熟知开球（开区间）是开集，闭球是闭集，$\overline{B}(a,r)$ 就是 $B(a,r)$ 的闭包。然而在超度量空间上，开球的闭包并不一定等于对应的闭球，甚至每一个开球和闭球既是开集又是闭集！

命题 1.3. 在超度量空间 $(\mathbf{k},d)$ 上有如下拓扑性质：

(1) 若 $b\in B(a,r)$ ，则 $B(a,r)=B(b,r)$（这说明开球里的任意一点都是开球的球心）。

(2) 若 $b\in\overline{B}(a,r)$ ，则 $\overline{B}(a,r)=\overline{B}(b,r)$ 。这里的证明和 (1) 是类似的。

(3) 开球 $B(a,r)$ 是既开又闭的，进而其边界为空集。

(4) 若 $r\neq 0$ ，则 $\overline{B}(a,r)$ 是既开又闭的。这里的证明和 (3) 是类似的。

(5) 若 $a,b\in\mathbf{k},r,s\in\mathbb{R}_+$ ，则 $B(a,r)\cap B(b,s)\neq\emptyset$ 当且仅当 $B(a,r)\subset B(b,s)$ 或 $B(b,s)\subset B(a,r)$ 。换句话说，两个开球要么不交，要么其中一个被另一个完全包含。若把两个开球都换成闭球，结论也是一样的。

证明. (1) 对任意的 $x\in B(a,r)$ ，有 $d(a,x)<r$ ，从而

$$d(b,x)\leq\max\{d(a,x),d(a,b)\}<r$$

故 $B(a,r)\subset B(b,r)$。反过来对任意的 $x\in B(b,r)$ ，有 $d(b,x)<r$ ，从而

$$d(a,x)\leq\max\{d(b,x),d(a,b)\}<r$$

故 $B(b,r)\subset B(a,r)$ ，进而有 $B(a,r)=B(b,r)$ 。我们也可以看到强三角不等式在证明中发挥的作用。

(3) 只需证明 $\mathbf{k}\backslash B(a,r)$ 是开集即可。取 $y\notin B(a,r)$ ，则 $d(a,y)\geq r$ ，取 $\epsilon=r$ ，我们断言 $B(y,\epsilon)\subset\mathbf{k}\backslash B(a,r)$ 。事实上，对任意的 $z\in B(y,\epsilon)$ ，有 $d(y,z)<\epsilon=r$。若 $z\in B(a,r)$ ，则 $d(a,z)<r$ ，从而

$$d(a,y)\leq\max\{d(a,z),d(z,y)\}<r$$

矛盾。因此 $z\in\mathbf{k}\setminus B(a,r)$ ，这就证明了 $B(y,\epsilon)\subset\mathbf{k}\setminus B(a,r)$ ，故 $\mathbf{k}\setminus B(a,r)$ 是开集，进而 $B(a,r)$ 是闭集。

(5) 若 $r\leq s$ ，且存在 $c\in B(a,r)\cap B(b,s)$ ，则由性质 (1) 我们可以得到

$$B(a,r)=B(c,r)\subset B(c,s)=B(b,s)$$

若 $r>s$ ，同理有 $B(b,s)\subset B(a,r)$ 。这就证明了 (5)。 □

在研究进一步的拓扑性质前，我们看一些具体的例子。假设在有理数集 $\mathbb{Q}$ 上赋予 p 进度量 $|\cdot|_p$ ，考虑

$$B(0,1)=\{z:|z|_p<1\}$$

这表示最简形式中，分子被 p 整除的所有有理数。此外可以注意到

$$B(0,1)=\bigcup_{k=0}^{p-1}B(kp,1/p)$$

这是 p 个开球的不交并，每一个小球也可以继续分解。我们发现这里似乎蕴含着一种和康托三分集类似的分形结构！下面我们要研究的拓扑性质也与其有关系。

我们回忆一下不连通集的概念。

定义 1.4. 设 (X,τ) 是拓扑空间，$S\subset X$ ，若存在 X 中的开集 U,V 满足

(1) $U\cap S\neq\emptyset$, $V\cap S\neq\emptyset$

(2) $U \cap V \cap S = \emptyset$

(3) $S \subset U \cup V$

则称 S 是不连通的。进一步，若 X 上的连通子集仅有单点集（严谨一些的话也可以把空集算上去），则称 X 是完全不连通的。

我们熟知 $\mathbb{Q}$ 在标准拓扑下是完全不连通的，而 $\mathbb{R}$ 是连通的。现在我们考虑超度量空间 $(\mathbf{k}, d)$。

定理 1.1. 若域 $\mathbf{k}$ 上配备了超度量距离，则 $\mathbf{k}$ 在该距离诱导的拓扑下是完全不连通的。

证明. 设 S 是 $\mathbf{k}$ 的子集，若 S 包含两个不同的点 x, y ，则记 $r = d(x, y) > 0$ ，并考虑 $U = B(x, r)$ 和 $V = \mathbf{k} \setminus B(x, r)$ ，易知它们是开集。显然有 $x \in U, y \in V$ ，这表明 U, V 都是非空开集，所以 S 是不连通的，进而 $\mathbf{k}$ 是完全不连通的。 □

回忆起康托尔三分集也是完全不连通的，在之后的文章里我们将讨论其与 p 进数域 $\mathbb{Q}_p$ 的联系（埋个坑）。

最后我们以一个有用的推论结束本文。

推论 1.1. 设 $\mathbf{k}$ 是超度量空间，$\mathbb{R}$ 是配备了通常的绝对值的实数集，$f : \mathbb{R} \to \mathbf{k}$ 是一个连续函数，则必有 f 是常值函数。

证明. 只需要利用连续函数的性质：f 把连通集映射成连通集，又因为 $\mathbf{k}$ 上的非空连通集只能是单点集，故 f 是常值函数，得证! □

（p 进分析真的好有意思!）

1.2 有理数 $\mathbb{Q}$ 的完备化与 Ostrowski 定理

本篇文章我们考虑 p 进分析中第一个核心问题——有理数集 $\mathbb{Q}$ 有哪些完备化方式，以及具体是如何完备化的。

1.2.1 度量空间的完备化

我们首先回顾一下 $\mathbb{Q}$ 是如何通过完备化得到 $\mathbb{R}$ 的：令 $\mathbb{Q}$ 配备通常的绝对值度量，记 $\mathbb{Q}$ 中在该度量下的所有柯西列的集合为 $C(\mathbb{Q})$，即

$$C(\mathbb{Q}) = \{\{z_n\} \subset \mathbb{Q} : \{z_n\}\text{是柯西列}\}$$

在 $C(\mathbb{Q})$ 上赋予如下的等价关系：

$$[z_n] \sim [y_n] \iff \lim_{n\to\infty} |z_n - y_n| = 0$$

容易验证这的确是一个等价关系。接着我们令 $\hat{\mathbb{Q}}$ 为这些等价类构成的集合，定义其上的度量为

$$d([z_n],[y_n]) = \lim_{n\to\infty} |z_n - y_n|$$

这里的 $[z_n],[y_n]$ 指的是分别以 $\{z_n\},\{y_n\}$ 为代表元的等价类。

这个 $\hat{\mathbb{Q}}$ 看上去和我们想象中的 $\mathbb{R}$ 相去甚远，我们想象中的 $\mathbb{R}$ 更接近于戴德金分割构造出的，然而实际上它们是等距同构（存在一个保持距离不变的双射）的，这里就不展开写了。

更一般地，对任意一个度量空间 X，我们都可以类似上文在柯西列集合上定义等价关系的方法将 X 完备化得到 $\hat{X}$ ，且 $\hat{X}$ 在等距同构意义下唯一。此外存在一个等距嵌入 $\phi : X \to \hat{X}$ 使得 $\phi(X)$ 在 $\hat{X}$ 中稠密（例如 $\mathbb{Q}$ 在 $\mathbb{R}$ 中稠密）。

我们对上述对度量空间完备化的方法做出如下的观察：

(1) 度量空间的完备化是由其配备的度量（赋值）决定的，配备了不同的度量可能导致完备化的空间有不同的结构。这启发我们寻找 $\mathbb{Q}$ 上不同的度量，可能会得到与 $\mathbb{R}$ 完全不同的完备化空间。

(2) 这种完备化的方法是一种“抽象”的构造方法，它保证了完备化的可行性、唯一性和原空间的稠密性，但是难以揭示某个特定的完备化之后的空间的具体性质，完备化之后的空间到底多了哪些东西？这个时候我们就需要一些具体的构造方法对其进行进一步的研究，例如通过戴德金分割构造无理数、通过定义勒贝格积分得到 L^p 空间等。在之后对 p 进数域的研究中，我们也会用 p 进级数的形式刻画里面的每一个元素。

有了这两点作为动机，我们继续研究 $\mathbb{Q}$ 的完备化。

1.2.2 $\mathbb{Q}$ 上的赋值类型

$\mathbb{Q}$ 上的绝对赋值有无穷多种，我们得先进行一次简单的分类，看看哪些赋值是“相似”的。

定义 1.5. 称 $\mathbb{Q}$ 上两个绝对赋值 $|\cdot|_1$ 和 $|\cdot|_2$ 是等价的，如果它们在 $\mathbb{Q}$ 上诱导了相同的拓扑。换言之，$\mathbb{Q}$ 的子集 U 在 $|\cdot|_1$ 诱导的拓扑下是开集当且仅当 U 在 $|\cdot|_2$ 诱导的拓扑下是开集。

这样定义之后我们可以保证 $\mathbb{Q}$ 在这两种赋值下得到的完备化空间具有相同的拓扑结构。

上述的定义有如下几条等价定义：

(1) $\mathbb{Q}$ 上的序列 $\{x_n\}$ 在度量 d_1 下收敛到 x $\iff$ 在度量 d_2 下收敛到 x。

(2) 对任意的 $x \in \mathbb{Q}$ ，$|x|_1 < 1 \iff |x|_2 < 1$。

(3) 存在正实数 α ，使得 $|x|_1 = |x|_2^\alpha$ 对一切 $x \in \mathbb{Q}$ 成立。

等价性的证明. (3) $\Rightarrow$ (1)：序列收敛到 0 可以等价的叙述为对任何包含 0 的开集 U ，$\{x_n\}$ 中只有有限项不在 U ，而等价的赋值诱导了相同的拓扑，故得证。

(1) $\Rightarrow$ (2)：若 $|x|_2 < 1$ ，则序列 x^n 在度量 d_2 下收敛到 0。由 (1) 序列在度量 d_1 下也收敛到 0，这表明 $|x|_1 < 1$。同理若 $|x|_2 > 1$ ，也有 $|x|_1 > 1$ ，故得证。

(2) $\Rightarrow$ (3)：这是唯一一个比较难证明的方向。首先若 $|\cdot|_1$ 是平凡的（非零点的赋值都为 1），则 $|\cdot|_2$ 也是平凡的，反之亦然。此时任取一个正实数 α 都成立。

以下考虑它们都是非平凡的赋值。此时存在 y 使得 $|y|_1 \neq 1$。对任意的 $x \neq 0$ 和正整数 m, n ，注意到

$$|x|_1 < |y|_1^{\frac{m}{n}} \iff \left|\frac{x^n}{y^m}\right|_1 < 1 \iff \left|\frac{x^n}{y^m}\right|_2 < 1 \iff |x|_2 < |y|_2^{\frac{m}{n}}.$$

两边取自然对数有

$$\frac{\ln|x|_1}{\ln|y|_1} < \frac{m}{n} \iff \frac{\ln|x|_2}{\ln|y|_2} < \frac{m}{n}.$$

若 $\frac{\ln|x|_1}{\ln|y|_1} \neq \frac{\ln|x|_2}{\ln|y|_2}$ ，不妨设 $\frac{\ln|x|_1}{\ln|y|_1} > \frac{\ln|x|_2}{\ln|y|_2}$ ，则根据有理数的稠密性存在有理数 $\frac{m}{n}$ ，使得

$$\frac{\ln|x|_1}{\ln|y|_1} > \frac{m}{n} > \frac{\ln|x|_2}{\ln|y|_2},$$

矛盾！从而对任意的 x ，都有 $\frac{\ln|x|_1}{\ln|y|_1} = \frac{\ln|x|_2}{\ln|y|_2}$ ，记 $\alpha = \frac{\ln|y|_1}{\ln|y|_2}$ ，则 $|x|_1 = |x|_2^\alpha$ ，得证！ □

接着我们证明一个非常优美且重要的定理，它告诉我们 $\mathbb{Q}$ 上的绝对赋值可以分为两类，从而也只有这两条完备化的方向。

定理 1.2 (Ostrowski). $\mathbb{Q}$ 上的非平凡赋值要么和 $|\cdot|_\infty$ （即通常的绝对值）等价，要么和某个 $|\cdot|_p$ 等价（其中 p 为素数）。

证明. 根据绝对赋值的乘性和定义中的 (3)，我们只需证明在 $\mathbb{Z}$ 上等价，即对任意的 $n \in \mathbb{Z}$ ，有 $|n| = |n|_\infty^\alpha$ 或者 $|n| = |n|_p^\alpha$ 。

情形一：该赋值是阿基米德赋值。我们记 n_0 是满足 $|n| > 1$ 的最小正整数（n_0 的存在性可由阿基米德性质保证），同时存在 $\alpha > 0$ 使得 $|n_0| = n_0^\alpha$ 。

接下来对任意的正整数 n ，我们考虑 n 的 n_0 进制展开：

$$n = \sum_{j=0}^{k} a_j n_0^j, \quad 0 \leq a_j < n_0,\ a_k \neq 0.$$

则由三角不等式

$$|n| = \left|\sum_{j=0}^{k} a_j n_0^j\right| \leq \sum_{j=0}^{k} |a_j||n_0|^j \leq \sum_{j=0}^{k} |n_0|^j < \frac{n_0^{(k+1)\alpha}}{n_0^\alpha - 1}.$$

令 $C=\frac{n_0^\alpha}{n_0^\alpha-1}$ ，则 $|n|\le Cn_0^{k\alpha}\le Cn^\alpha$ ，于是对任意的正整数 N ，有 $|n^N|\le Cn^{N\alpha}$ 。两边开 N 次方根得到 $|n|\le\sqrt[N]{C}\,n^\alpha$ ，从而令 $N\to\infty$ 得 $|n|\le n^\alpha$ 。

另一方面，由于 $n_0^{(k+1)}>n\ge n_0^k$ ，所以 $n_0^{(k+1)\alpha}=|n_0^{(k+1)}|\le|n|+|n_0^{(k+1)}-n|$ ，进而有

$$|n|\ge n_0^{(k+1)\alpha}-|n_0^{k+1}-n|\ge n_0^{(k+1)\alpha}-(n_0^{k+1}-n)^\alpha>C'n^\alpha.$$

于是同理有 $|n|\ge n^\alpha$ ，这说明 $|n|=n^\alpha$ ，从而该赋值和通常的绝对值 $|\cdot|_\infty$ 等价。

情形二：该赋值是非阿基米德赋值，则对任意的正整数 n ，有 $|n|\le1$ 。由于该赋值非平凡，故存在一个最小的 n_0 满足 $|n_0|<1$ 。

我们断言 n_0 必然是某个素数 p ，事实上若 $n_0=ab$ ，$1<a,b<n_0$ ，则由 n_0 的最小性，$|a|=|b|=1$ ，但此时 $|n_0|=|a||b|=1$ ，矛盾！这就证明了 n_0 必然是某个素数 p 。

再证明对任意的不被 p 整除的整数 n ，作带余除法 $n=rp+s$ ，其中 $1\le s\le p-1$ 。由于 $|rp|=|r||p|\le|p|<1$ ，$|s|=1$ ，结合强三角不等式有

$$|n|=|rp+s|=\max\{|rp|,|s|\}=1.$$

最后对任意的 $n\in\mathbb{Z}$ ，将 n 写成 $n=p^{v_p(n)}\cdot n'$ ，其中 $p\nmid n'$ ，则

$$|n|=|p|^{v_p(n)}=(p^{-\alpha})^{v_p(n)}=|n|_p^\alpha,$$

这里 α 满足 $p^{-\alpha}=|p|<1$ ，故 α 是正实数，从而该赋值和 p 进赋值 $|\cdot|_p$ 等价。

综上所述，定理得证！ □

若我们在 $\mathbb{Q}$ 上定义 p 进赋值 $|\cdot|_p$ ，则可以通过柯西列对 $\mathbb{Q}$ 完备化得到 $\mathbb{Q}_p$ 。

1.3 细探 $\mathbb{Q}_p$

1.3.1 $\mathbb{Q}_p$ 中的元素组成

在通过 p-adic 对 $\mathbb{Q}$ 完备化得到 $\mathbb{Q}_p$ 后，我们自然关心 $\mathbb{Q}_p$ 的元素构成及其上面的结构。接下来我们用分析和代数两种视角进行探究。

首先我们定义 p-adic 整数环:

$$\mathbb{Z}_p=\{x\in\mathbb{Q}_p:|x|_p\le1\}$$

容易看出这是一个主理想整环，且 (p) 是其唯一的极大理想，从而 $\mathbb{Z}_p$ 在 p 处的局部化就是 $\mathbb{Z}_p$ 的分式域，即

$$\mathbb{Z}_p[1/p]=\mathrm{Frac}(\mathbb{Z}_p)=\mathbb{Q}_p$$

这表明对任意的 $x\in\mathbb{Q}_p$ ，其可被唯一写成 $\frac{u}{p^m}$ 的形式，其中 $m\ge0,u\in\mathbb{Z}_p$

我们考虑 p-adic 度量下的嵌入映射 $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ ，其在 $\mathbb{Z}_p$ 中有稠密的像，即对于任意的 $x \in \mathbb{Z}_p$ 和 $n \geq 1$ 存在模 p 意义下唯一的整数 α 使得 $|x-\alpha|_p \leq p^{-n}$ （这由 $\mathbb{Q}$ 在 $\mathbb{Q}_p$ 中稠密可以得出)。从而有推论：

对任意的 $x \in \mathbb{Z}_p$ ，存在柯西列 $\{x_n\}$ 收敛于 x ，这里 $\{x_n\}$ 满足 $x_{n+1} \equiv x_n \pmod{p^n}$ 且每个 x_n 在模 p^n 意义下唯一。这便以分析的视角刻画了 $\mathbb{Z}_p$ 。

接下来我们考虑如下的投射系统：集簇 $\{A_n\}$ 和投影同态 $\phi_{m,n}$ 。其中 $A_n = \mathbb{Z}/p^n\mathbb{Z}$ ，$\phi_{m,n}$ 定义为自然同态，即 $m \geq n$ 时，有

$$\phi_{m,n} : A_m \to A_n, \quad x \pmod{p^m} \mapsto x \pmod{p^n}$$

容易验证 $\phi_{n,n} = \mathrm{id}_{A_n}$ ，且对任意的 $m \geq n \geq l$ 有 $\phi_{m,l} = \phi_{m,n} \circ \phi_{n,l}$ ，于是我们可以定义该投射系统的极限（也叫逆向极限）为：

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{\{x_n\} \in \prod_{n\geq 1} A_n : \phi_{n,m}(x_n) = x_m\}$$

（这里逆向极限的定义在之后的无穷 Galois 理论里也会遇到）

这里定义出来的 $\mathbb{Z}_p$ 中的元素恰好对应着上面提及的柯西列 $\{x_n\}$ ，从而这两种对 $\mathbb{Z}_p$ 的刻画是一致的。这也表明对每一个 $x \in \mathbb{Z}_p$ ，其可被唯一表示成如下 p-adic 级数的形式：

$$x = \sum_{n=0}^{\infty} a_n p^n, \quad 0 \leq a_n \leq p-1$$

最后因为 $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$ ，所以对每一个 $x \in \mathbb{Q}_p$ ，其可被唯一写成如下的形式：

$$x = \sum_{n=-k}^{\infty} a_n p^n, \quad 0 \leq a_n \leq p-1$$

1.3.2 Hensel 引理

在给出了 $\mathbb{Q}_p$ 中元素的表示形式后，我们接着考虑如何判断一个元素是否在 $\mathbb{Q}_p$ 中，比如 $\sqrt{2}$ 是否在 $\mathbb{Q}_7$ 中。注意这里的 $\sqrt{2}$ 和我们平常所认为的 $\sqrt{2}$ 不同，而指的是多项式 x^2-2 的根。在 $\mathbb{R}$ 中解这个方程自然得到实数 $\sqrt{2}$ ，那么在 $\mathbb{Q}_7$ 中是否也有根呢? 这就需要用到一个强有力的工具——Hensel 引理。

定理 1.3 (Hensel 引理)**.** 设 $f(x) \in \mathbb{Z}_p[x]$ ，若存在 $\alpha_0 \in \mathbb{Z}_p$ 使得

$$f(\alpha_0) \equiv 0 \pmod{p}, \quad f'(\alpha_0) \not\equiv 0 \pmod{p}$$

则存在唯一的 $\alpha \in \mathbb{Z}_p$ 使得 $f(\alpha) = 0$ ，且 $\alpha \equiv \alpha_0 \pmod{p}$。

证明. 我们构造按如下的递推序列 $\{\alpha_n\}$

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

并用数学归纳法证明对任意的 $n \geq 0$ ，有 $f(\alpha_n) \equiv 0 \pmod{p^{n+1}}$ 且 $f'(\alpha_n) \not\equiv 0 \pmod{p}$。

归纳的初始条件是自动成立的，现假设对 n 成立，记 $h_n = -\frac{f(\alpha_n)}{f'(\alpha_n)}$ ，则 $v_p(h_n) \geq n+1$ ，于是有 $\alpha_{n+1} \equiv \alpha_n \pmod{p^{n+1}}$ ，所以 $f'(\alpha_{n+1}) \not\equiv 0 \pmod{p}$ 。接着考虑 $f(\alpha_{n+1})$ 在 α_n 处的泰勒展开，有

$$f(\alpha_n + h_n) = f(\alpha_n) + f'(\alpha_n)h_n + h_n^2 Q$$

其中 $Q = \sum_{i=2}^{\deg f} f^{(i)}(\alpha_n) h_n^{i-2} \in \mathbb{Z}_p$ ，将 $h_n = -\frac{f(\alpha_n)}{f'(\alpha_n)}$ 代入得 $f(\alpha_{n+1}) = h_n^2 Q$ ，注意到

$$v_p(h_n^2 Q) \geq 2v_p(h_n) \geq 2(n+1) \geq n+2$$

所以有 $f(\alpha_{n+1}) \equiv 0 \pmod{p^{n+2}}$ 。由归纳假设，我们构造出来的序列 $\{\alpha_n\}$ 是一个 $\mathbb{Z}_p$ 中的柯西列，从而存在唯一的 $\alpha \in \mathbb{Z}_p$ 使得 $\alpha_n \to \alpha$ 。又因为 $|f(\alpha_n)|_p \leq p^{-(n+1)}$ ，所以令 $n \to \infty$ 即可得到 $f(\alpha) = 0$ 。 □

这便证明了 Hensel 引理。回到 $\sqrt{2}$ 是否在 $\mathbb{Q}_7$ 中这个问题，令 $f(x) = x^2 - 2$ ，则

$$f(3) \equiv 0 \pmod{7}, \quad f'(3) \not\equiv 0 \pmod{7}$$

由 Hensel 引理，$\sqrt{2} \in \mathbb{Z}_7$ ，进而也在 $\mathbb{Q}_7$ 中。

我们注意到这里 $\{\alpha_n\}$ 的构造和求 $\mathbb{R}$ 上方程的近似解时所用的牛顿切线迭代法是类似的，每一次迭代都可以提高近似解的精度，从而逼近精确解。

此外这里的 Hensel 引理并不是一个判断解是否存在的充分必要条件。例如考虑 $f(x) = x^p - 1$ ，此时 $f'(x) = px^{p-1} \equiv 0 \pmod{p}$ ，但是显然 $1 \in \mathbb{Q}_p$ 且 $f(1) = 0$ 。事实上我们可以将 Hensel 引理稍加修改得到如下的版本：

定理 1.4 (推广版本)**.** 设 $f(x) \in \mathbb{Z}_p[x]$ ，若存在 $\alpha_0 \in \mathbb{Z}_p$ 使得

$$|f(\alpha_0)|_p < |f'(\alpha_0)|_p^2$$

则存在唯一的 $\alpha \in \mathbb{Z}_p$ 使得 $f(\alpha) = 0$ ，且 $|\alpha - \alpha_0|_p \leq \frac{|f(\alpha_0)|_p}{|f'(\alpha_0)|_p}$。

证明. 此时和经典版本类似，令 $h_n = -\frac{f(\alpha_n)}{f'(\alpha_n)}$ ，利用数学归纳法，假设已经有

$$|f(\alpha_n)|_p < |f'(\alpha_n)|_p^2, \quad |f'(\alpha_n)|_p = |f'(\alpha_0)|_p$$

则

$$|h_n|_p = \frac{|f(\alpha_n)|_p}{|f'(\alpha_n)|_p} < \frac{|f'(\alpha_n)|_p^2}{|f'(\alpha_n)|_p} = |f'(\alpha_n)|_p$$

对 $f'(\alpha_{n+1})$ 在 α_n 处进行泰勒展开有

$$|f'(\alpha_{n+1}) - f'(\alpha_n)|_p \leq |h_n|_p < |f'(\alpha_n)|_p$$

这表明 $|f'(\alpha_{n+1})|_p = |f'(\alpha_n)|_p = |f'(\alpha_0)|_p$ 。同时对 $f(\alpha_{n+1})$ 在 α_n 处进行泰勒展开有

$$|f(\alpha_{n+1})|_p \leq |h_n|_p^2 \leq \frac{|f(\alpha_n)|_p^2}{|f'(\alpha_n)|_p^2} < |f(\alpha_n)|_p$$

进而得到

$$|f(\alpha_{n+1})|_p < |f(\alpha_n)|_p < |f'(\alpha_n)|_p^2 = |f'(\alpha_{n+1})|_p^2$$

由数学归纳法知 $\{h_n\}$ 和 $\{f(\alpha_n)\}$ 的幂次是严格递增的，故 $\{\alpha_n\}$ 是 $\mathbb{Z}_p$ 中的柯西列收敛至唯一的 $\alpha \in \mathbb{Z}_p$ ，且 $f(\alpha) = 0$。

注意到当 $f'(\alpha_0) \not\equiv 0 \pmod{p}$ 时，$|f'(\alpha_0)|_p \geq 1$ ，故 $f(\alpha_0)$ 只需满足 $|f(\alpha_0)|_p < 1$ ，即 $f(\alpha_0) \equiv 0 \pmod{p}$ ，这便退化成 Hensel 引理经典版本。然而推广之后的版本也不能成为判断根是否存在的充要条件，事实上情况比这复杂得多。 □

尽管如此，Hensel 引理涵盖了大部分的情形，且其更深远的意义在于为局部——整体原则提供了强有力的判断工具。这里局部——整体原则在 $\mathbb{Q}$ 上的体现是 $\mathbb{Q}$ 的所有非平凡局部域只有 $\mathbb{Q}_p$ 和 $\mathbb{R}$ （由 Ostrowski 定理保证），我们把所有局部域上的信息整合起来可以反应整体域 $\mathbb{Q}$ 上的信息。这一点在有理二次型上是完美的，即对于一个有理系数的齐次二次方程，该方程有解当且仅当其在 $\mathbb{R}$ 和每个 $\mathbb{Q}_p$ 上都有解，此时 $\mathbb{Q}_p$ 上解的存在性就可以由 Hensel 引理判断。关于有理二次型的研究和局部——整体原则的运用这也是我们之后文章的核心之一。

1.4 $\mathbb{Q}_p$ 上的初等分析

1.4.1 $\mathbb{Q}_p$ 上的幂级数

本篇文章我们考虑在 $\mathbb{Q}_p$ 上做一些最基本的分析，探究其上的幂级数和函数的性质。

引理 1.1. $\mathbb{Q}_p$ 上的级数 $\sum_{n=1}^{\infty} a_n$ 收敛当且仅当 $\lim_{n\to\infty} |a_n|_p = 0$。

证明. 记级数的部分和为 $S_N = \sum_{n=1}^{N} a_n$，由超度量不等式的性质，我们有

$$|S_M - S_N|_p = \left| \sum_{n=N+1}^{M} a_n \right|_p \leq \max_{N+1\leq n\leq M} \{|a_n|_p\}$$

所以 $\{S_N\}$ 是柯西列当且仅当 $\lim_{n\to\infty} |a_n|_p = 0$，从而级数 $\sum_{n=1}^{\infty} a_n$ 收敛当且仅当 $\lim_{n\to\infty} |a_n|_p = 0$。 □

这个充要条件在 $\mathbb{R}$ 上是不成立的（调和级数发散）。该引理说明 $\mathbb{Q}_p$ 上的无穷级数 $\sum_{n=1}^{\infty} a_n$ 收敛性的判断要比 $\mathbb{R}$ 上简单的多，从而我们在 $\mathbb{Q}_p$ 上研究幂级数会更为方便。一个重要的性质是 $\mathbb{Q}_p$ 上的幂级数没有“绝对收敛”和“条件收敛”之分，这由收敛的充要条件可立刻得出。于是 $\mathbb{R}$ 上一些需要绝对收敛才能成立的结论在 $\mathbb{Q}_p$ 上自动成立，例如：

1. 若级数 $\sum_{n=1}^{\infty} a_n$ 在 $\mathbb{Q}_p$ 中收敛，那么我们可以任意改变求和的顺序，得到的级数和收敛至 $\mathbb{Q}_p$ 中的同一值。

2. 若级数 $\sum_{n=1}^{\infty} a_n, \sum_{n=1}^{\infty} b_n$ 分别在 $\mathbb{Q}_p$ 收敛至 a 和 b，记 $c_n = \sum_{k=1}^{n} a_k b_{n-k}$，则 $\lim_{n\to\infty} c_n = ab$。

1.4.2 $\mathbb{Q}_p$ 上的函数和导数

接下来我们定义 $\mathbb{Q}_p$ 上的连续函数和导数，这和 $\mathbb{R}$ 上的定义是类似的。

定义 1.6. 设 $f(x)$ 是 $\mathbb{Q}_p$ 到 $\mathbb{Q}_p$ 的函数。若对任意的 $\epsilon > 0$, 存在 $\delta > 0$ 使得当 $|x-x_0|_p < \delta$ 时，有 $|f(x) - f(x_0)|_p < \epsilon$，则称 $f(x)$ 在 x_0 处连续。若极限 $\lim_{h\to 0} \frac{f(x_0+h)-f(x_0)}{h}$ 存在，则称 $f(x)$ 在 x_0 处可导。

然而我们在此不展开 $\mathbb{Q}_p$ 上的微分学研究，因为很多 $\mathbb{R}$ 上的微分学定理在 $\mathbb{Q}_p$ 上失效，例如微分中值定理。我们考虑映射

$$f : \mathbb{Z}_p \to \mathbb{Z}_p, \quad \sum_{k=0}^{\infty} a_k p^k \mapsto \sum_{k=0}^{\infty} a_k p^{2k}$$

容易验证 f 是单射且 $f'(x) \equiv 0$，但是 $f(x)$ 不会在任何一个点的邻域内为常值函数。

事实上 $\mathbb{Q}_p$ 上的微分学研究比较复杂，故我们先研究形式较为简洁的幂级数，并考虑用幂级数定义函数。

$\mathbb{Q}_p$ 上的幂级数 $f(x) = \sum_{n=1}^{\infty} a_n x^n$ 的收敛半径 r 由 Hadamard 公式给出：

$$\frac{1}{r} = \limsup_{n\to\infty} \sqrt[n]{|a_n|_p}$$

此时在开球 $B(0,r)$ 内收敛。同时在闭球 $\overline{B}(0,r)$ 上收敛当且仅当 $|a_n|_p r^n \to 0$。回顾 $\mathbb{C}$ 上的幂级数，其在收敛区域边界上的收敛性的情形可能非常复杂，而我们在此看到 $\mathbb{Q}_p$ 上的情形是非常简洁的，即收敛区域是一个半径为 r 的开球或者闭球。(不要忘了在 $\mathbb{Q}_p$ 上一个开球也是闭的，所以半径为 r 的开球的闭包就是它自己，和半径为 r 的闭球是两个东西!!)

同时注意到 p-adic 赋值是一个离散赋值，即如果收敛半径 r 满足 $p^k < r \le p^{k+1}$，其中 $k \in \mathbb{Z}$，那么 $|x|_p < r \iff |x|_p \le p^k$，也就是说一个半径为 r 的开球就是一个半径小一些的闭球。

引理 1.2. 设 $f(x) = \sum_{n=1}^{\infty} a_n x^n$ 是 $\mathbb{Q}_p$ 中的幂级数。若 $f(x)$ 在 $\overline{B}(0,r)$ 中收敛，则 $f(x)$ 在 $\overline{B}(0,r)$ 中是有界且一致连续的。

证明. 首先 $|x|_p \le r$ 时，我们有

$$|f(x)|_p = \left|\sum_{n=1}^{\infty} a_n x^n\right|_p \le \max_{n\ge 1}\{|a_n x^n|_p\} \le \max_{n\ge 1}\{|a_n|_p r^n\}$$

又因为级数 $\sum_{n=1}^{\infty} a_n r^n$ 收敛，所以存在 M 使得 $|f(x)|_p \leq M$ 对任意的 $x \in \overline{B}(0,r)$ 成立。

进一步地，

$$\begin{aligned}
|f(x)-f(y)|_p &= \left|\sum_{n=1}^{\infty} a_n(x^n-y^n)\right|_p \\
&= \left|\sum_{n=1}^{\infty} a_n(x-y)(x^{n-1}+x^{n-2}y+\cdots+y^{n-1})\right|_p \\
&\leq |x-y|_p \max_{n\geq 1}\{|a_n|_p r^{n-1}\} \\
&\leq |x-y|_p \frac{M}{r}
\end{aligned}$$

这就证明了 $f(x)$ 在 $\overline{B}(0,r)$ 上是一致连续的。 □

引理表明只要 $f(x)$ 的收敛区域不是整个 $\mathbb{Q}_p$ 那么在其收敛区域上是一致连续的。而对于在整个 $\mathbb{Q}_p$ 上收敛的幂级数，其在 $\mathbb{Q}_p$ 上不一定是一致连续的（这是一个很自然的观察，因为引理的证明依赖于 $f(x)$ 的有界性），例如考虑 $f(x)=x^2$，这是一个有限项的幂级数，故在整个 $\mathbb{Q}_p$ 上收敛。再考虑

$$x_n = p^{-n}, \quad y_n = p^n + p^{-n}$$

我们有 $x_n - y_n \to 0$ 但 $|f(x_n)-f(y_n)|_p = |2+p^{2n}|_p = 1 \quad (p \neq 2)$。这就说明了 $f(x)$ 在 $\mathbb{Q}_p$ 上不是一致连续的。

1.4.3 Strassman 定理

现在我们介绍 p-adic 幂级数中非常强力的结论 Strassman 定理。

定理 1.5 (Strassman)**.** 设非零幂级数 $f(x)=\sum_{n=0}^{\infty} a_n x^n$ 在 $\mathbb{Z}_p$ 上收敛，记

$$N = \max\left\{ n \in \mathbb{N} \;\middle|\; |a_n|_p = \max_{k\geq 0}|a_k|_p \right\}$$

即 N 为最后一个使得系数绝对值达到最大的下标，则 $f(x)$ 在 $\mathbb{Z}_p$ 上的零点个数不超过 N。

该定理有一个较为初等且自然的证明思路。首先由于 $f(x)$ 在 $\mathbb{Z}_p$ 上收敛当且仅当 $|a_n|_p \to 0$，故我们可以确保 N 的存在性。接下来对 N 进行归纳，若 a 是 $f(x)$ 的一个零点，则可以利用因式定理将 $f(x)$ 写成 $(x-a)g(x)$，对 $g(x)$ 应用归纳假设即可。这里对 $g(x)$ 的幂级数展开系数的估计较为复杂，这里便略过了。

注. *Strassman 定理限制了解析幂级数零点的有限性，从而为幂级数的唯一性提供了简单的判别方式。*

推论 1.2. 设 $f(x)$ 和 $g(x)$ 是在 $\mathbb{Z}_p$ 上收敛的两个幂级数。若 $f(x)=g(x)$ 在 $\mathbb{Z}_p$ 上有无穷多个互异的解，则在整个 $\mathbb{Z}_p$ 上有 $f(x)=g(x)$，即 $f(x)$ 和 $g(x)$ 的幂级数系数完全相同。

证明. 考虑 $f(x)-g(x)$ 运用 Strassman 定理即可。 □

该推论表示 p-adic 幂级数的判别比 $\mathbb{C}$ 上幂级数更为简单。回顾 $\mathbb{C}$ 上的幂级数，如果其零点集有聚点，我们可以判定该幂级数恒等于 0，而 $\mathbb{Q}_p$ 上的幂级数只要求零点集是无穷集即可。

推论 1.3. 若在整个 $\mathbb{Z}_p$ 上收敛的幂级数 $f(x)$ 是周期函数，则 $f(x)$ 是常函数。

该推论就体现出了 $\mathbb{Q}_p$ 和 $\mathbb{C}$ 上幂级数的区别，$\mathbb{C}$ 上是允许非常数幂级数的存在的（例如 $\sin x$）。

现在我们考虑用幂级数定义 $\mathbb{Q}_p$ 上最基本的两个函数——p-adic 对数 log 和指数函数 exp。

1.4.4 log、exp 以及 LTE 引理

现在我们考虑用幂级数定义 $\mathbb{Q}_p$ 上最基本的两个函数——对数函数 log 和指数函数 exp。

定义 1.7. 在 $\mathbb{Q}_p$ 上，我们定义对数函数 $\log(1+x)$ 的形式幂级数形式为：

$$\log(1+x)=\sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$$

当 $x\in 1+p\mathbb{Z}_p$ 时，可以通过平移定义 p 进对数函数 $\log_p(x)$ 为：

$$\log_p(x)=\log(1+(x-1))=\sum_{n=1}^{\infty}(-1)^{n+1}\frac{(x-1)^n}{n}$$

命题 1.4. 上述对数函数 $\log(1+x)$ 的形式幂级数收敛半径 $\rho=1$。该级数在 $\mathbb{Q}_p$ 中收敛当且仅当 $|x|_p<1$。

证明. 根据 Hadamard 公式，级数的收敛半径满足 $1/\rho=\limsup_{n\to\infty}\sqrt[n]{|a_n|_p}$。由于 $|a_n|_p=\left|\frac{1}{n}\right|=p^{v_p(n)}$，且根据极限性质有 $\lim_{n\to\infty}\frac{v_p(n)}{n}=0$，可得：

$$\rho=\frac{1}{\limsup_{n\to\infty}\sqrt[n]{|a_n|_p}}=p^0=1$$

对于边界情形 $|x|_p=1$，由于通项的赋值 $|a_nx^n|_p=\left|\frac{1}{n}\right|_p=p^{v_p(n)}$ 在 $n\to\infty$ 时不收敛于 0，此时幂级数发散。综上所述，$\log(1+x)$ 函数收敛当且仅当 $|x|_p<1$。因此，$\log_p(x)$ 级数收敛当且仅当 $|x-1|_p<1$，即 $x\in 1+p\mathbb{Z}_p$。 □

定义 1.8. 在 $\mathbb{Q}_p$ 上，我们定义指数函数 $\exp(x)$ 的形式幂级数形式为：

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

命题 1.5. 指数函数 $\exp(x)$ 幂级数的收敛半径为 $p^{-1/(p-1)}$。分析边界情形可知，$\exp(x)$ 在 $\mathbb{Q}_p$ 中收敛当且仅当 $|x|_p < p^{-1/(p-1)}$。

命题 1.6. 若 $a, b \in 1 + p\mathbb{Z}_p$，则 $\log_p(ab) = \log_p(a) + \log_p(b)$。

证明. 令 $a = 1 + x, b = 1 + y$，其中 $x, y \in p\mathbb{Z}_p$。固定 $y \in p\mathbb{Z}_p$，定义：

$$f(x) = \log_p(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

逐项求导有：

$$f'(x) = \sum_{n=0}^{\infty} (-x)^n = \frac{1}{1 + x}$$

再定义复合函数：

$$g(x) = \log_p((1 + x)(1 + y)) = f(y + (1 + y)x)$$

根据复合函数求导的链式法则有：

$$g'(x) = (1 + y)f'(y + (1 + y)x) = \frac{1 + y}{1 + y + (1 + y)x} = \frac{1}{1 + x}$$

这表明 $f'(x) = g'(x)$。又因为 $f(x), g(x)$ 在 $|x|_p < 1$ 时一致收敛，故 $g(x) = f(x) + c$。将 $x = 0$ 代入得到 $c = g(0) = f(y)$，从而 $g(x) = f(x) + f(y)$，即：

$$\log_p(ab) = \log_p(a) + \log_p(b)$$

证毕。 □

命题 1.7. 若 $|x|_p < p^{-1/(p-1)}$，则 $|\log_p(1 + x)|_p = |x|_p$。这表明 log 函数在原点附近是一个等距映射。

证明. 此时显然有 $|x|_p < 1$，考虑级数每一项的 p 进赋值。第一项的赋值为 $|x|_p$。根据超度量不等式，我们只需证明后面每一项的 p 进幂次都严格大于 $v_p(x)$ 即可，即对任意 $n \geq 2$：

$$v_p\left(\frac{x^n}{n}\right) > v_p(x) \implies n \cdot v_p(x) - v_p(n) > v_p(x)$$

整理得：

$$(n - 1)v_p(x) > v_p(n)$$

由于已知 $v_p(x) > \frac{1}{p-1}$，故只需证明：

$$v_p(n) < \frac{n - 1}{p - 1}$$

而由 Legendre 公式，我们有：

$$v_p(n) \le v_p(n!) = \frac{n - s_p(n)}{p-1} \le \frac{n-1}{p-1}$$

其中 $s_p(n) \ge 1$ 为 n 的 p 进制各数位之和。于是引理得证。 □

此外，可以证明 exp 在其收敛区域内也是一个等距同构，并和 $\log_p$ 互为反函数。这就阐明了为什么上式中要求 $|x|_p < p^{-1/(p-1)}$，以及指数函数对收敛的限制更为严苛。然而由于 p 进赋值的离散性，这一点只会对 $p = 2$ 带来实质影响：注意到当 $p \ge 3$ 时，$|x|_p < 1$ 和 $|x|_p < p^{-1/(p-1)}$ 二者实际上是完全等价的，只有在 $p = 2$ 时后者要求更强。

接下来，我们将上述性质应用到数论中的一个非常强力的技巧——LTE 引理（Lifting the Exponent Lemma）的证明中。

定理 1.6 (LTE 引理)**.** 设整数 a, b 满足 $p|(a-b)$ 且 $p \nmid a, b$，则对任意的正整数 n：

(1) 若 p 是奇素数，则 $v_p(a^n - b^n) = v_p(a-b) + v_p(n)$；

(2) 若 $p = 2$，则

$$v_2(a^n - b^n) = \begin{cases} v_2(a-b), & n \text{ 为奇数}, \\ v_2(a^2 - b^2) + v_2(n) - 1, & n \text{ 为偶数}. \end{cases}$$

初等数论证明. 先考虑 p 是奇素数的情形。由二项式展开，我们有：

$$a^p - b^p = (a - b + b)^p - b^p = \sum_{k=1}^{p} \binom{p}{k} (a-b)^k b^{p-k}$$

当 $k < p$ 时，$p|\binom{p}{k}$。上式中 $k = 1$ 这一项的幂次为 $v_p(a-b) + 1$；而由于 p 为奇素数，其余项（$k \ge 2$）的幂次都严格大于 $v_p(a-b) + 1$。故由强三角不等式得到：

$$v_p(a^p - b^p) = v_p(a-b) + 1$$

接着对于 $n = p^t$ 的情形，通过递推可知：

$$v_p(a^{p^t} - b^{p^t}) = v_p\left((a^{p^{t-1}})^p - (b^{p^{t-1}})^p\right) = v_p(a^{p^{t-1}} - b^{p^{t-1}}) + 1 = \cdots = v_p(a-b) + t$$

最后考虑一般情形 $n = p^t m$，其中 $p \nmid m$。我们有：

$$a^n - b^n = (a^{p^t})^m - (b^{p^t})^m = (a^{p^t} - b^{p^t}) \left(\sum_{j=0}^{m-1} a^{jp^t} b^{(m-1-j)p^t} \right)$$

由于 $a \equiv b \pmod p$，故乘积的第二项在模 p 意义下与 $ma^{p^t(m-1)}$ 同余。因为 $p \nmid m$ 且 $p \nmid a$，该项不被 p 整除，于是我们有：

$$v_p(a^n - b^n) = v_p(a^{p^t} - b^{p^t}) = v_p(a-b) + t = v_p(a-b) + v_p(n)$$

这便完成了奇素数情形的初等数论证明。 □

p 进分析证明. 由于 $p \nmid a, b$，我们可在 $\mathbb{Q}_p$ 中设 $c = a/b$，则 $v_p(c) = 0$，$v_p(c-1) = v_p(a-b) \geq 1$。当 p 为奇素数时，$v_p(c-1) \geq 1 > 1/(p-1)$。由前面关于对数函数的等距映射性质，我们有：

$$v_p(a^n - b^n) = v_p(c^n - 1) = v_p(\log_p c^n) = v_p(n \log_p c) = v_p(n) + v_p(\log_p c)$$

再利用等距性 $v_p(\log_p c) = v_p(c-1)$，可得：

$$v_p(a^n - b^n) = v_p(n) + v_p(c-1) = v_p(n) + v_p(a-b)$$

这就利用 p 进分析的视角极其自然地证明了奇素数情形的 LTE 引理。 □

注. 从 *p-adic* 分析的角度看，*LTE* 引理的成立是非常直观的，它本质上就是利用了 p 进对数函数的等距同构性质。

至于 $p = 2$ 的情形，上述初等证明与 p 进证明失效的本质原因在于：等距同构对自变量的要求变成了 $|x|_2 < 1/2$，即 $v_2(x) > 1$。这意味着 $v_2(a-b) = 1$ 时是不够的。这刚好对应了初等证明中：

$$a^2 - b^2 = 2b(a-b) + (a-b)^2$$

当 $v_2(a-b) = 1$ 时，两项的 2 进幂次相同（均为 *2*），从而无法使用强三角不等式。

为了解决这一边界问题，我们对 $p = 2$ 时的完整形式进行分类讨论：

1. 若 n 为奇数，我们有：

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$

右边乘积的第二项是奇数个奇数相加，其结果为奇数，不被 *2* 整除。故此时：

$$v_2(a^n - b^n) = v_2(a-b)$$

2. 若 n 为偶数，由于 a, b 为奇数，可得 $a^2 \equiv b^2 \equiv 1 \pmod 4$，从而 $v_2(a^2 - b^2) \geq 2 > 1$。此时已落入等距同构的生效半径内。我们将 $a^n - b^n$ 改写为 $(a^2)^{n/2} - (b^2)^{n/2}$，并重复上述奇素数情形的论证（或使用对数等距性质），即可得到：

$$v_2(a^n - b^n) = v_2(a^2 - b^2) + v_2\left(\frac{n}{2}\right) = v_2(a^2 - b^2) + v_2(n) - 1$$

这就完整阐明了 $p = 2$ 时 *LTE* 引理形式会有所不同的数论与分析本质。

1.4.5 $\mathbb{Z}_p^\times$ 的结构

我们回顾 exp 和 log 函数的共同的收敛域：$p \neq 2$ 时，它们共同在 $p\mathbb{Z}_p$ 中收敛且在 $p\mathbb{Z}_p$ 中互为反函数；$p = 2$ 时，相应的收敛域要修改成 $4\mathbb{Z}_2$。我们约定

$$q = \begin{cases} p, & p \neq 2 \\ 4, & p = 2 \end{cases}$$

并定义

$$U_1 = \{x \in \mathbb{Z}_p^\times \mid |x-1|_p < 1\} = 1 + p\mathbb{Z}_p, \quad U_p = \{x \in \mathbb{Z}_p^\times \mid |x-1|_p < p^{-1/(p-1)}\} = 1 + q\mathbb{Z}_p$$

和

$$W = \{x \in \mathbb{Z}_p \mid |x|_p < p^{-1/(p-1)}\} = q\mathbb{Z}_p$$

由 log 函数的性质知，$\log_p$ 定义了从 U_p 到 W 的等距同构，从而 $U_p \cong W$。显然 W 是无挠的，故 U_p 也是无挠的，即不含单位根。

定理 1.7. 对任意的素数 p，存在同构 $\mathbb{Z}_p^\times \cong V \times U_p$，其中 $U_p \cong \mathbb{Z}_p^+$ 是一个无挠的 pro-p 群，V 是 $\mathbb{Z}_p^\times$ 的扭部分。进一步地：

1. V 为 $\mathbb{Q}_p$ 的单位根集合，且是 $\mathbb{Z}_p^\times$ 的子群。

2. $V \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong \varphi(q)$ 阶循环群。

证明. 我们断言以下的序列

$$1 \to U_p \to \mathbb{Z}_p^\times \xrightarrow{\pi} (\mathbb{Z}/q\mathbb{Z})^\times \to 1$$

是正合列，其中 π 是模 q 约化的自然同态。显然有 $\ker \pi = U_p$，我们只需证明 π 是满射即可。

若 p 是奇素数，对任意的 $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$，选取其代表元 a，则 $a^{p-1} \equiv 1 \pmod p$，故由 Hensel 引理，存在唯一的 $\omega(a) \equiv a \pmod p$ 使得 $\omega(a)$ 是多项式 $x^{p-1} - 1$ 在 $\mathbb{Z}_p$ 中的根（称为 Teichmüller 提升）。又因为 $|\omega(a)|_p = 1$，故 $\omega(a) \in \mathbb{Z}_p^\times$，进而表明 π 是满射。

若 $p = 2$，显然 $\overline{1}, \overline{3}$ 在 $\mathbb{Z}_2^\times$ 中有原像，故此时 π 也是满射。

综上所述上述序列在 $\mathbb{Z}_p^\times$ 处正合，且注意到该短正合列是分裂的且每一部分都是交换群，故我们有分解

$$\mathbb{Z}_p^\times \cong (\mathbb{Z}/q\mathbb{Z})^\times \times U_p$$

这就完成了证明。 □

同时注意到 $\mathbb{Z}_p^\times$ 的扭部分是通过 Teichmüller 提升显式构造的，于是对任意的 $x \in \mathbb{Z}_p^\times$，我们有

$$x = \omega(x) \cdot \langle x \rangle$$

这里 $\omega(x) \in V$ 是 $\mathbb{Z}_p$ 中某个 $p-1$ 次单位根（扭部分），$\langle x \rangle \in 1 + q\mathbb{Z}_p$ 是解析部分。

这就是 $\mathbb{Z}_p^\times$ 的结构，之后我们会进一步研究 $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ 以及 $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ 的结构来解决 $\mathbb{Q}_p$ 上二次型的问题。

第二章　有理二次型的局部–整体原则

2.1　准备工具

2.1.1　从 p 进数到局部–整体问题

在上一章中，我们从绝对赋值出发构造了 p 进数域 $\mathbb{Q}_p$，并由 Ostrowski 定理知道：$\mathbb{Q}$ 的非平凡完备化只有通常绝对值给出的 $\mathbb{R}$ 以及各个 p 进赋值给出的 $\mathbb{Q}_p$。因此，当我们研究一个有理系数方程是否有有理解时，一个自然的想法是：先把它放到所有局部域

$$\mathbb{R},\quad \mathbb{Q}_2,\quad \mathbb{Q}_3,\quad \mathbb{Q}_5,\quad \cdots$$

中考察。如果方程在某个局部域中已经无解，那么它当然不可能在 $\mathbb{Q}$ 上有解。

例如，方程

$$x^2+y^2+z^2=0$$

在 $\mathbb{R}$ 上只有平凡解，因此在 $\mathbb{Q}$ 上也不可能有非平凡解。再如，二元二次方程

$$x^2-2y^2=0$$

有非平凡有理解当且仅当 2 是 $\mathbb{Q}$ 中的平方。另一方面，在 $\mathbb{Q}_3$ 中，由于 2 不是模 3 的平方，故 2 也不是 $\mathbb{Q}_3$ 中的平方，于是该方程在 $\mathbb{Q}_3$ 中已经没有非平凡解。这类现象说明：局部域能够检测出某些整体无解的原因。

但是，局部处处有解并不总能推出整体有解。一个经典反例是 Selmer 曲线

$$3X^3+4Y^3+5Z^3=0.$$

它在 $\mathbb{R}$ 和所有 $\mathbb{Q}_p$ 上都有非平凡解，但在 $\mathbb{Q}$ 上没有非平凡解。这说明一般的有理方程并不满足局部–整体原则。

令人惊讶的是，对于有理二次型，局部–整体原则却是完全成立的。这就是我们接下来要证明的核心定理。

定理 2.1 (Hasse–Minkowski 定理，预告)**.** 设 $q(x_1,\dots,x_n)$ 是 $\mathbb{Q}$ 上的非退化齐次二次型。则 q 在 $\mathbb{Q}$ 上表示零，即存在非零向量 $x\in\mathbb{Q}^n$ 使得

$$q(x)=0,$$

当且仅当 q 在 $\mathbb{R}$ 和每个 $\mathbb{Q}_p$ 上都表示零。

换言之，对于有理二次型，判断整体解的问题可以完全分解为所有局部域上的解的问题。接下来我们先准备两个工具：有限域上的二次型结论，以及 $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ 的平方类结构。

2.1.2 有限域的基本性质

我们先回顾有限域的一些基本性质。设 $\mathbb{F}_q$ 是含有 $q = p^r$ 个元素的有限域，其中 p 是素数。其乘法群

$$\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$$

是一个阶为 $q-1$ 的有限群。

命题 2.1. $\mathbb{F}_q^*$ 是一个 $q-1$ 阶循环群。

证明. 因为 $\mathbb{F}_q^*$ 是域的乘法群，所以它是有限交换群。设 e 是 $\mathbb{F}_q^*$ 中所有元素阶数的最小公倍数，即该群的指数。由有限交换群结构定理，存在元素的阶正好为 e。另一方面，任意 $a \in \mathbb{F}_q^*$ 都满足

$$a^e = 1,$$

所以 $\mathbb{F}_q^*$ 中的全部 $q-1$ 个元素都是多项式 $X^e - 1$ 的根。由于域上次数为 e 的多项式最多有 e 个根，故

$$q - 1 \leq e.$$

但显然 $e \leq q-1$，于是 $e = q-1$。因此存在一个元素的阶为 $q-1$，从而 $\mathbb{F}_q^*$ 是循环群。 □

由此立刻得到：若 q 为奇数，则 $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ 只有两个元素，即平方类和非平方类。换言之，$\mathbb{F}_q^*$ 中恰有一半元素是平方。

下面证明一个非常重要的有限域定理，它将给出有限域上二次型的非平凡零点。

引理 2.1. 设 $m \geq 0$。在有限域 $\mathbb{F}_q$ 中有

$$\sum_{x \in \mathbb{F}_q} x^m = \begin{cases} 0, & 0 \leq m < q-1, \\ -1, & m > 0 \text{ 且} q-1 \mid m. \end{cases}$$

这里的等式是在 $\mathbb{F}_q$ 中成立的。

证明. 当 $m = 0$ 时，

$$\sum_{x \in \mathbb{F}_q} x^0 = q = 0$$

在 $\mathbb{F}_q$ 中成立。当 $m > 0$ 时，$0^m = 0$，所以只需求 $\sum_{x \in \mathbb{F}_q^*} x^m$。取 $\mathbb{F}_q^*$ 的生成元 g，则

$$\sum_{x \in \mathbb{F}_q^*} x^m = \sum_{i=0}^{q-2} g^{im}.$$

若 $q-1 \nmid m$，则 $g^m \neq 1$，这是一个有限几何级数，故和为 0。若 $q-1 \mid m$，则每一项都等于 1，故和为

$$q-1=-1$$

在 $\mathbb{F}_q$ 中成立。 □

定理 2.2 (Chevalley–Warning 定理)**.** 设 $f_1,\dots,f_r \in \mathbb{F}_q[X_1,\dots,X_n]$。若

$$\deg f_1+\cdots+\deg f_r<n,$$

则方程组

$$f_1=\cdots=f_r=0$$

在 $\mathbb{F}_q^n$ 中的公共零点个数被 p 整除，其中 $q=p^r$。

证明. 记公共零点个数为 N。对任意 $a\in\mathbb{F}_q$，有

$$1-a^{q-1}=\begin{cases}1, & a=0,\\ 0, & a\neq 0.\end{cases}$$

因此

$$N=\sum_{x\in\mathbb{F}_q^n}\prod_{j=1}^{r}\bigl(1-f_j(x)^{q-1}\bigr).$$

我们在 $\mathbb{F}_q$ 中计算这个和。展开乘积后，每一项都是形如

$$\sum_{x\in\mathbb{F}_q^n}F(x)$$

的表达式，其中 F 是某个多项式。常数项对应的和为

$$\sum_{x\in\mathbb{F}_q^n}1=q^n=0$$

在 $\mathbb{F}_q$ 中成立。

现在考虑非平凡项。每个非平凡项的多项式次数至多为

$$(q-1)(\deg f_1+\cdots+\deg f_r)<n(q-1).$$

将其展开成单项式，只需证明每个单项式在 $\mathbb{F}_q^n$ 上求和为 0。设其中一个单项式为

$$X_1^{m_1}\cdots X_n^{m_n}.$$

由于

$$m_1+\cdots+m_n<n(q-1),$$

所以至少存在某个 i 使得 $m_i<q-1$。于是

$$\sum_{x\in\mathbb{F}_q^n}x_1^{m_1}\cdots x_n^{m_n}=\prod_{i=1}^{n}\left(\sum_{x_i\in\mathbb{F}_q}x_i^{m_i}\right)=0.$$

因此 $N=0$ 在 $\mathbb{F}_q$ 中成立，也就是说整数 N 被 p 整除。 □

推论 2.1. 设 $q(X_1,\dots,X_n)$ 是 $\mathbb{F}_q$ 上的齐次二次型。若 $n\geq 3$，则 q 在 $\mathbb{F}_q^n$ 中存在非平凡零点。

证明. 由于 q 是齐次二次型，原点一定是它的零点。又因为

$$\deg q = 2 < n$$

当 $n\geq 3$ 时成立，所以由 Chevalley–Warning 定理可知，零点个数 N 被 p 整除。既然 $N\geq 1$ 且 $p\mid N$，便有 $N\geq p\geq 2$。因此除了原点外，至少还有一个非平凡零点。 □

这个推论是之后研究 $\mathbb{Q}_p$ 上二次型的关键工具。粗略地说，若一个 $\mathbb{Z}_p$ 系数二次型在模 p 意义下有一个非奇异零点，那么 Hensel 引理可以将其提升为 $\mathbb{Q}_p$ 上的零点。因此，有限域上的零点结论会成为 p 进域上二次型理论的第一步。

2.1.3 $\mathbb{Q}_p$ 的平方类

接下来回顾并补充 $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ 的结构。由于

$$\mathbb{Q}_p = \mathbb{Z}_p[1/p],$$

任意 $x\in\mathbb{Q}_p^*$ 都可以唯一写成

$$x = p^m u, \qquad m\in\mathbb{Z},\quad u\in\mathbb{Z}_p^*.$$

因此研究 $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ 可以分成两部分：一部分来自 p 的幂次奇偶，另一部分来自单位群 $\mathbb{Z}_p^*$ 的平方类。

先考虑 p 为奇素数的情形。

命题 2.2. 若 $p\neq 2$，则

$$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

更具体地，若 $u\in\mathbb{Z}_p^*$ 且其模 p 剩余类 $\overline{u}\in\mathbb{F}_p^*$ 是非平方，则

$$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 = \{1, u, p, up\}.$$

证明. 任意 $x\in\mathbb{Q}_p^*$ 都可以写成 $x=p^m a$，其中 $a\in\mathbb{Z}_p^*$。模掉平方后，m 只需要考虑奇偶性，因此 p 的幂次部分只贡献两个平方类。

下面考虑单位部分。我们证明：对 $a\in\mathbb{Z}_p^*$，

$$a\in(\mathbb{Z}_p^*)^2 \quad\Longleftrightarrow\quad \overline{a}\in(\mathbb{F}_p^*)^2.$$

若 $a=b^2$，则显然 $\overline{a}=\overline{b}^2$。反过来，若 $\overline{a}=\overline{b}^2$，取 $b\in\mathbb{Z}_p^*$，考虑

$$f(X) = X^2 - a.$$

则

$$f(b) \equiv 0 \pmod{p}, \qquad f'(b) = 2b \not\equiv 0 \pmod{p}.$$

由 Hensel 引理，存在 $\alpha \in \mathbb{Z}_p^*$ 使得 $\alpha^2 = a$。因此单位平方类与 $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ 一一对应。由于 $\mathbb{F}_p^*$ 是循环群，$\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ 有两个元素。综合 p 的幂次奇偶，得到 $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ 有四个元素。 □

$p = 2$ 的情形略有不同，这是因为 Hensel 引理中导数 $2X$ 总是被 2 整除，不能直接用模 2 的平方类判断。

引理 2.2. 设 $u \in \mathbb{Z}_2^*$。则 u 是 $\mathbb{Z}_2^*$ 中的平方，当且仅当

$$u \equiv 1 \pmod{8}.$$

证明. 若 $u = a^2$，其中 $a \in \mathbb{Z}_2^*$，则 a 是奇数，所以

$$a^2 \equiv 1 \pmod{8}.$$

反过来，若 $u \equiv 1 \pmod{8}$，考虑

$$f(X) = X^2 - u.$$

取初值 $X_0 = 1$，则

$$v_2(f(1)) = v_2(1-u) \geq 3, \qquad v_2(f'(1)) = v_2(2) = 1.$$

于是

$$|f(1)|_2 < |f'(1)|_2^2.$$

由 Hensel 引理的推广形式，存在 $\alpha \in \mathbb{Z}_2$ 使得 $\alpha^2 = u$。又因为 u 是单位，所以 $\alpha \in \mathbb{Z}_2^*$。 □

命题 2.3. 有同构

$$\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

一组代表元可以取为

$$1,\ -1,\ 5,\ -5,\ 2,\ -2,\ 10,\ -10.$$

证明. 任意 $x \in \mathbb{Q}_2^*$ 都可以写成 $x = 2^m u$，其中 $u \in \mathbb{Z}_2^*$。模掉平方后，2^m 只保留 m 的奇偶性。由上一个引理，单位 u 的平方类只由其模 8 的剩余类决定，而

$$\mathbb{Z}_2^*/(\mathbb{Z}_2^*)^2$$

有四个元素，可取代表元

$$1,\ -1,\ 5,\ -5.$$

再乘上 2 的幂次部分，得到八个平方类，代表元为

$$1,\ -1,\ 5,\ -5,\ 2,\ -2,\ 10,\ -10.$$

□

综上，我们得到了 $\mathbb{Q}_p$ 上平方类的完整结构：

$$\#\big(\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2\big) = \begin{cases} 4, & p \neq 2, \\ 8, & p = 2. \end{cases}$$

这些平方类将直接进入后文的 Hilbert 符号计算，并最终用于刻画 $\mathbb{Q}_p$ 上二次型的分类与表示零问题。

2.2 Hilbert 符号

2.2.1 Hilbert 符号介绍

前面我们已经看到，研究 $\mathbb{Q}_p$ 上二次型时，平方类

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$$

会自然出现。Hilbert 符号正是用来刻画两个平方类之间相互关系的基本工具。

定义 2.1 (Hilbert 符号)**.** 设 $k = \mathbb{R}$ 或 $k = \mathbb{Q}_p$，对 $a, b \in k^\times$，定义

$$(a,b)_k = \begin{cases} 1, & z^2 = ax^2 + by^2 \text{ 在} k \text{ 上有非平凡解}, \\ -1, & \text{否则}. \end{cases}$$

这里“非平凡解”指 $(x, y, z) \neq (0, 0, 0)$。

换言之，$(a, b)_k = 1$ 当且仅当三元二次型

$$ax^2 + by^2 - z^2$$

在 k 上表示零。这个定义看起来只是关于一个特殊三元二次型的可解性判断，但它实际上包含了局部二次型理论中最核心的信息。

首先，Hilbert 符号只依赖于 a, b 的平方类。若 $a' = a\alpha^2$，$b' = b\beta^2$，其中 $\alpha, \beta \in k^\times$，则方程

$$z^2 = ax^2 + by^2$$

和

$$z^2 = a'X^2 + b'Y^2$$

通过变量替换 $x = \alpha X$，$y = \beta Y$ 等价。因此 Hilbert 符号可以看作定义在

$$k^\times/(k^\times)^2 \times k^\times/(k^\times)^2$$

上的函数。

其次，Hilbert 符号还有一个范数解释：

$$(a,b)_k = 1 \quad \Longleftrightarrow \quad a \in N_{k(\sqrt{b})/k}\big(k(\sqrt{b})^\times\big).$$

事实上，若 b 不是平方，则

$$N_{k(\sqrt{b})/k}(u + v\sqrt{b}) = u^2 - bv^2.$$

经过简单变形，范数条件和方程 $z^2 = ax^2 + by^2$ 的非平凡可解性是等价的。这个解释说明 Hilbert 符号不仅是二次型的语言，也和二次扩张的范数群密切相关。

2.2.2 局部计算公式

Hilbert 符号满足下面这些基本性质。它们可以由定义和范数刻画推出，也可以通过后面的局部计算公式逐一验证。

命题 2.4 (Hilbert 符号的基本性质)**.** 设 $k = \mathbb{R}$ 或 $k = \mathbb{Q}_p$，$a, b, c \in k^\times$。则：

$$(a,b)_k = (b,a)_k,$$

$$(a,b)_k = 1 \quad \text{若} a \in (k^\times)^2 \text{ 或} b \in (k^\times)^2,$$

$$(a,bc)_k = (a,b)_k(a,c)_k,$$

$$(a,-a)_k = 1,$$

$$(a,1-a)_k = 1 \qquad (a \neq 1).$$

这些性质说明 Hilbert 符号在平方类群上是一个对称双线性函数：

$$k^\times/(k^\times)^2 \times k^\times/(k^\times)^2 \longrightarrow \{\pm 1\}.$$

因此只要知道平方类代表元之间的取值，就可以完全计算 Hilbert 符号。

先看实数情形。由实数平方非负可知：

$$(a,b)_\infty = \begin{cases} -1, & a < 0,\ b < 0, \\ 1, & \text{否则}. \end{cases}$$

事实上，当 $a, b < 0$ 时，方程 $z^2 = ax^2 + by^2$ 右边非正，只有平凡解；其余情形可以直接取某个变量为 0 构造非平凡解。

下面考虑 p 进情形。我们先回顾 Legendre 符号和二次互反律。对奇素数 p 和整数 a，若 $p \nmid a$，定义

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ 是模} p \text{ 的非零平方}, \\ -1, & a \text{ 不是模} p \text{ 的平方}. \end{cases}$$

二次互反律断言：若 p, q 是不同的奇素数，则

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

此外还有补充公式：

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

定理 2.3 (奇素数处的 Hilbert 符号公式)**.** 设 $p \neq 2$，且

$$a = p^{\alpha}u, \qquad b = p^{\beta}v,$$

其中 $\alpha, \beta \in \mathbb{Z}$，$u, v \in \mathbb{Z}_p^{\times}$。则

$$(a, b)_p = (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{\overline{u}}{p}\right)^{\beta} \left(\frac{\overline{v}}{p}\right)^{\alpha},$$

其中 $\overline{u}, \overline{v}$ 分别是 u, v 在 $\mathbb{F}_p^{\times}$ 中的像。

证明. 由前面已经得到的平方类分解可知，当 $p \neq 2$ 时，

$$\mathbb{Q}_p^{\times}/(\mathbb{Q}_p^{\times})^2$$

只有四个元素。因此利用 Hilbert 符号关于两个变量的双线性，只需计算几个基本情形。

首先，若 $u, v \in \mathbb{Z}_p^{\times}$，则

$$(u, v)_p = 1.$$

这是因为模 p 后的三元二次型

$$Z^2 - uX^2 - vY^2$$

在有限域 $\mathbb{F}_p$ 上变量数为 3，由 Chevalley–Warning 推论存在非平凡零点。由于 $p \neq 2$，该非平凡零点必为非奇异零点，于是可由 Hensel 引理提升到 $\mathbb{Q}_p$ 上。

其次，

$$(u, p)_p = \left(\frac{\overline{u}}{p}\right).$$

这是因为方程

$$Z^2 = uX^2 + pY^2$$

模 p 后变为

$$Z^2 = \overline{u}X^2.$$

它有非平凡解当且仅当 $\overline{u}$ 是 $\mathbb{F}_p^{\times}$ 中的平方。

最后，由性质 $(p, -p)_p = 1$ 和双线性可得

$$(p, p)_p = (p, -1)_p.$$

再由上一种情形得到

$$(p,-1)_p = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

综合这些基本取值，再将

$$a = p^\alpha u, \qquad b = p^\beta v$$

代入双线性公式，就得到

$$(a,b)_p = (p,p)_p^{\alpha\beta}(u,p)_p^{\beta}(v,p)_p^{\alpha}(u,v)_p,$$

也就是

$$(a,b)_p = (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha}.$$

□

$p=2$ 的情形要更细致。原因在于奇素数处单位是否为平方只由模 p 的剩余类决定，而在 $\mathbb{Q}_2$ 中，单位是否为平方要看模 8 的信息：

$$u \in (\mathbb{Z}_2^\times)^2 \quad \Longleftrightarrow \quad u \equiv 1 \pmod 8.$$

定理 2.4 (2 进 Hilbert 符号公式)**.** 设

$$a = 2^\alpha u, \qquad b = 2^\beta v,$$

其中 $\alpha,\beta \in \mathbb{Z}$，$u,v \in \mathbb{Z}_2^\times$。定义

$$\epsilon(u) = \frac{u-1}{2} \pmod 2, \qquad \omega(u) = \frac{u^2-1}{8} \pmod 2.$$

则

$$(a,b)_2 = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}.$$

这里的公式和奇素数情形的差别在于：奇素数处只需要知道单位的模 p 平方类，而 2 进情形中必须同时记录模 4 和模 8 的信息。换句话说，$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ 有八个平方类，这比奇素数处的四个平方类更加复杂。

计算 $(-1,-1)_2$。此时

$$\alpha = \beta = 0, \qquad u = v = -1.$$

于是

$$\epsilon(-1) = \frac{-2}{2} \equiv 1 \pmod 2, \qquad \omega(-1) = \frac{(-1)^2-1}{8} = 0.$$

所以

$$(-1,-1)_2 = (-1)^{\epsilon(-1)\epsilon(-1)} = -1.$$

这也说明四元数代数在 2 进处会出现特殊现象。

2.2.3 Hilbert 乘积公式

现在我们从局部计算转向全局性质。Hilbert 符号最重要的全局性质是乘积公式。

定理 2.5 (Hilbert 符号的乘积公式)**.** 设 $a, b \in \mathbb{Q}^\times$，则

$$\prod_v (a,b)_v = 1,$$

其中 v 遍历 $\mathbb{Q}$ 的所有位置，即

$$v = \infty, 2, 3, 5, \ldots.$$

证明. 首先注意到，除了有限多个位置外都有

$$(a,b)_v = 1.$$

事实上，若奇素数 p 不整除 $2ab$，则 a, b 在 $\mathbb{Q}_p$ 中都是单位。由奇素数处的局部公式可知 $(a,b)_p = 1$。因此上面的无穷乘积实际上只有有限多个因子不等于 1。

由 Hilbert 符号的双线性，且

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

由 -1 和所有素数的平方类生成，所以只需要验证下面三类基本情形：

$$(-1,-1), \qquad (-1,p), \qquad (p,q),$$

其中 p, q 为素数。

首先考虑 $(-1,-1)$。在实数处，

$$(-1,-1)_\infty = -1.$$

在奇素数 p 处，-1 和 -1 都是单位，所以

$$(-1,-1)_p = 1.$$

在 2 进处，由前面的例子，

$$(-1,-1)_2 = -1.$$

因此

$$\prod_v (-1,-1)_v = (-1)\cdot(-1) = 1.$$

再考虑 $(-1,p)$。若 p 是奇素数，则非平凡贡献只可能来自 $v = p$ 与 $v = 2$。由奇素数处公式，

$$(-1,p)_p = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

另一方面，由 2 进公式，

$$(-1,p)_2=(-1)^{\frac{p-1}{2}}.$$

所以二者乘积为 1。若 $p=2$，直接由 2 进公式可得

$$(-1,2)_2=1,$$

其余位置也都没有贡献，因此乘积仍为 1。

最后考虑 (p,q)。若 p,q 是不同的奇素数，则非平凡贡献可能来自 $v=p,q,2$。由奇素数处公式，

$$(p,q)_p=\left(\frac{q}{p}\right),\qquad (p,q)_q=\left(\frac{p}{q}\right).$$

由 2 进公式，

$$(p,q)_2=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

因此

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

其中最后一步正是二次互反律。

若 $p=q$ 为奇素数，则

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

而

$$(p,p)_2=(-1)^{\frac{p-1}{2}},$$

故乘积为 1。若其中一个素数为 2，例如考虑 $(2,p)$，其中 p 为奇素数，则

$$(2,p)_p=\left(\frac{2}{p}\right),\qquad (2,p)_2=(-1)^{\frac{p^2-1}{8}}=\left(\frac{2}{p}\right),$$

故乘积仍为 1。$(2,2)$ 的情形由 2 进公式直接得到。

综上，所有生成元情形都满足乘积公式，由双线性可得任意 $a,b\in\mathbb{Q}^\times$ 的情形。 □

乘积公式说明：各个局部域上的 Hilbert 符号并不是相互独立的。虽然 $(a,b)_v$ 是在单个局部域 $\mathbb{Q}_v$ 上定义的，但所有位置上的符号相乘必须等于 1。这为之后从局部信息拼接回全局信息提供了必要的约束。

2.2.4 Hilbert 符号的全局存在性

乘积公式给出了局部 Hilbert 符号之间必须满足的全局约束。反过来，只要这些局部符号满足乘积条件，就可以在全局上构造出有理数实现它们。为了证明这个结论，我们先列出三个会用到的工具。

中国剩余定理. 设 $m_1, \ldots, m_r$ 两两互素，则对任意整数 $a_1, \ldots, a_r$，同余方程组

$$x \equiv a_i \pmod{m_i} \qquad (1 \le i \le r)$$

存在模 $m_1 \cdots m_r$ 意义下唯一的解。

Dirichlet 算术级数素数定理. 若 $(A, M) = 1$，则存在无穷多个素数 ℓ 满足

$$\ell \equiv A \pmod{M}.$$

Hilbert 符号乘积公式. 对任意 $a, b \in \mathbb{Q}^\times$，有

$$\prod_v (a, b)_v = 1.$$

定理 2.6 (给定 Hilbert 符号的存在性)**.** 固定 $a \in \mathbb{Q}^\times$。设对每个位置 v 给定

$$\varepsilon_v \in \{\pm 1\},$$

并满足：

1. 除有限多个 v 外，$\varepsilon_v = 1$；
2. $$\prod_v \varepsilon_v = 1;$$
3. 对每个 v，局部条件可实现，即存在 $x_v \in \mathbb{Q}_v^\times$ 使得
$$(a, x_v)_v = \varepsilon_v.$$

则存在 $x \in \mathbb{Q}^\times$，使得对所有位置 v 都有

$$(a, x)_v = \varepsilon_v.$$

证明. 取有限集合 S，使其包含 $\infty, 2$、所有整除 a 的素数，以及所有满足 $\varepsilon_v = -1$ 的位置。这样当 $v \notin S$ 时，预期符号都是

$$\varepsilon_v = 1.$$

我们先只考虑 S 中的有限素数。对每个有限素数 $p \in S$，由局部可实现性，存在某个局部数 $x_p \in \mathbb{Q}_p^\times$ 使得

$$(a, x_p)_p = \varepsilon_p.$$

因为 Hilbert 符号只依赖于第二个变量的平方类，所以我们只需要让最后构造出来的全局数 $x \in \mathbb{Q}^\times$ 在 $\mathbb{Q}_p$ 中和 x_p 属于同一个平方类即可。

我们把 x_p 的平方类写成标准形式。任意 $x_p \in \mathbb{Q}_p^\times$ 都可以写成

$$x_p = p^{m_p} u_p, \qquad u_p \in \mathbb{Z}_p^\times.$$

模掉平方以后，m_p 只需要保留奇偶性。因此可令

$$e_p \equiv m_p \pmod 2, \qquad e_p \in \{0, 1\},$$

并把 x_p 的平方类写成

$$p^{e_p} u_p.$$

下面解释如何把“x 在 $\mathbb{Q}_p$ 中属于 $p^{e_p}u_p$ 这个平方类”翻译成一个普通的同余条件。

若 $p \neq 2$，则前面已经证明过：

$$w \in (\mathbb{Z}_p^\times)^2 \quad \Longleftrightarrow \quad \overline{w} \in (\mathbb{F}_p^\times)^2.$$

因此，为了保证两个单位在 $\mathbb{Z}_p^\times$ 中属于同一个平方类，只需保证它们模 p 的剩余类相同，或者至少相差一个模 p 的平方。为了简化构造，我们直接要求它们模 p 相等。

若 $p = 2$，则单位平方的判别条件是

$$w \in (\mathbb{Z}_2^\times)^2 \quad \Longleftrightarrow \quad w \equiv 1 \pmod 8.$$

所以为了保证两个 2 进单位属于同一个平方类，我们只需让它们模 8 相等。

现在令

$$D = \prod_{\substack{p \in S \\ p < \infty}} p^{e_p}.$$

我们准备构造

$$x = \delta D \ell,$$

其中 $\delta \in \{\pm 1\}$ 用来控制实数处的符号，ℓ 是一个稍后选取的辅助素数，并要求 $\ell \notin S$。

先确定 δ。若实数处需要 $x > 0$，取 $\delta = 1$；若实数处需要 $x < 0$，取 $\delta = -1$。如果实数处对符号没有限制，则任取 $\delta = 1$。这一步利用的是

$$(a, x)_\infty = -1 \quad \Longleftrightarrow \quad a < 0,\ x < 0.$$

接下来对每个有限素数 $p \in S$ 写

$$D = p^{e_p} D_p, \qquad p \nmid D_p.$$

于是

$$x = \delta D \ell = p^{e_p}(\delta D_p \ell).$$

这里 $\delta D_p \ell$ 是 p 进单位。因此 x 在 $\mathbb{Q}_p$ 中的赋值奇偶已经和 x_p 一样，剩下只需要让单位部分 $\delta D_p \ell$ 和 u_p 属于同一个单位平方类。

于是我们施加如下同余条件：

当 $p \neq 2$ 时，要求

$$\delta D_p \ell \equiv u_p \pmod{p}.$$

当 $p = 2$ 时，要求

$$\delta D_2 \ell \equiv u_2 \pmod{8}.$$

这些都是关于 ℓ 的有限个同余条件。由于 D_p 在模 p 意义下可逆，D_2 在模 8 意义下也可逆，所以它们都可以改写成

$$\ell \equiv A_p \pmod{p} \qquad (p \neq 2),$$

以及

$$\ell \equiv A_2 \pmod{8} \qquad (p = 2).$$

由中国剩余定理，这些同余条件可以合并成一个同余条件

$$\ell \equiv A \pmod{M},$$

其中

$$M = 8^{\eta} \prod_{\substack{p \in S \\ p \neq 2,\ p < \infty}} p,$$

这里 $\eta = 1$ 表示 $2 \in S$，否则 $\eta = 0$。而且由于每个局部目标都是单位类，所以可以保证

$$(A, M) = 1.$$

由 Dirichlet 算术级数素数定理，存在无穷多个素数 ℓ 满足

$$\ell \equiv A \pmod{M}.$$

我们取其中一个不属于 S 的素数 ℓ，并定义

$$x = \delta D \ell.$$

根据构造，对每个有限素数 $p \in S$，数 x 和 x_p 在 $\mathbb{Q}_p^{\times}$ 中属于同一个平方类，因此

$$(a, x)_p = (a, x_p)_p = \varepsilon_p.$$

同时 δ 的选取保证了实数处也有

$$(a, x)_{\infty} = \varepsilon_{\infty}.$$

现在考虑 $v \notin S$。若 v 不是辅助素数 ℓ，则 v 不整除 $2ax$。于是 a 和 x 在 $\mathbb{Q}_v$ 中都是单位，且 $v \neq 2$，由奇素数处的 Hilbert 符号公式可知

$$(a, x)_v = 1.$$

这正好等于 ε_v。

所以唯一还没有直接控制的位置是 $v=\ell$。但是由 Hilbert 符号乘积公式，

$$\prod_v (a,x)_v = 1.$$

另一方面，假设中已经给出

$$\prod_v \varepsilon_v = 1.$$

除 $v=\ell$ 以外，我们已经证明

$$(a,x)_v = \varepsilon_v.$$

因此最后一个位置也只能满足

$$(a,x)_\ell = \varepsilon_\ell.$$

又因为 $\ell \notin S$，所以 $\varepsilon_\ell = 1$。于是对所有位置 v 都有

$$(a,x)_v = \varepsilon_v.$$

□

注. 上面的定理是固定一个 $a \in \mathbb{Q}^\times$，构造 $x \in \mathbb{Q}^\times$ 使得 $(a,x)_v$ 实现预定符号。Serre 中还会用到更一般的版本：允许每个位置给定不同的局部元素 $a_v \in \mathbb{Q}_v^\times$，然后构造全局的 x 去同时满足

$$(a_v,x)_v = \varepsilon_v.$$

这种形式需要额外使用弱逼近定理：若 S 是有限个位置构成的集合，则 $\mathbb{Q}$ 在

$$\prod_{v\in S} \mathbb{Q}_v$$

中稠密。由于每个局部平方类都是 $\mathbb{Q}_v^\times$ 中的开集，我们可以选取 $a \in \mathbb{Q}^\times$，使得

$$a/a_v \in (\mathbb{Q}_v^\times)^2, \qquad v \in S.$$

于是对所有 $v \in S$，有

$$(a,x)_v = (a_v,x)_v.$$

这样便可以把更一般的版本约化为固定全局 a 的版本。这里需要注意：这是有限位置集上的弱逼近；虽然在全体 $\prod_v \mathbb{Q}_v$ 的乘积拓扑中也可作类似表述，但不要与 Adele 环中的拓扑混淆，在 Adele 环中 $\mathbb{Q}$ 是离散嵌入而非稠密子集。