有理数域上二次型分类报告稿

姓名

大家好，我是 [机构] 的 [姓名]。今天很高兴为大家报告《有理数域上二次型的分类》。

本次报告将分为两个主要部分：

首先，我会介绍研究该问题的主要动机以及常用的方法。

其次，我将展示在有理数域 $\mathbb{Q}$ 上二次型的分类结果。

第三部分是附录，简要介绍 Hasse-Minkowski 定理的证明。

在开始之前，先说明一些记号：

- K 表示任意域。
- X、Y、Z 表示变量。
- $\left(\dfrac{a}{p}\right)$ 表示 Legendre 符号。
- 我们常用同一个字母表示元素及其模类。

下面进入第一部分。

首先，什么是二次型？什么是二次空间？设 V 是域 k 上的线性空间，一个函数 $Q : V \to k$ 称为一个二次型，只要它满足以下两个条件。一个二次空间就是空间 V 与二次型 Q 配成的一个对。

定义标量积 $x \cdot y$ 为 $B_Q(x, y)$ 的一半，注意 $Q(x) = x \cdot x$。

对于给定的一组 V 的基，二次型 Q 有一个对应的矩阵 A。若 x 在这组基下的线性表示为 $x = (x_1, \ldots, x_n)$，则 $Q(x) = x^T A x$，这说明 $Q(x)$ 是 $x_1, \ldots, x_n$ 的二次型。

考虑更平凡的二次型：如 $f(x) = \sum X_i^2$。二次空间 (k^n, f) 是一个典型例子。

若 f 是 n 元二次型，g 是 m 元二次型，记 $f \oplus g$ 为 $n+m$ 元二次型，其矩阵为块对角形式。

当我们改变 V 的一组基时，对应的矩阵 A 变为 $A' = PAP^T$。

两个二次型等价意味着它们对应的矩阵是合同的，并且任何对称矩阵都能作合同对角化。因此我们只需讨论如下类型：

$$f \sim \sum_{i=1}^{n} a_i X_i^2$$

此外，$\det(A) = \det(PAP^T)$，这意味着 $\det A$ 在 $k^\times/(k^\times)^2$ 的同余类中是不变量，称为判别式。

接下来复习 $\mathbb{R}$ 与 $\mathbb{F}_q$ 上的二次型分类：

谢尔维施特惯性定理告诉我们，$\mathbb{R}$ 上的非退化二次型总能通过合同对角化并消去平方因子化简为对角线元素全为 ± 1 的形式。因此 $\mathbb{R}$ 上的二次型完全由秩（rank）和符号数（signature）分类，这两个量都是不变量。

由此我们得到一些普遍性的结论：

1. 秩（rank）总是不变量，因此我们只需考虑秩为 n 的非退化二次型。
2. 两个二次型的系数若相差一个平方元，则它们等价。

这说明，弄清 $k^\times/(k^\times)^2$ 中元素在对角线上的分布即可粗略分类二次型。

常见域上的例子：- 对于 $\mathbb{C}$，所有元素都是平方元，因此只需秩分类。- 对于 $\mathbb{R}$，$\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{\pm 1\}$，需考虑正负号。- 对于 $\mathbb{F}_q$，$\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2 = \{1, a\}$，$a$ 为非平方元。

上述讨论给出了对角线元素的粗略分类，但这还不是完全分类。

例如，设 a 为 $\mathbb{F}_q$ 上的非平方元，考虑秩 2 的二次型 $f_1 = aX^2 + aY^2$ 与 $f_2 = X^2 + Y^2$。做基变换 $X = sX' + tY'$，$Y = tX' - sY'$，若要求 $aX'^2 + aY'^2 = X^2 + Y^2$，则需 $s^2 + t^2 = a$。

注意 s^2 和 $a - t^2$ 各有 $(q+1)/2$ 种取值，共 $q+1$ 个，而有限域只有 q 个元素，由鸽笼原理知方程有非平凡解。

不过，判别式可以作为二次型分类的不变量。

刚才我们处理了一个不定方程是否有解的问题，这启发我们推广：

定义 a 和 b 的 Hilbert 记号 $(a,b)_K$：若 $Z^2 - aX^2 - bY^2 = 0$ 有非平凡解则取 1，否则取 -1。容易发现 a, b 相差平方因子时 Hilbert 记号不变，因此它是 $k^\times/(k^\times)^2 \times k^\times/(k^\times)^2$ 上的映射。

从现在起，假设 $K = \mathbb{Q}_p$。

Hilbert 记号有具体算法（细节略），但需注意 Hilbert 记号是对称、非退化的双线性型。

记 $\mathbb{V}$ 为所有素数及 ∞，$Q_\infty = \mathbb{R}$。$(a,b)_v$ 表示 a, b 在 Q_v 上的 Hilbert 记号，对所有 $v \in \mathbb{V}$。

有乘法公式：a, b 的 Hilbert 记号除有限个 v 外都为 1，且所有 v 的乘积为 1。

Hilbert 记号在秩 2 时已足够，推广到更高秩：设 $\varepsilon(f)$ 为对角线元素 Hilbert 记号的乘积，称为 f 的 Hasse 不变量。

总结目前工作：

我们已将问题简化为秩 n 的非退化对角二次型，并得到了判别式 $d(f)$ 和 Hasse 不变量 $\varepsilon(f)$。

为后续归纳证明，提前计算去掉一个变量后的不变量：

若 $f = a_1 X_1^2 \oplus f_1$，则判别式 $d(f)$ 是所有 a_i 的乘积，可分解为 $a_1 \cdot d(f_1)$。$\varepsilon(f)$ 是所有 (a_i, a_j) 的乘积，利用 Hilbert 记号的双线性性可化简为 $\varepsilon(f_1) \cdot (a_1, a_1 d(f_1))$。

那么，满足什么条件时我们才能将一个二次型分解为两个二次型的直和？二次型的表数问题是关键。

如果存在一个非零元素 $v \in V$，使得 $f(v) = a$，那么我们说 f 表示 $a \in K$。

对于 K 中的一个元素 a，f 表示 a 等价于：- $f \sim g \oplus aZ^2$ - $f \oplus -aZ^2$ 表示 0。

第 3 条意味着检测 a 是否可以被 f 表示只需要考虑 $f \oplus -aZ^2$ 是否可以表示 0。

第 2 条意味着如果 f 能够表示 a，我们就可以把 f 分解为 $aZ^2 \oplus f_1$。

也就是说，第 2 条让我们成功将如何将二次型分解的问题转化为了二次型什么时候表示 a 的问题，而第 3 条告诉我们二次型表示 a 可以转化为表示 0 的问题。

关于何时能够表示 0 这涉及大量繁琐的分类讨论，因时间关系这里不再展开细节。

f 表示 0 当且仅当：

- 秩 2 时 $d = -1$
- 秩 3 时 -1 和 $-d$ 的 Hilbert 记号等于 Hasse 不变量
- 秩 4 时，$d \neq -1$ 或 $d = 1$ 且 Hasse 不变量 $= (-1, -1)$
- 秩 ≥ 5 时无条件成立

将这个定理应用在 $f_a = f \oplus -aZ^2$，我们可以直接得到 f 表示 a 需要的条件，这里不再赘述。但你应该注意到二次型的表数完全由秩、判别式以及 Hasse 不变量所决定。

最后，我们在此简单提及一些结果。

Witt 定理告诉我们，一个二次空间的子空间到另一个二次空间的单保距映射可以扩张成全空间上的保距映射。

如果我们考虑同一个二次空间 V 下的两个同构的子空间 U 与 W，由 Witt 定理可以扩张成 V 上的自同构，将自同构限制到补空间就可以得到补空间上的同构。

因此有 Witt 消去定理：如果两个二次型等价并且一个直和项等价，那么另一直和项也等价。

接下来让我们进入第二部分：$\mathbb{Q}_p$ 与 $\mathbb{Q}$ 上的二次型。

首先是 $\mathbb{Q}_p$ 上的讨论。

$\mathbb{Q}_p$ 上的非退化秩 n 二次型完全由 Hasse 不变量与判别式分类：

如果 f 和 g 有相同的 d 和 ε，那么它们可以同时表示某个 a。因此 f 可以分解 $f_1 \oplus aZ^2$，对 g 也类似。

直接计算可知 f_1 与 g_1 的不变量相等，由对秩的归纳可知 $f_1 \sim g_1$，因此 $f \sim g$。

但是不变量 d 与 ε 的选取不是任意的，必须受到一些条件的约束。同时我们也可以证明满足这些约束的二次型一定存在。

$n = 1$ 时，Hilbert 记号必须为 1，而 d 没有限制。

$n = 2$ 时，由 Hilbert 记号的性质限制，如果 $d = -1$ 时 ε 必须为 1。两种情况下均可构造 $f = aX^2 + adY^2$ 符合不变量。

$n = 3$ 时总可以先选任意 $a \neq d$，然后由上面的 $n = 2$ 的讨论构造 g 满足 $d(g) = ad$, $\varepsilon(g) = \varepsilon(a, -d)$。$f = g \oplus aZ^2$ 即可。

$n > 3$ 时直接取 $g(X_1, X_2, X_3)$ 满足条件，然后再添上 X_i^2 即可。

最后我们来解决今天的核心问题，$\mathbb{Q}$ 上二次型分类。

Hasse-Minkowski 定理告诉我们 f 在 $\mathbb{Q}$ 上表示 0 当且仅当在 $\mathbb{R}$ 与所有的 $\mathbb{Q}_p$ 上都表示 0。

Hasse-Minkowski 定理是今天主题的核心，因此我已将其证明放在附录第三部分。如果感兴趣，欢迎报告后与我讨论。

借助 Hasse-Minkowski 定理我们可以完全分类 $\mathbb{Q}$ 上的二次型。秩 n 的非退化二次型在 $\mathbb{Q}$ 上等价当且仅当在所有 $\mathbb{Q}_v$ 上等价。

一侧结论显然，我们只考虑充分性。

如果 f 和 g 在所有 $\mathbb{Q}_v$ 上等价，那么由 Hasse-Minkowski 定理存在一个 a 可以在 $\mathbb{Q}$ 上表示。因此我们可以分解 $f \sim f_1 \oplus aZ^2$，$g \sim g_1 \oplus aZ^2$，我们有在 $\mathbb{Q}_v$ 上 $f \sim g$，并且显然 $aZ^2 \sim aZ^2$。再由 Witt 消去定理，我们知道在所有 $\mathbb{Q}_v$ 上 $f_1 \sim g_1$。由归纳假设 $f_1 \sim g_1$ over $\mathbb{Q}$，因此 $f \sim g$ over $\mathbb{Q}$。

当然，这里的不变量选取将会受到更大的限制，除了局部的限制还有全局的限制。

首先需要满足 Hilbert 记号的全局性质——乘法公式。

其次要满足刚才 $\mathbb{Q}_p$ 上不变量的限制。

最后需要满足 $\mathbb{R}$ 上的限制：符号数、d_∞、ε_∞。

我今天就讲到这里，这就完成了 $\mathbb{Q}$ 上二次型的分类。谢谢大家！