Main goals :

1. Determine whether a quadratic form over $\mathbb{Q}$ has a nontrivial zero.

2. Do the classification of quadratic forms over $\mathbb{Q}$.
(Determine whether two quadratic forms are equivalent)

In general, it is very hard to determine whether an equation over $\mathbb{Q}$ of more than two variables has a solution, but it is much easier to to that in finite fields. Actually, you only have to test all the cases.

Our process of this problem begin with $\mathbb{F}_p$, then the p-adic field $\mathbb{Q}_p$, and then $\mathbb{Q}$.

Main results :

1. A quadratic form over $\mathbb{Q}$ has a nontrivial zero if and only if it has anontrivial zero in each l-adic field $\mathbb{Q}_l$ (p-adic field $\mathbb{Q}_p$ or $\mathbb{R}$).

2. One can use Hilbert symbol to determine whether a quadratic form over $\mathbb{Q}_p$ has a non-trivial zero.
3. Two quadratic forms over $\mathbb{Q}$ are equivalent if and only if the are equivalent over all $\mathbb{Q}_l$.

4. One can use the invariants rank, discriminat and another invariant ε to determine whether two quadratic forms over $\mathbb{Q}_p$ are equivalent.

Part 1. Basic results and definition of quadratic forms.

Definition 1 — Let V be a module over a commutative ring A.
(Bourbaki, Alg chap. IX, 3, n°4)
A function $Q: V \to A$ is called a quadratic form on V if:

1) $Q(ax) = a^2 Q(x)$ for $a \in A$ and $x \in V$
2) The function $(x, y) \mapsto Q(x+y) - Q(x) - Q(y)$ is a bilinear form. ~~Such~~

Such a pair (V, Q) is called a quadratic module.

In this note, we only consider when A is a field k with characteristic $\neq 2$ and V is a vector field over k of finite dimension.

Let $(e_i)_{1 \leq i \leq n}$ be a basis of V. Then we can express Q in a concrete way:

There exists a symmetric matrix $A = (a_{ij})$ with respect to the basis (e_i). If $\underset{V}{\overset{\cap}{x}} = \sum_{i=1}^{n} x_i e_i$, then $Q(x) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} a_{ij} x_i x_j$.

Furthermore, we can choose a basis such that A is diagonal, then $Q(x) = \sum_{1 \leq i \leq n} a_{ii} x_i^2$, which is more convinient to discuss its zeros.

We call $\det(A)$ (with is determined by Q if we ignore the multiplication of an element of k^{*2}) the discriminant of Q and denote it by $\operatorname{disc}(Q)$.

We say Q is nondegenerate if for any $x \neq 0 \in V$, there exists $y \in V$ s.t. $\frac{1}{2}[Q(x+y) - Q(x) - Q(y)] \neq 0$ (We can define $x \cdot y = \frac{1}{2}[Q(x+y) - Q(x) - Q(y)]$).

It is easy to see that Q is nondegenerate if and only if $\mathrm{disc}(Q) \neq 0$.

Definition 2. Let (V, Q) and (V', Q') be two quadratic modules over k. Let $s: V \to V'$ be a linear map of k-vector spaces. We say s is an metric morphism if ~~and~~ ~~only~~ for any $x \in V$, $Q(x) = Q'(s(x))$.

(If ametric morphism s is an isomorphism between vector spaces, then it is a metric isomorphigm)

Then we state the famous thm of Witt without proof.

If (V, Q) and (V', Q') are isomorphic and non-degenerate, then every injective metric morphism

$$s: U \to V'$$

of a subspace U of V can be extended to a metric isomorphism of V onto V'.

Remark: We can state Witt's thm in a concrete way when u is nondegenerate.
First, let us make some notions.

Let $f(X) = \sum_{i=1}^{n} a_{ii} x_i^2 + 2 \sum_{i<j} a_{ij} x_i x_j$ be a quadratic form in n variables over k (we put $a_{ji} = a_{ij}$ if $i>j$). The pair (k^n, f) is a quadratic module, associated to f.

To quadratic forms f and f' are called equivalent if the corresponding modules are isomorphic.

Let $f(X_1, \cdots, X_n)$ and $g(X_1, \cdots, X_m)$ be two quadrat. forms; we will denote $f \dotplus g$ the quadratic form

$f(X_1, \cdots, X_n) + g(X_{n+1}, \cdots, X_{n+m})$ in $n+m$ variables.

Then Witt's thm indicates:

Let $f = g \dotplus h$ and $f' = g' \dotplus h'$ be two nondegenerate quadratic forms. If $f \sim f'$ and $g \sim g'$, then $h \sim h'$ ($\sim$ means equivalent

Part 2 Equations over $\mathbb{F}_p$ and $\mathbb{Q}_p$

2.1 Theorem 1. (Chevalley - Warning)

- K is a finite field.
- Let $f_\alpha \in K[X_1, \cdots, X_n]$ be polynomials in n variables such that $\sum_\alpha \deg f_\alpha < n$, and let V be the set of their common zeros in k^n. One has $\mathrm{Card}(V) \equiv 0 \pmod p$.

Proof see A course in arithmetic Chap 1 2.2

Cor. All quadratic forms in at least 3 variables over a finite field have a nontrivial zero.

2.2 Amelioration of approximate solutions

Assume $f \in \mathbb{Z}[X]$ (or $f \in \mathbb{Z}_p[X]$) and we have already find a solution of $f(x) \equiv 0 \pmod p$ or $(\bmod\ p^n)$.

There is an elementary way to try lifting it to a solution in $\mathbb{Z}_p$. Let's first see an easy example:

Try to solve $x^2+1=0$ over $\mathbb{Z}_5$

look at $x^2+1\equiv 0 \pmod 5$.

There is a solution $x\equiv 2 \pmod 5$.

Assume $x = 5y+2 \pmod{5^2}$.

Then $(5y+2)^2+1\equiv 0 \pmod{25}$,

$\Rightarrow 20y\equiv 20 \pmod{25} \Rightarrow y\equiv 1 \pmod 5$.

And then assume $x = 25y+5+2 = 25y+7$

Then $(25y+7)^2+1\equiv 0 \pmod{125} \Rightarrow 2\times 7\times 25y+50\equiv 0 \pmod{125}$

$\Rightarrow y\equiv 2 \pmod 5$.

And them assume $x = 125y+25\times 2+5+2$

......

Do this over and over. ~~whe~~ we have $x = 2+5+2\times 25+\cdots$ in $\mathbb{Z}_p$ is a solution lifted from $x\equiv 2 \pmod 5$.

However, this sometimes fails. For example, a solution of $x^2+1\equiv 0 \pmod 2$ can not ~~ea~~ even be lift to a solution of $x^2+1\equiv 0 \pmod 4$.

But just by some easy attempts, we can get the theorem below:

Lemma ~~Theorem~~. - Let $f\in \mathbb{Z}_p[X_1,\dots,X_m]$, $x=(x_i)\in(\mathbb{Z}_p)^m$, $n,k\in\mathbb{Z}$ and j an integer such that $0\le j\le m$. Suppose that $0<2k<n$ and that

$f(x)\equiv 0 \pmod{p^n}$ and $v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k$, then for the eq $f(x)\equiv 0 \pmod{p^{n+1}}$.

~~Then~~, there exists a solution ~~zero~~ y of in $(\mathbb{Z}_p)^m$ which is congruent to x module p^{n-k}. (Proof see A course in arithmetic Chap 2 2.2 lemma ~~thm~~ 1).

Note that in the thm above, $\left(\frac{\partial f}{\partial X_j}(y)\right) \equiv \left(\frac{\partial f}{\partial X_j}(x)\right) \pmod{p^{n-k}}$.

So applying the lemma over and over again, we conclude the thm:

Thm 1: Let f and x be mentioned in the lemma, then there exists a zero y in $(\mathbb{Z}_p)^m$ which is congruent to x module p^{n-k}.

For quadratic forms, there are some corollaries:

Case 1 - Suppose $p \neq 2$. Let $f(x) = \sum a_{ij} x_i x_j$ with $a_{ij} = a_{ji}$ be a quadratic form with coefficients in $\mathbb{Z}_p$ whose discriminant $\det(a_{ij})$ is invertible. Let $a \in \mathbb{Z}_p$. Every primitive solution of the equation $f(x) \equiv a \pmod p$ lifts to a true solution. (Here primitive means not all congruent to 0 mod p).

Case 2 - Suppose $p = 2$. Let $f = \sum a_{ij} X_i X_j$ with $a_{ij} = a_{ji}$ be a quadratic form with coefficients in $\mathbb{Z}_2$ and let $a \in \mathbb{Z}_2$. Let x be a primitive solution of $f(x) \equiv a \pmod 8$. We can lift x to a true solution provided x does not annihilate all the $\frac{\partial f}{\partial X_j}$ module 4 (which is satisfied when $\det(a_{ij}) \neq 0 \pmod 2$)

Part 3. Quadratic forms over $\mathbb{F}_p$ and $\mathbb{Q}_p$

For convinience we consider $f = \sum_{i \geq 1}^{n} a_n X^n$., $a_i \neq 0$.

1) When a quadratic form over $\mathbb{F}_p$ has an nontrivial zero.

If $n = 2$ $f(x) = a_1 X^2 + a_2 X^2$ has an nontrivial zero if and only if $-\frac{a_1}{a_2}$ is a quadratic residue module p.,

which means $\begin{cases} \left(-\frac{a_1}{a_2}\right)^{\frac{p-1}{2}} \equiv 1 \pmod p & \text{if } p > 2 \\ a_1 = -a_2 \pmod p & \text{if } p = 2. \end{cases}$

If $n > 2$. By thm 1 in Part 2, f must have an nontrivial zero

2). When a quadratic form over $\mathbb{F}_p$ represents $a \in \mathbb{F}_p$.

In fact, if $n \geq 2$, for any $a \in \mathbb{F}_p$.

$f(x) = \sum_{i=1}^{n} a_i x_i^2$ $(a_i \neq 0$ in $\mathbb{F}_p)$ always represents n.

pf: Consider $a_1 x_1^2 + a_2 x_2^2 - a x_3^2$.

If $a = 0$, then $f(0) = 0$. If $a \neq 0$, then by thm 1 in part 2, it must has an nontrivial zero $x = (x_1, x_2, x_3)$

If $(-\frac{a_2}{a_1}) \notin \mathbb{F}_p^{*2}$, then $x_3 \neq 0$, so $a_1(\frac{x_1}{x_3})^2 + a_2(\frac{x_2}{x_3})^2 = a$.

If $(-\frac{a_2}{a_1}) \in \mathbb{F}_p^2$, assume $b^2 = \frac{-a_2}{a_1}$, then

$x_1^2 + \frac{a_2}{a_1} x_2^2 = (x_1 - \cancel{a}bx_2)(x_1 + bx_2)$, easy discussion shows it represents all elements in $\mathbb{F}_p$.

Rmk: In fact if char $k \neq 2$, then $x_1^2 - x_2^2$ alway represents all elements in K

3) How to classify quadratic forms over $\mathbb{F}_p$.

As mention before, two equivalent quadratic forms have same two invariants rank and discriminant (in $k^*/(k^*)^2$) ~~of equivalence~~

(We only need to discuss the case that the form is nondegenerate).

In fact, for quadratic forms over $\mathbb{F}_p$, these two invariants determine the equivalent class uniquely.

This is because every quadratic form is equivalent to a form of the form $x_1^2 + \cdots + x_{n-1}^2 + a x_n^2$.

To see it, note that in 2) we proved if f is of rank $n \geq 2$, then f represents. Then there exists $v \in \mathbb{F}_p^n$ s.t. $f(v) = 1$. Assume $\mathbb{F}_p^n = \langle v \rangle \oplus \langle v \rangle^{\perp}$

(This is a direct sum because $\langle v \rangle$ is a nondegenerate subspace)

Then there exists a quadratic form g of rank $n-1$ s.t. $f = x^2 \dotplus g$.

4) How to determine whether a quadratic form over $\mathbb{Q}_p$ ha an nontrivial zero.

This is much harder than that over $\mathbb{F}_p$. The answer is when $n \geq 5$, always, when $n \leq 4$, ~~there are~~ the result is quite a bit complicated.

First we have to introduce the Hilbert symbol.

Definition 1.

Let $a, b \in k^*$. We put:

$(a,b) = 1$ if $z^2 - ax^2 - by^2 = 0$ has a solution $(x,y,z) \neq (0,0,0)$ in k^3.

$(a,b) = -1$ otherwise.

Notions: $\varepsilon(x) = \frac{x-1}{2}$, $w(x) = \frac{x^2-1}{8}$ (Here x is a prime or a unit in $\mathbb{Q}_2$)

~~Thero~~ Theorem 1

If $k = \mathbb{R}$, ~~then~~ we have $(a,b)=1$ if a or b is >0, and $(a,b) = -1$ if a and b are <0.

If $k = \mathbb{Q}_p$ and if we write a, b in the form $p^\alpha u$, $p^\beta v$ where u and v belong to the group U of p-adic units, ~~then~~ we have

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

$(a,b) = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha w(v) + \beta w(u)}$ if $p = 2$.

Rmk: From the result of this theorem, we know that the Hilbert symbol if bilinear (Here we regards multiplication of k^*/k^{*2} as addition so it is bilinear).

However the elementary proof requires quite a lot of computation. If one wants to try it, one can try in this way:

First notice the two resuts (~~In~~ A course in arithmetic, chap 3 1.1 prop 1 and 2).

① - Let $a, b \in k^*$ and let $k_b = k(\sqrt{b})$. For $(a,b)=1$ it is necessary and sufficient that a belongs to the group Nk_b^* of norms of elements of k_b^*

②
i) $(a,b)=(b,a)$ and $(a,c^2)=1$.
ii) $(a,-a)=1$ and $(a,1-a)=1$
iii) $(a,b)=1 \Rightarrow (aa',b)=(a',b)$
(iiii) $(a,b) = (a,-ab) = (a,(1-a)b)$.

Also note that we only need to consider the case $\alpha, \beta \in \{0,1\}$. And for $\alpha=\beta=1$, by (iii) in prop ①,

$$(pu, pv) = (pu, -p^2uv) = (pu, -uv).$$

Then we can try to discuss all situations.

Now go back to quadratic froms

First we introduce another invariance ε.

For $f = \sum_{k=1}^{n} a_k X_k^2$, $\varepsilon(f) = \prod_{i<j} (a_i, a_j)$.

It can be shown that ε is invariant with ~~the~~ change of basis of the quadratic module. Witt's lemma might be useful here.

Thm 2 - For f to represents 0 it is necessary and sufficient that:
i) $n=2$ and $d=-1$ (in k^*/k^{*2})
ii) $n=3$ and $(-1,-d)=\varepsilon$.
iii) $n=4$ and either $d\neq 1$ or $d=1$ and $\varepsilon=(-1,-1)$.
iv) $n\geq 5$

Where $f = \sum_{k=1}^{n} a_k X_k^2$, $d = d(f)$, $\varepsilon = \varepsilon(f)$.

Corollary. Let $a \in k^*/k^{*2}$. In order that f represent a it is necessary and sufficient that:

i) $n=1$ and $a=d$,

ii) $n=2$ and $(a,-d)=\varepsilon$

iii) $n=3$ and either $a\neq -d$ or $a=-d$ and $(-1,-d)=\varepsilon$

iv) $n\geq 4$.

Thm 3 (Classification) Two quadratic forms over $k=\mathbb{Q}_p$ are equivalent if and only if they have the same rank, discriminate and invariant ε.

Pf: "$\Leftarrow$" is trivial.

"$\Rightarrow$" Assume f and g have same invariants d, ε, n then by previous theorem and corollary. f and g represents same elements of k.

Assume f represents $a \in k^*$.

Then there exists f_1, g_1 of rank $n-1$ s.t.

$f = f_1 \dotplus aX^2$, $g = g_1 \dotplus aX^2$.

Then $d(f_1) = d(g_1) = \frac{d}{a}$, $\varepsilon(f_1) = \varepsilon(g_1) = \frac{\varepsilon}{(a, \frac{d}{a})}$.

So by induction on n $f_1 \sim g_1$, and $f \sim g$.

Part 4. Quadratic forms over $\mathbb{Q}$.

First we need to introduce some global properties of the Hilbert symbol.

Let V denotes the set of all primes in $\mathbb{Z}$ and ∞

Theorem 1 (product formula). If $a, b \in \mathbb{Q}^*$, we have $(a,b)_v = 1$ for almost all $v \in V$ and

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

Theorem 2 Let $(a_i)_{i \in I}$ be a finite family of elements in $\mathbb{Q}^*$ and let $(\varepsilon_{i,v})_{i \in I, v \in V}$ be a family of numbers equal to ± 1. In order that there exists $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$, $v \in V$. it is necessarry and sufficient that the following conditions are satisfied:

(1) Almost all $\varepsilon_{i,v}$ are equal to 1.

(2) For all $i \in I$ we have $\prod_{v \in V} \varepsilon_{i,v} = 1$

(3) For all $v \in V$ there exists $x_v \in \mathbb{Q}_v^*$ such that (a_i, x_v) for all $i \in I$.

Rmk. Theorem 2 can be viewed as the reverse of theorem 1, (1) (2) just come from the result of theorem 2 and (3) is just natural.

It requires some preparations to proof thm 2.

Lemma 1. Chinese remainder theorem.

The topology structure on $\mathbb{Q}_p$ and $\mathbb{Z}_p$.

The topology structure on $\mathbb{Q}_p$ and $\mathbb{Z}_p$ can be defined by 2 ways which are equivalent.

One comes from p-adic metric/norm on $\mathbb{Z}$ and $\mathbb{Q}$.

Assume $r = p^a \frac{u}{v}$ where $a \in \mathbb{Z}$, $p \nmid uv$ is an element of $\mathbb{Q}$.

Then then norm $|r|$ is defined to be p^{-a}.

And for $r, s \in \mathbb{Q}$, $d(r,s) = |r-s|$.

Then d is a ~~metric~~ well-defined metric and introduces a topology on $\mathbb{Q}$ (or $\mathbb{Z}$).

Then $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are defined to be the completion of metric spaces $\mathbb{Z}$ and $\mathbb{Q}$.

The other comes from filtralization.

Here $\mathbb{Z}_p$ is defined to be the direct limit of the system

$$\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots \leftarrow \mathbb{Z}/p^n\mathbb{Z} \leftarrow \cdots .$$

Then $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$ and there is a filtralization $\mathbb{Z}_p \supseteq (p) \supseteq (p)^2 \supseteq \cdots$

A topology ~~structure~~ can be defined by this filtralization by taking a topology base to be $\{ x + (p)^n \mid x \in \mathbb{Z}_p, n \in \mathbb{N} \}$.

Similarly things work for $\mathbb{Q}_p$.

In fact, $(\mathbb{Q}_p, +)$ is a topological group and $(\mathbb{Q}_p^*, \times)$ is also a topological group. ~~In other words~~ Moever $\mathbb{Q}_p$ is a topological field.

Lemma 2 ("Approximation theorem") - Let S be a finite subset of V. Then image of $\mathbb{Q}$ in $\prod_{v\in S}\mathbb{Q}_v$ is dense in this product (product topology of those of $\mathbb{Q}_v$)

Pf: We can suppose $S = \{\infty, p_1, \dots, p_n\}$.

Assume $(x_\infty, x_1, \dots, x_n) \in \mathbb{R}\times\mathbb{Q}_{p_1}\times\cdots\mathbb{Q}_{p_n}$.

Note that $\mathbb{Q}_v^*$ is a topological ~~group~~ field for each v.

So if $\{r_n\}$ converges to x_i,

$\{a r_n\}$ converges to $a x_i$ for any integer i.

Therefore without loss of generality we can assume $x_i \in \mathbb{Z}_{p_i}$ by multiplying an integer.

By CRT there exists $x_0 \in \mathbb{Z}$ such that $v_{p_i}(x_0 - x_i) \geq N$ for all i.

Choose an integer $q \geq 2$ which is prime to all p_i.

Then rational numbers of the form a/q^m, $a\in\mathbb{Z}$, $m\geq 0$ are dense in $\mathbb{R}$.

Choose such ~~one~~ a number $u = a/q^m$ with

$|x_0 - x_\infty + u\, p_1^N \cdots p_n^N| \leq \varepsilon$

Then let $x = x_0 + u\, p_1^N \cdots p_n^N$, $|x - x_\infty| < \varepsilon$

and $|x - x_{p_i}|_{p_i} \leq \frac{1}{p_i^N}$ for each i.

So the image of $x \in \mathbb{Q}$ and $(x_\infty, x_1, \dots, x_n)$ can be ~~ass~~ as close as possible, which proves the image of $\mathbb{Q}$ is dense.

[illegible] There exists infinitely many primes $p \equiv a \pmod m$ for any a, m s.t. $(a, m) = 1$.

Back to thm 4.

Sketch proof :

Let $(\varepsilon_{i,v})$ be a family of numbers satisfying (1), (2), (3).

WLOG a_i are all integers.

Let $S = \{\infty, 2\} \cup \{p \mid p \mid a_i \text{ for some } i\}$,

$T = \{v \mid \exists i \in I \text{ with } \varepsilon_{i,v} = -1\}$.

Case 1) $S \cap T = \emptyset$. Set $a = \prod_{\substack{l \in T \\ l \neq \infty}} l$, $m = 8 \prod_{\substack{l \in S \\ l \neq 2, \infty}} l$,

there exists a prime $p \equiv a \pmod m$ with $p \notin S \cup T$.

Then $x = ap$ has the desired property.

Case 2) In general

Since $(\mathbb{Q}_v^*)^2$ is open in $\mathbb{Q}_v$, its intersection with the image of $\mathbb{Q}^*$ is non-empty by lemma 2.

So there exists $x' \in \mathbb{Q}^*$ s.t. x'/x_v is a square in $\mathbb{Q}_v^*$ for all $v \in S$. Then $(x', a_i)_v = (a_i, x_v)_v$ for all $v \in S$.

Set $\eta_{i,v} = \varepsilon_{i,v}(a_i, x')$. Then $(\eta_{i,v})$ verifies conditions (1), (2), (3) and $\eta_{i,v} = 1$ if $v \in S$.

So by Case 1) there exists $y \in \mathbb{Q}^*$ s.t. $(a_i, y)_v = \eta_{i,v}$ for all i, v

Set $x = yx'$ then x has the desired properties.

Theorem 3 (Hasse - Minkowski) - In order that a quadratic form f over $\mathbb{Q}$ represents 0, it is necessary and sufficient that for all $v \in V$. f_v ~~the~~ which is a quadratic form over $\mathbb{Q}_v$ whose coefficients are images of coefficients of f represents 0.

Rmk Hasse's principle says if an ~~fun~~ equation of polynomials (Homogeneous polynomials) has 0 (nontrivial 0) in all local field, then it has a zero in the global field.

~~This~~ Not all equations verifie this principle.

For example, the equation

$3x^3 + 4y^3 + 5z^3$ has a nontrival solution in each $\mathbb{Q}_v$ but none in $\mathbb{Q}$.

(See reference on the link).

However, Hasse's principle is valid for all algebraic curves of genus 0.

Sketch proof of the thm.

Consider n = the rank of f.
It is quite easy for $n=2$.
For $n=3$, the proof is very technical so skipped.
~~The theorem 2 is usefull for the case~~
For $n \geq 5$, we use induction on n.

We write f in the form $f = h - g$

with $h = a_1X_1^2 + a_2X_2^2$, $g = -(a_3X_3^2 + \cdots + a_nX_n^2)$.

Let S be the subset of V consisting of ∞, 2 and primes p

such that $v_p(a_i) \neq 0$ for one $i \geq 3$; it is finite.

Let $v \in S$. Since f_v represents 0, there exists

$a_v \in \mathbb{Q}_v^*$ which is represented by both h and g.

There exists $x_i^v \in \mathbb{Q}_v$, $i=1,\dots,n$ s.t. $h(x_1^v, x_2^v) = a_v = g(x_3^v, \dots, x_n^v)$

Since $(\mathbb{Q}_v^*)^2$ is open in $\mathbb{Q}_v$, by approximation theorem

this implies the existence of $x_1, x_2 \in \mathbb{Q}$ s.t.

$a/a_v \in \mathbb{Q}_v^{*2}$ for all a_v represented by $h(x_1, x_2)$ and all $v \in S$.

Now consider $f_1 = aZ^2 - g$.

Then f_1 represents 0 in all $\mathbb{Q}_v$.

By induction f_1 represents 0 in $\mathbb{Q}$ so g represents $a \in \mathbb{Q}$

then f represents 0.

For $n=4$, theorem 2 is useful.

Write $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. There exists $x_v \in \mathbb{Q}_v^*$ represented by both $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$. And $(x_v, -ab)_v = (a,b)_v$ and $(x_v, -cd)_v = (c,d)_v$

Since $\prod_{v \in V} (a,b)_v = \prod_{v \in V} (c,d)_v = 1$ by thm 1. By thm 4.

there exists $x \in \mathbb{Q}^*$ s.t. $(x, -ab)_v = (a,b)_v$ and $(x, -cd)_v = (c,d)_v$ for all v.

Then it is reduced to the case $n=3$.

地址：广东省深圳市南山区学苑大道1088号南方科技大学湖畔书院15栋
ADD: No.1088 Xueyuan Blvd. Nanshan District Shenzhen Guangdong China

Classification

Thm 4 - Let f and f' be two quadratic forms over $\mathbb{Q}$. For f and f' to be equivalent over $\mathbb{Q}$ it is necessary and sufficient that they are equivalent ~~for~~ over each $\mathbb{Q}_v$.

" $\Rightarrow$ " Trivial

" $\Leftarrow$ " By thm 3, there exists $a \in \mathbb{Q}^*$ represented by both f and f'. Then we can use induction to show $f \sim f'$.

Remark: Invariants of a quadratic form f over $\mathbb{Q}$.

rank n,

$d_v(f)$, $v \in V$,

$\varepsilon_v(f)$, $v \in V$.

and the invariant s, r for the real case

i.e. $f \sim X_1^2 + \cdots + X_s^2 - Y_1^2 - \cdots - Y_r^2$ over $\mathbb{R}$.