Criteria for solvability of $a_1x_1^2+\cdots+a_nx_n^2=0$ $(a_i\neq 0)$

Ultimate goal: solvability in $\mathbb{Q}^n\setminus\{0\}$ ($\Leftrightarrow$ in $\mathbb{Z}^n\setminus\{0\}$) (next week)

First step: solvability in $\mathbb{Q}_p^n\setminus\{0\}$ ($\Leftrightarrow$ in $\mathbb{Z}_p^n\setminus\{0\}\Leftrightarrow$ "in all $(\mathbb{Z}/p^m\mathbb{Z})^n$")

Squares in $\mathbb{Q}_p^*=p^{\mathbb{Z}}\times\mathbb{Z}_p^*$:

$\mathbb{Q}_p^{*2}=(p^2)^{\mathbb{Z}}\times\mathbb{Z}_p^{*2}$ (1) $p\neq 2$: $pr_1:\mathbb{Z}_p^*\longrightarrow(\mathbb{Z}/p\mathbb{Z})^*=\mathbb{F}_p^*$, $a\longmapsto a\pmod p$

Hensel: $\boxed{\mathbb{Z}_p^{*2}=pr_1^{-1}(\mathbb{F}_p^{*2})}$

$\mathbb{Z}_p^*/\mathbb{Z}_p^{*2}\xrightarrow{\overline{pr_1}}\mathbb{F}_p^*/\mathbb{F}_p^{*2}\xrightarrow{\sim}\{\pm 1\}$

$a\longmapsto\left(\frac{a\pmod p}{p}\right)$ Legendre symbol

$\mathbb{Q}_p^*\longrightarrow\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}=\{\overline{1},\overline{u},\overline{p},\overline{pu}\}$ $(p\neq 2)$, $a\longmapsto\overline{a}$

$u\in\mathbb{Z}_p^*$, $\left(\frac{u\pmod p}{p}\right)=-1$ $\quad|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}|=4$

(2) $p=2$: $\overline{pr_3}:\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}\xrightarrow{\sim}(\mathbb{Z}/8\mathbb{Z})^*=\{\overline{1},\overline{-1},\overline{5},\overline{-5}\}$ $\quad\boxed{\mathbb{Z}_2^{*2}=1+8\mathbb{Z}_2}$

$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}=\{\overline{1},\overline{-1},\overline{5},\overline{-5},\overline{2},\overline{-2},\overline{10},\overline{-10}\}$ $\quad|\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}|=8$

$n=2$: $a_1x_1^2+a_2x_2^2=0$ has a solution in $\mathbb{Q}_p^2\setminus\{0\}\Leftrightarrow -a_1a_2\in\mathbb{Q}_p^{*2}$

$n=3$: $a_1x_1^2+a_2x_2^2+a_3x_3^2=0\Leftrightarrow -\frac{a_1}{a_3}x_1^2-\frac{a_2}{a_3}x_2^2=x_3^2$ ($a=\frac{a_1}{a_3}$, $b=\frac{a_2}{a_3}$)

Hilbert symbol (p = prime)

Def. Let $a,b\in\mathbb{Q}_p^*$. $H_b=\{z^2-by^2\mid z,y\in\mathbb{Q}_p\}\cap\mathbb{Q}_p^*$ is a subgroup of $\mathbb{Q}_p^*$, $H_b\supset\mathbb{Q}_p^{*2}$.

It depends only on $\overline{b}\in\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Let $\overline{H}_b=H_b/\mathbb{Q}_p^{*2}\subset\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Define

$(a,b)_p=\begin{cases}1 & \text{if } a\in H_b\\ -1 & \text{if } a\notin H_b\end{cases}\Leftrightarrow\exists(x,y,z)\in\mathbb{Q}_p^3\setminus\{(0,0,0)\}\quad ax^2+by^2=z^2\Leftrightarrow b\in H_a$

This depends only on $\overline{a},\overline{b}\in\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

If: $\left.\begin{aligned}z_1^2-by_1^2&=(z_1+y_1\sqrt{b})(z_1-y_1\sqrt{b})\\ z_2^2-by_2^2&=(z_2+y_2\sqrt{b})(z_2-y_2\sqrt{b})\end{aligned}\right\}\Rightarrow\frac{z_1^2-by_1^2}{z_2^2-bz_2^2}=z_3^2-by_3^2$, $z_3+y_3\sqrt{b}=\frac{z_1+y_1\sqrt{b}}{z_2+y_2\sqrt{b}}=\frac{(z_1z_2-by_1y_2)+\sqrt{b}(y_1z_2-y_2z_1)}{z_2^2-by_2^2}$

$\Rightarrow H_b$ is a group

Thm: the Hilbert symbol $(\ ,\ )_p:\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\times\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\longrightarrow\{\pm 1\}$ satisfies:

(1) $(a,1-a)_p=1$ (the Steinberg relation), $(a,-a)_p=1$

(2) $(a,b)_p=(b,a)_p$ (symmetry)

(3) $(aa',b)_p=(a,b)_p(a',b)_p$, $(a,bb')_p=(a,b)_p(a,b')_p$ (bimultiplicativity)

(4) $[\forall a\in\mathbb{Q}_p^*\quad(a,b)_p=1]\Leftrightarrow H_b=\mathbb{Q}_p^*\Leftrightarrow b\in\mathbb{Q}_p^{*2}\Leftrightarrow\overline{b}=1$ (non-degeneracy)

If: (1) $a\cdot 1^2+(1-a)\cdot 1^2=1^2$, $a\cdot 1^2+(-a)\cdot 1^2=0^2$, (2) OK

(3), (4) Enough to show: if $\overline{b}\neq 1\Rightarrow\overline{H}_b\subset\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ has index 2 ($\Leftrightarrow|\overline{H}_b|=\begin{cases}2 & p\neq 2\\ 4 & p=2\end{cases}$),

since $\mathbb{Q}_p^*\longrightarrow\mathbb{Q}_p^*/H_b=(\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})/\overline{H}_b\simeq\{\pm 1\}$, $a\longmapsto(a,b)_p$ will then be a group morphism

Lemma 1. $p\neq 2$, $a,b\in\mathbb{Z}_p^*\Rightarrow (a,b)_p=1$. **Cor:** $\mathbb{Z}_p^*\mathbb{Q}_p^{*2}/\mathbb{Q}_p^{*2}=\langle\overline{1},\overline{u}\rangle\subset\overline{H_u}$

Pf. $ax^2+by^2\equiv 1\pmod p$ has a solution $x,y\in\mathbb{F}_p\Rightarrow p\nmid x$ or $p\nmid y\overset{\text{Hensel}}{\Rightarrow} ax^2+by^2=1$ has a solution $x,y\in\mathbb{Z}_p$.

Lemma 2. $a\in\mathbb{Z}_p^*$, $b\in p\mathbb{Z}_p^*$, $(a,b)_p=1\Rightarrow$ $\begin{cases}\left(\frac{a}{p}\right)=1, & p\neq 2\\ a\equiv 1,\ 1-b\pmod 8, & p=2\end{cases}$

Pf. If $ax^2+by^2-z^2=0$, $(x,y,z)\in\mathbb{Z}_p^3\setminus\{(0,0,0)\}$, $v_p(ax^2),v_p(z^2)\equiv 0\pmod 2$, $v_p(by^2)\equiv 1\pmod 2$ $\Rightarrow$ $\underbrace{v_p(ax^2)}_{2v_p(x)}=\underbrace{v_p(z^2)}_{2v_p(z)}\leq\underbrace{v_p(by^2)}_{2v_p(y)+1}$

Divide x,y,z by $p^{v_p(x)}\Rightarrow x,z\in\mathbb{Z}_p^*$, $y\in\mathbb{Z}_p\setminus\{0\}$.

If $p\neq 2\Rightarrow a\equiv(zx^{-1})^2\pmod p\Rightarrow\left(\frac{a}{p}\right)=1$.

If $p=2\Rightarrow x^2\equiv z^2\equiv 1\pmod 8$, $by^2\equiv 0,b\pmod 8\Rightarrow a\equiv 1,1-b\pmod 8$.

Cor: $p\neq 2$: $(u,p)_p\overset{\text{lemma2}}{=}-1\Rightarrow\overline{H_u}=\langle\overline{1},\overline{u}\rangle$, $|\overline{H_u}|=2$; $(u,pu)_p=-1\Rightarrow\overline{u}\notin\overline{H_p}$ ($\overline{H_p}=\overline{H_{-p}}$), $\overline{H_{pu}}=\overline{H_{-pu}}\Rightarrow|\overline{H_p}|=|\overline{H_{pu}}|=2$ $\Rightarrow$ Thm for $p\neq 2$.

$p=2$: if $b\in 2\mathbb{Z}_2^*\overset{\text{lemma2}}{\Rightarrow}\overline{H_b}\subsetneq\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}\Rightarrow|\overline{H_b}|$ divides $\frac{8}{2}=4$, $\overline{H_b}\supset\langle\overline{1},\overline{-b},\overline{1-b},\overline{-b(1-b)}\rangle$ $\Rightarrow|\overline{H_b}|=4$

if $a\in\mathbb{Z}_2^*\setminus\mathbb{Z}_2^{*2}\Rightarrow\exists b\in 2\mathbb{Z}_2^*$ $a\not\equiv 1,1-b\pmod 8$ ($2\nmid a$, $a\not\equiv 1\pmod 8$) $\overset{\text{lemma2}}{\Rightarrow}\overline{a}\notin\overline{H_b}\Rightarrow\overline{b}\notin\overline{H_a}\Rightarrow|\overline{H_a}|\leq 4$

$\overline{H_a}\supset\langle\overline{1},\overline{-a},\overline{1-a},\overline{-a(1-a)}\rangle$ distinct if $\overline{a}\neq\overline{-1}$ $\Rightarrow|\overline{H_a}|=4$ if $\overline{a}\neq\overline{-1}$

$\overline{H_5}=\{\overline{1},\overline{-5},\overline{-4},\overline{20}\}=\{\overline{1},\overline{-1},\overline{5},\overline{-5}\}=\mathbb{Z}_2^*\mathbb{Q}_2^{*2}/\mathbb{Q}_2^{*2}$

$-1\in\overline{H_5}\Rightarrow\overline{5}\in\overline{H_{-1}}\Rightarrow\overline{H_{-1}}\supset\{\overline{1},\overline{5},\overline{2},\overline{10}\}\Rightarrow|\overline{H_{-1}}|=4$

Formulas: (1) $p\neq 2$: $a,b\in\mathbb{Z}_p^*$ $(a,b)_p=1$, $(a,p)_p=\left(\frac{a}{p}\right)$, $(p,-p)_p=1\Rightarrow(p,p)_p=(p,-1)_p=\left(\frac{-1}{p}\right)$

$A,B\in\mathbb{Q}_p^*$ $A=p^m a$, $B=p^n b$, $a,b\in\mathbb{Z}_p^*$, $m=v_p(A)$, $n=v_p(B)$

$$(A,B)_p=(p,p)_p^{mn}(p,b)_p^m(a,p)_p^n=\left(\frac{T_p(A,B)}{p}\right),\quad T_p(A,B)=\underbrace{(-1)^{mn}\frac{A^n}{B^m}}_{(-1)^{mn}\frac{a^n}{b^m}}\pmod p\in\mathbb{F}_p^*$$

Def: $T_p:\mathbb{Q}_p^*\times\mathbb{Q}_p^*\longrightarrow\mathbb{F}_p^*$ is the tame symbol

(2) $p=2$: $(2,-2)_2=(2,-1)_2=1\Rightarrow(2,2)_2=1$

$a,b\in\mathbb{Z}_2^*$ $(a,2)_2\overset{\text{lemma2}}{=}\begin{cases}1, & a\equiv\pm 1\pmod 8\\ -1, & a\equiv\pm 5\pmod 8\end{cases}=(-1)^{\frac{a^2-1}{8}}$, $(a,-2)_2\overset{\text{lemma2}}{=}\begin{cases}1, & a\equiv 1,3\pmod 8\\ -1, & a\equiv -1,-3\pmod 8\end{cases}$

$(a,-1)_2=(a,2)_2(a,-2)_2=\begin{cases}1, & a\equiv 1,5\pmod 8\\ -1, & a\equiv -1,-5\pmod 8\end{cases}=(-1)^{\frac{a-1}{2}}$, $(a,5)_2=1$ $(\overline{a}\in\overline{H_5})$

$\Rightarrow(a,3)_2=(a,-5)_2=(a,-1)_2$,

$(a,b)_2=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$ depends only on $a,b\pmod 4\in(\mathbb{Z}/4\mathbb{Z})^*$

Hilbert symbol in $\mathbb{R}$

Write $\mathbb{Q}_\infty=\mathbb{R}$; $\operatorname{sgn}:\mathbb{R}^*/\mathbb{R}^{*2}\xrightarrow{\sim}\{\pm 1\}$. For $a,b\in\mathbb{R}^*$ $H_b=\{z^2-by^2\mid z,y\in\mathbb{R}\}\cap\mathbb{R}^*=\begin{cases}\mathbb{R}^*, & b>0\\ \mathbb{R}_{>0}^*, & b<0\end{cases}$

$$(a,b)_\infty=\begin{cases}1, & a\in H_b\\ -1, & a\notin H_b\end{cases}=(-1)^{\frac{\operatorname{sgn}(a)-1}{2}\cdot\frac{\operatorname{sgn}(b)-1}{2}}=\begin{cases}-1, & a,b<0\\ 1, & \text{if not.}\end{cases}$$

Hilbert's reformulation of the quadratic reciprocity law (+its complements)

Thm (Product formula for the Hilbert symbols)
$\forall\, a,b \in \mathbb{Q}^*$ $\quad \prod_{v} (a,b)_v = 1$ $\quad v \in P \cup \{\infty\}$, $\quad P = \{\text{primes } p\}$

Pf: write $a = \pm \prod p^{n_p}$, $b = \pm \prod p^{n_p}$. Bimultiplicativity + symmetry $\Rightarrow$ enough to consider

a	-1	-1	p	p
b	-1	p	p	q

$p \neq q$ primes

(equivalent, since $(-1,p)_v = \underbrace{(-p,p)_v}_{1}\,(p,p)_v$)

- $a = b = -1$: $\underbrace{(-1,-1)_\infty}_{-1}\ \underbrace{(-1,-1)_2}_{-1} = 1$
- $a = -1$, $b = p \neq 2$ prime: $\underbrace{(-1,p)_\infty}_{1}\ \underbrace{(-1,p)_p}_{\left(\frac{-1}{p}\right)}\ \underbrace{(-1,p)_2}_{(-1)^{\frac{p-1}{2}}} = 1 \quad \left(\Leftrightarrow \left(\tfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}\right)$
- $a = -1$, $b = p = 2$: $a+b = 1 \overset{\text{Steinberg}}{\Longrightarrow} (-1,2)_v = 1 \quad \forall v$
- $a = p \neq 2$ prime, $b = q = 2$: $\underbrace{(p,2)_\infty}_{1}\ \underbrace{(p,2)_p}_{\left(\frac{2}{p}\right)}\ \underbrace{(p,2)_2}_{(-1)^{\frac{p^2-1}{8}}} = 1 \quad \left(\Leftrightarrow \left(\tfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}\right)$
- $a = p \neq 2$ prime, $b = q \neq 2$ prime: $\underbrace{(p,q)_\infty}_{1}\ \underbrace{(p,q)_p}_{\left(\frac{q}{p}\right)}\ \underbrace{(p,q)_q}_{\left(\frac{p}{q}\right)}\ \underbrace{(p,q)_2}_{(-1)^{\frac{p-1}{2}\frac{q-1}{2}}} = 1 \quad \left(\Leftrightarrow \left(\tfrac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\tfrac{q}{p}\right)\right)$

Structure of $\mathbb{Z}_p^*$

Prop. The canonical sections $(\mathbb{Z}/p^n\mathbb{Z})^* \hookleftarrow (\mathbb{Z}/p\mathbb{Z})^*$ define a sectional $\mathbb{Z}_p^* \underset{pr_1}{\overset{s}{\hookleftarrow}} (\mathbb{Z}/p\mathbb{Z})^*$ with image $\mathrm{Im}(s) = \mu_{p-1}(\mathbb{Z}_p)$. Therefore $\mathbb{Z}_p^* = \mu_{p-1}(\mathbb{Z}_p) \times (1+p\mathbb{Z}_p)$.

Pf. Exercise (one can use Hensel's Lemma for $X^{p-1} - 1$).

Exercice. Let $q = \begin{cases} p & p \neq 2 \\ 4 & p = 2 \end{cases}$. Fix any $a \in \mathbb{Z}_p^*$ such that $a \in 1 + q\mathbb{Z}_p$, $a \notin 1 + pq\mathbb{Z}_p$.

Show that the map $\alpha : (\mathbb{Z}_p, +) \longrightarrow (1+q\mathbb{Z}_p, \cdot)$, $x \longmapsto a^x$ is well-defined and defines a topological group isomorphism (a group isomorphism + homeomorphism).

Cor. For $n \geq 1$,

$$\mathbb{Z}_p^*/\mathbb{Z}_p^{*n} \simeq \begin{cases} C_{\gcd(p-1,n)} \times C_{p^{v_p(n)}} & p \neq 2 \\ \{1\} & p = 2,\ 2 \nmid n \\ C_2 \times C_2 & p = 2,\ 2 \mid n \end{cases}$$

(**Note**: $\mathbb{Z}_2^* = \{\pm 1\} \times (1+4\mathbb{Z}_2)$)

Rmk: α induces isomorphisms $(p^r\mathbb{Z}_p, +) \xrightarrow{\sim} (1+qp^r\mathbb{Z}_p, \cdot)$ $\quad (\forall r \geq 0)$

Geometric analogue of $\prod_v (a,b)_v = 1 \quad \forall a,b \in \mathbb{Q}^*$

The tame symbol on $\mathbb{P}^1(\mathbb{C})$: $a \in \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, $T_a : \mathbb{C}(X)^* \times \mathbb{C}(X)^* \longrightarrow \mathbb{C}^*$

$$T_a(f,g) = (-1)^{v_a(f)v_a(g)} \left(\frac{f^{v_a(g)}}{g^{v_a(f)}} \right)(a) \in \mathbb{C}^*$$

Properties:
(1) $T_a(f_1 f_2, g) = T_a(f_1,g) T_a(f_2,g)$
(2) $T_a(f, g_1 g_2) = T_a(f,g_1) T_a(f,g_2)$
(3) $T_a(f, 1-f) = 1$
(4) $T_a(f,-f) = T_a(f,g) T_a(g,f) = 1$ (follows formally from (1)–(3)).

Exercise: $\forall f,g \in \mathbb{C}(X)^* \quad \prod_{a \in \mathbb{P}^1(\mathbb{C})} T_a(f,g) = 1$.

Def. F field, G abelian group. A *symbol* on F with values in G is a map $\{\ ,\ \} : F^* \times F^* \longrightarrow G$ such that
$\{aa', b\} = \{a,b\}\{a',b\}$, $\{a, bb'\} = \{a,b\}\{a,b'\}$, $\{a, 1-a\} = 1$ (*Steinberg relation*)
$(\Rightarrow \{a,-a\} = \{a,b\}\{b,a\} = 1)$.

Fact There exists a *universal symbol* $F^* \times F^* \longrightarrow K_2(F)$ (Matsumoto) through which every symbol factors

The usual groups: $F^* = K_1(F)$, $\mathbb{Z} = K_0(F)$
So we have: $v_a : K_1(\mathbb{C}(X)) \longrightarrow K_0(\mathbb{C})$
$T_a : K_2(\mathbb{C}(X)) \longrightarrow K_1(\mathbb{C})$

Thm (Tate) the tame symbols $T_p : \mathbb{Q}^* \times \mathbb{Q}^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$ $(p \neq 2)$
$a, b \longmapsto (-1)^{v_p(a)v_p(b)} \frac{a^{v_p(b)}}{b^{v_p(a)}} \pmod p$
and $(\ ,\ )_\infty : \mathbb{Q}^* \times \mathbb{Q}^* \longrightarrow \{\pm 1\}$
induce an isomorphism $K_2(\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\} \times \bigoplus_{p \neq 2 \text{ prime}} (\mathbb{Z}/p\mathbb{Z})^*$

Cor: $(\ ,\ )_2 : \mathbb{Q}^* \times \mathbb{Q}^* \longrightarrow \{\pm 1\}$ must be of the form

$$(\ ,\ )_2 = (\ ,\ )_\infty^{n_\infty} \prod_{p \neq 2} (\ ,\ )_p^{n_p}$$ for some *universal* $n_v \in \{0,1\}$

($\overset{\text{exercise}}{\Longrightarrow} \forall v \ n_v = 1$). This is not a completely modern proof of Quadratic Reciprocity, since Tate's argument use a Lemma of Gauss that played a key role in Gauss's first proof of QRL.

Quadratic forms over fields

K = field such that $2 = 1+1 \in K^*$ ($\iff K \supset \mathbb{Q}$ or $K \supset \mathbb{F}_p$, $p \neq 2$ prime)

Def. A *quadratic form* of dim $=n$ over K is a homogeneous polynomial

$$f = \sum_{i,j=1}^{n} a_{ij} x_i x_j \quad (a_{ij} = a_{ji} \in K)$$ of degree 2 in n variables, with coefficients in K.

The coefficients are determined by the values of f on $K^n = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in K\}$, since

$$f(e_i+e_j) - f(e_i) - f(e_j) = 2a_{ij} \qquad (e_i = (0, \dots, \underbrace{1}_{i\text{th place}}, 0, \dots, 0)), \quad f(e_i) = a_{ii}$$

Matrix form: $x = (x_1, \dots, x_n)$, $A = (a_{ij})_{1 \le i,j \le n} = {}^tA \in M_n(K)$, ${}^tx = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$$f(x) = x A\, {}^tx$$ (A symmetric matrix)

Change of variables: $x = yC$, $C \in M_n(K)$, $\det(C) \in K^* = K \setminus \{0\}$

$$xA\,{}^tx = yCA\,{}^tC\,{}^ty = yA_1\,{}^ty, \qquad A_1 = CA\,{}^tC \ (= {}^tA_1) \ (\Rightarrow \det(A_1) = \det(A)\underbrace{\det(C)^2}_{\in K^{*2}})$$

Def: We say that quadratic forms f, f_1 in n variables are *equivalent* (notation: $f \sim f_1$) if their matrices are related by $A_1 = CA\,{}^tC$, for suitable $C \in M_n(K)$, $\det(C) \neq 0$ ($\iff A = C^{-1}A_1\,{}^t(C^{-1})$).

Def: f is *non-degenerate* if $\det(A) \neq 0$; if this is the case, we let

$d(f) :=$ the class of $\det(A)$ modulo the squares $\in K^*/K^{*2}$ (the *discriminant* of f)

Note: (1) f non-degenerate and $f \sim f_1 \Rightarrow f_1$ non-degenerate and $d(f) = d(f_1)$.

(2) $\mathbb{C}^*/\mathbb{C}^{*2} = \{1\}$, $\mathbb{R}^*/\mathbb{R}^{*2} = \mathbb{R}^*/\mathbb{R}^*_{>0} \xrightarrow{\sim} \{\pm 1\}$, $\mathbb{F}_p^*/\mathbb{F}_p^{*2} \xrightarrow{\sim} \{\pm 1\}$

$a\mathbb{R}^{*2} \longmapsto \operatorname{sgn}(a)$ $\qquad a\mathbb{F}_p^{*2} \longmapsto \left(\frac{a}{p}\right)$.

Orthogonal direct sum: f quadratic form in m variables $x_1, \dots, x_m$

g ——— " ——— n ——— " ——— $y_1, \dots, y_n$

$\Rightarrow \quad f \perp g = f + g$ ——— " ——— $m+n$ ——— " ——— $x_1, \dots, x_m, y_1, \dots, y_n$.

($f \perp g$ non-degenerate $\iff f, g$ non-degenerate; if true, then $d(f \perp g) = d(f)d(g)$)

Matrix form: $f(x) = xA\,{}^tx$, $g(y) = yB\,{}^ty \Rightarrow (f \perp g)(x,y) = (x\ y)\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)\begin{pmatrix} {}^tx \\ {}^ty \end{pmatrix}$

Diagonal forms: $a \in K$ $\quad \langle a \rangle = ax^2$ of dim $=1$

$\langle a_1, \dots, a_n \rangle = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle = a_1x_1^2 + \dots + a_nx_n^2$, $A = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$

Def: f *represents* $a \in K$ if $\exists\, \alpha \in K^n \setminus \{0\}$ $f(\alpha) = a$.

f is *isotropic* (over K) if it represents 0 (if not, it is *anisotropic*).

Ex: $f = \underbrace{x_1^2 - x_2^2}_{\langle 1, -1 \rangle} = y_1y_2$ $\qquad (y_1 = x_1 + x_2,\ y_2 = x_1 - x_2)$ is isotropic

Note: (1) $f \sim f_1$, $g \sim g_1 \Rightarrow f \perp g \sim f_1 \perp g_1$. (2) $f \sim f_1$, f represents $a \Rightarrow$ so does f_1.

Prop. 1. If f represents $a \in K \setminus \{0\} \Rightarrow f \sim \langle a \rangle \perp f_1$.

Pf: If $f(\alpha_1, \dots, \alpha_n) = a$, take any $C = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \\ & * & \end{pmatrix} \in M_n(K)$ with $\det(C) \neq 0$; then

$A' = CA\,{}^tC = \begin{pmatrix} a & u \\ {}^tu & * \end{pmatrix}$ $(u \in K^{n-1})$ and $C' = {}^t\begin{pmatrix} 1 & -a^{-1}u \\ 0 & I_{n-1} \end{pmatrix}$ satisfies $C'A'\,{}^tC' = \begin{pmatrix} a & 0 \\ 0 & * \end{pmatrix}$.

Prop. 2. Every f is equivalent to a diagonal form: $f \sim \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$.

Pf: If $f = 0 \Rightarrow f = \langle 0 \rangle \perp \dots \perp \langle 0 \rangle$. If $f \neq 0 \Rightarrow \exists\, \alpha \in K^n$, $a = f(\alpha) \neq 0 \xRightarrow{\text{Prop. 1}} f \sim \langle a \rangle \perp f_1$, etc.

Prop. 3 If f is non-degenerate and isotropic $\Rightarrow$ f represents each $a \in K$.

Pf. $f \sim f_1 = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$, $a_i \in K^\times$, $\exists (\alpha_1, \dots, \alpha_n) \in K^n$, $\alpha_1 \neq 0$,

$a_1\alpha_1^2 + \dots + a_n\alpha_n^2 = 0$. We want to take $\beta_1 = \alpha_1(1+t)$, $\beta_k = \alpha_k(1-t)$ $(k>1)$, $t \in K$.

then $f_1(\beta_1, \dots, \beta_n) = 2t(a_1\alpha_1^2 - a_2\alpha_2^2 - \dots - a_n\alpha_n^2) = \underbrace{(4a_1\alpha_1^2)}_{\neq 0} t = a$ if $t = \frac{a}{4a_1\alpha_1^2}$.

Prop. 4 If f is non-degenerate, then:

f represents $a \in K^\times \iff \langle -a \rangle \perp f$ represents 0

Pf: $\Rightarrow$ if $f(\alpha) = a \Rightarrow (-a)\cdot 1^2 + f(\alpha) = 0$

$\Leftarrow$ if $-a\alpha_0^2 + f(\alpha_1, \dots, \alpha_n) = 0 \Rightarrow \begin{cases} \text{if } \alpha_0 \neq 0 \Rightarrow f(\alpha_1/\alpha_0, \dots, \alpha_n/\alpha_0) = a \\ \text{if } \alpha_0 = 0 \overset{\text{Prop. 3}}{\Rightarrow} f \text{ represents } a \end{cases}$

Prop. 5 If f is non-degenerate and isotropic $\Rightarrow$ $n \geq 2$ and $f \sim \langle 1, -1 \rangle \perp g$

$(\Rightarrow$ $f \sim x_1x_2 + g(x_3, \dots, x_n)$.

Pf. f represents $0 \overset{\text{Prop. 3}}{\Rightarrow} f$ represents $1 \overset{\text{Prop. 1}}{\Rightarrow} f \sim \langle 1 \rangle \perp f_1$

$\langle 1 \rangle \perp f_1$ — " — $\overset{\text{Prop. 4}}{\Rightarrow}$ f_1 — " — $-1 \overset{\text{Prop. 1}}{\Rightarrow} f_1 \sim \langle -1 \rangle \perp g$

$\Rightarrow f \sim \underbrace{\langle 1, -1 \rangle}_{\text{equiv. to } x_1x_2} \perp g$

Quadratic forms over $\mathbb{F}_p$ $(p \neq 2)$

(A) $\mathbb{F}_p^\times / \mathbb{F}_p^{\times 2} \xrightarrow{\sim} \{\pm 1\}$, $a\,\mathbb{F}_p^{\times 2} \longmapsto \left(\frac{a}{p}\right)$

(B) For $a, b \in \mathbb{F}_p^\times$ $ax^2 + by^2 = 1$ always has a solution $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$

Prop. 6 Let f be a non-degenerate quadratic form over $\mathbb{F}_p$ of $\dim(f) = n \geq 1$.

(1) If $n = 2 \Rightarrow f \sim \langle 1 \rangle \perp \langle d(f) \rangle = \langle 1, d(f) \rangle$

(2) If $n > 2 \Rightarrow$ f is isotropic and $f \sim \langle 1, -1 \rangle \perp g \sim x_1x_2 \perp g$,
g non-degenerate of $\dim(g) = n - 2$

(3) If $n = 2k \geq 2$, $f \sim \underbrace{\langle 1, -1 \rangle \perp \dots \perp \langle 1, -1 \rangle}_{(k-1) \text{ times}} \perp \langle 1, (-1)^{k-1} d(f) \rangle$

(4) If $n = 2k+1 \geq 3$, $f \sim \underbrace{\langle 1, -1 \rangle \perp \dots \perp \langle 1, -1 \rangle}_{k \text{ times}} \perp \langle (-1)^k d(f) \rangle$

(5) $\left\{\begin{array}{l}\text{equivalence classes of} \\ \text{non-degenerate quadratic} \\ \text{forms over } \mathbb{F}_p\end{array}\right\} \longrightarrow \{1, 2, 3, \dots\} \times \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2}$ is a bijection.

$$f \longmapsto (\dim(f),\ d(f))$$

Pf: (1) $f \sim \langle a \rangle \perp \langle b \rangle \overset{(B)}{\Rightarrow} f$ represents $1 \overset{\text{Prop. 1}}{\Rightarrow} f \sim \langle 1 \rangle \perp \langle d \rangle$, $1 \cdot d = d(f) \in K^\times / K^{\times 2}$

(2) $f \sim \langle a \rangle \perp \langle b \rangle \perp \langle c \rangle \perp f_1$; $\langle a, b, c \rangle = (c)\underbrace{\langle -\tfrac{a}{c}, -\tfrac{b}{c}, -1 \rangle}_{\text{isotropic, by (B)}}$; appl. Prop. 5.

(3), (4) $\Leftarrow$ (1), (2) + induction.

(5) $\Leftarrow$ (3), (4) if $\dim \geq 2$. The case $\dim = 1$ is trivial.

Anisotropic forms: dim	0	0	$\langle 1 \rangle, \langle u \rangle$	$\langle 1, -u \rangle$	$\left(\frac{u}{p}\right) = -1$
			1	2	

Witt's Thm: $\left\{\begin{matrix} f, f' \text{ quadratic forms in } x_1,\dots,x_m \\ g, g' \text{ ——— " ——— } y_1,\dots,y_n \end{matrix}\right\}$ If $f \sim f'$; f non-degenerate $\Rightarrow g \sim g'$

$f \perp g \sim f' \perp g'$

Pf: Induction on $m = \dim(f) = \dim(f')$. Enough for $m=1$: $\langle a\rangle \perp g \sim \langle a\rangle \perp g'$, $a \neq 0 \Rightarrow g \sim g'$.
$B = {}^tB$ (resp. $B' = {}^tB'$) the matrix of g (resp. of g'). We have (for some $\alpha \in K$, $u, v \in K^n$, $C \in M_n(K)$):

$$\begin{pmatrix} a & 0 \\ 0 & B' \end{pmatrix} = \begin{pmatrix} \alpha & u \\ {}^tv & C \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}\begin{pmatrix} \alpha & v \\ {}^tu & {}^tC \end{pmatrix} = \begin{pmatrix} \overbrace{\alpha^2 a + u B\,{}^tu}^{a} & \alpha a v + u B\,{}^tC \\ \underbrace{\alpha a\,{}^tv + C B\,{}^tu}_{0} & \underbrace{a\,{}^tv v + C B\,{}^tC}_{B'} \end{pmatrix}$$

Try $C' = C + \lambda\, {}^tv u$ $(\lambda \in K)$:

$$C' B\,{}^tC' = \underbrace{CB\,{}^tC}_{B' - a\,{}^tvv} + \lambda\Big(\underbrace{CB\,{}^tu v}_{-\alpha a\,{}^tvv} + \underbrace{{}^tv u B\,{}^tC}_{-\alpha a\,{}^tvv}\Big) + \lambda^2 \underbrace{{}^tv u B\,{}^tu v}_{a(1-\alpha^2)\,{}^tvv} = B' - a\,{}^tvv\,\underbrace{\big(1 + 2\alpha\lambda + (\alpha^2-1)\lambda^2\big)}_{(1+\alpha\lambda)^2 - \lambda^2 =}$$

$$= (1 + (\alpha+1)\lambda)(1 + (\alpha-1)\lambda)$$

If $\begin{cases} \alpha \neq 1 & \text{take } \lambda = (1-\alpha)^{-1} \in K \\ \alpha = 1 & \lambda = (1+\alpha)^{-1} = -1/2 \in K \end{cases} \Rightarrow C' B\,{}^tC' = B' \Rightarrow g \sim g'$.

Equivalences between diagonal forms

Prop. 7. If $f = \langle a_1,\dots,a_n\rangle \sim \langle b_1,\dots,b_n\rangle = g$ are non-degenerate, then $\exists\ f = f^{(0)}, f^{(1)}, \dots, f^{(M)} = g$ such that $f^{(j)} = \langle c_1^{(j)},\dots,c_n^{(j)}\rangle$; $\forall i = 1,\dots,n$ $c_i^{(0)} = a_i$, $c_i^{(M)} = b_i$; $\forall j = 1,\dots,M$ $c_i^{(j)} = c_i^{(j-1)}$ for $i \neq i_0^{(j)}, i_1^{(j)}$.

Pf: The order of $\{a_i\}$ (or $\{b_i\}$) does not matter (every permutation is a product of transpositions).
Enough to find $f^{(1)}$ with $f^{(M)} = \langle b_1, b_2', \dots, b_n'\rangle = \langle b_1\rangle \perp h'$; then $g = \langle b_1\rangle \perp h \overset{\text{Witt}}{\Rightarrow} h \sim h'$;
apply induction on n. After permutation of $\{a_i\}$, $\exists\ \alpha_i \in K$ $b_1 = f(\alpha_1,\dots,\alpha_n) = \sum_{i=1}^{n} a_i \alpha_i^2$ $\alpha_1,\dots,\alpha_N \neq 0$ / $\alpha_{N+1},\dots,\alpha_n = 0$.

If $N=1$: $b_1 = a_1\alpha_1^2$ take $b_i' = a_i$ for $i > 1$

If $N > 1$ and $a_1\alpha_1^2 + a_2\alpha_2^2 \neq 0$ (true if $N=2$): $\langle a_1, a_2\rangle \sim \langle a_1\alpha_1^2 + a_2\alpha_2^2,\ \frac{a_1 a_2}{a_1\alpha_1^2 + a_2\alpha_2^2}\rangle$ >
After this change of variables N is replaced by $N-1$; apply induction on N.

If $N \geq 3$ and $a_i\alpha_i^2 + a_j\alpha_j^2 = 0$ whenever $1 \leq i < j \leq 3 \Rightarrow a_i\alpha_i^2 = 0$ $\forall i = 1,2,3$ — contradiction.
So the previous case applies.

Prop. 8. If f is non-degenerate $\Rightarrow$ $f \sim \underbrace{\langle 1,-1\rangle \perp \dots \perp \langle 1,-1\rangle}_{m\langle 1,-1\rangle} \perp \underbrace{f_{an}}_{\text{anisotropic (non-degenerate if } \dim > 0)}$

If $f \sim g \Rightarrow f_{an} \sim g_{an}$.

Pf: Existence of f_{an}: Prop. 5 + induction. Equivalence $f_{an} \sim g_{an}$: Witt's Thm.

Def (1) Non-degenerate (or equal to 0 if $\dim = 0$) f, g are Witt equivalent if $\exists m, n \geq 0$ $f \perp m\langle 1,-1\rangle \sim g \perp n\langle 1,-1\rangle$
($\Leftrightarrow$ $f_{an} \sim g_{an}$, by Witt's thm).

(2) The Witt equivalence classes $[f] = [g]$ form an abelian group $W(K)$ with addition $[f] + [f'] = [f \perp f']$ and inverse $-[f] = [-f]$ the Witt group of K.

(3) the product $[\langle a\rangle] \cdot [\langle b\rangle] = [\langle ab\rangle]$ defines a commutative ring structure on $W(K)$. (the Witt ring of K)

$\dim = \dim \pmod 2 : W(K) \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is well-defined, since $\dim \langle 1,-1\rangle = 2$.

Ex: $\dim : W(\mathbb{C}) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$, $\operatorname{sgn} : W(\mathbb{R}) \xrightarrow{\sim} \mathbb{Z}$

$m\langle 1\rangle \perp n\langle -1\rangle \longmapsto m - n$

Over $\mathbb{C}$: $f \sim n\langle 1\rangle$; Over $\mathbb{R}$: $f \sim m\langle 1\rangle \perp n\langle -1\rangle$ (m,n) = signature of f (Sylvester)
$n = \dim(f)$

Quadratic forms over $\mathbb{Q}_p$

f non-degenerate quadratic form over $\mathbb{Q}_p$ of $\dim(f)=n \Rightarrow$

$f \sim \langle a_1, \dots, a_m \rangle \perp \langle pb_1, \dots, pb_{m'} \rangle$ $\quad a_i, b_i \in \mathbb{Z}_p^*$ $\quad (m+m'=n)$

$pf \sim \langle b_1, \dots, b_{m'} \rangle \perp \langle pa_1, \dots, pa_m \rangle$

(since $\mathbb{Q}_p^* = \coprod_{i\in\mathbb{Z}} (p^{2i}\mathbb{Z}_p^* \sqcup p^{2i+1}\mathbb{Z}_p^*)$)

Prop. If $p\neq 2$, $f=0$ has a solution in $\mathbb{Q}_p^n \setminus \{(0,\dots,0)\} = \mathbb{Q}_p^n \setminus \{0\}$

$\Updownarrow$

(a) $\sum_{i=1}^{m} a_i x_i^2 \equiv 0 \pmod p$ has a solution in $\mathbb{F}_p^m \setminus \{0\}$ (always true if $m\geq 3$) OR (b) $\sum_{j=1}^{m'} b_j y_j^2 \equiv 0 \pmod p$ has a solution in $\mathbb{F}_p^{m'} \setminus \{0\}$ (always true if $m'\geq 3$).

Cor. If $\dim(f)\geq 5$ and $p\neq 2$, $f=0$ always has a solution in $\mathbb{Q}_p^n \setminus \{0\}$ (f is isotropic).

Pf of Prop.: $\Uparrow$ Hensel's Lemma. $\Downarrow$ $\exists\, x \in \mathbb{Z}_p^n \setminus (p\mathbb{Z}_p)^n$ such that $f(x)=0$,

$\sum_{i=1}^{m} a_i x_i^2 + \sum_{j=1}^{m'} pb_j y_j^2 = 0$. If $p\nmid x_{i_0}$ $\Rightarrow$ (a) holds. If $\forall i\ p\mid x_i$ $\exists j_0\ p\nmid y_{j_0}$ and $\sum_{j=1}^{m'} b_j y_j^2 + \sum_{i=1}^{m} pa_i (x_i/p)^2 = 0 \Rightarrow$ (b) holds.

Prop. If $p=2$, $f=0$ has a solution in $\mathbb{Q}_2^n \setminus \{0\}$

$\Updownarrow$

(a) $\sum_i a_i x_i^2 + \sum_j 2b_j y_j^2 \equiv 0 \pmod 8$ has a solution with $2\nmid x_{i_0}$ for some i_0

OR (b) $\sum_j b_j y_j^2 + \sum_i 2a_i x_i^2 \equiv 0 \pmod 8$ ——— " ——— $2\nmid y_{j_0}$ — " — j_0

Pf: As in the case $p\neq 2$.

Non-degenerate quadratic forms over $\mathbb{Q}_v$

$f \sim a_1 x_1^2 + \dots + a_n x_n^2 = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle = \langle a_1, \dots, a_n \rangle$,

$d(f) = \overline{a_1}\cdots\overline{a_n} \in \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$, $\dim(f)=n$

determinant — dimension

$\mathbb{Q}_v^* \longrightarrow \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$, $a_i \mapsto \overline{a_i}$

Are there other invariants?

Over $\mathbb{Q}_\infty = \mathbb{R}$: $f \sim x_1^2 + \dots + x_{n_+}^2 - x_{n_++1}^2 - \dots - x_n^2 = n_+\langle 1\rangle \perp n_-\langle -1\rangle$, $n_+ + n_- = n$

Sylvester's law of inertia: (n_+, n_-) depends only on the equivalence class of f

Over $\mathbb{Q}_p$

dim=1: $\langle a_1\rangle \sim \langle a_1'\rangle \iff \overline{a_1} = \overline{a_1'} \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$

$\langle a\rangle$ represents $b \in \mathbb{Q}_p^* \iff \overline{a} = \overline{b}$

$$|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}| = \begin{cases} 4 & p\neq 2 \\ 8 & p=2 \end{cases}$$

Non-degenerate quadratic forms over $\mathbb{Q}_p$

($f \sim \langle a_1\rangle \perp \cdots \perp \langle a_n\rangle$, $a_i \in \mathbb{Q}_p^*$)

Prop (1) For $c \in \mathbb{Q}_p^*$, $\varepsilon = \pm 1$

$$\left|\{\bar{x} \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \mid (x,c)_p = \varepsilon\}\right| = \frac{1}{2}\left|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\right| \cdot \begin{cases} 1 & \bar{c} = 1,\ \varepsilon = 1 \\ 0 & \bar{c} = 1,\ \varepsilon = -1 \\ 1/2 & \bar{c} \neq 1 \end{cases}$$

(2) If $\bar{c}, \bar{c}' \neq 1$, the system

$$\begin{aligned} (x,c)_p &= \varepsilon \\ (x,c')_p &= \varepsilon' \end{aligned}$$

has no solution $x \in \mathbb{Q}_p^*$ $\iff$ $\bar{c} = \bar{c}' \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, $\varepsilon = -\varepsilon'$

Pf. (1) Non-degeneracy of $(\ ,\ )_p$ on $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \times \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

(2) By (1), there is no solution $\iff$ $\forall x \in \mathbb{Q}_p^*$ $[(x,c)_p = \varepsilon \iff (x,c')_p = -\varepsilon']$ $\iff$ $\forall x \in \mathbb{Q}_p^*$ $(x, c/c')_p = -\varepsilon/\varepsilon'$

$\iff$ $-\varepsilon/\varepsilon' = 1$, $\overline{c/c'} = 1$

Prop. Let $a, b, a' \in \mathbb{Q}_p^*$. $d = ab$ ($\bar{d} = d(f)$)

(1) $f = \langle a, b\rangle$ is isotropic $\iff$ $\bar{d} = -1$

(2) $f = \langle a, b\rangle$ represents a' $\iff$ $(a', -d)_p = (a, -d)_p$ $(= (a,b)_p)$

(3) $f = \langle a, b\rangle \sim \langle a', b'\rangle$ $\iff$ $\overline{ab} = \overline{a'b'}$ and $(a,b)_p = (a',b')_p$

Pf: (1) f isotropic $\Rightarrow$ $f \sim \langle 1, -1\rangle \Rightarrow \bar{d} = -1$. If $\overline{ab} = -1 \Rightarrow f \sim \langle a, -a\rangle$ isotropic.

(2) f represents $a' \iff \frac{a}{a'}x^2 + \frac{b}{a'}y^2 - z^2 = 0$ has a non-zero solution in $\mathbb{Q}_p^3 \iff \left(\frac{a}{a'}, \frac{b}{a'}\right)_p = 1$.

But $\left(\frac{a}{a'}, \frac{b}{a'}\right)_p = \left(\frac{a}{a'}, -\frac{a}{a'}\right)_p \left(\frac{a}{a'}, -ab\right)_p = \left(\frac{a}{a'}, \underbrace{-ab}_{-d}\right)_p$, $(a, -ab)_p = \underbrace{(a,-a)_p}_{1} (a,b)_p$.

(3) $\langle a, b\rangle \sim \langle a', b'\rangle \overset{1}{\iff} \begin{cases} f \text{ represents } a' \\ \overline{ab} = \overline{a'b'} \end{cases} \iff (a', b')_p = (a', -ab)_p \overset{(2)}{=} (a, -ab)_p = (a,b)_p$

Def. The Minkowski-Hasse invariant of a non-degenerate $f \sim \langle a_1\rangle \perp \cdots \perp \langle a_n\rangle$ is

$$c(f) = \prod_{i<j} (a_i, a_j)_p \in \{\pm 1\}$$

(invariant under permutations).

($c(f) = 1$ if $n = 0, 1$).

Prop. $c(f)$ is well-defined.

Pf. $n = 2$ Prop. (3) above

$n > 2$ Any equivalence $\langle a_1, \dots, a_n\rangle \sim \langle b_1, \dots, b_n\rangle$ is obtained from a chain of equivalences $f = \langle a_1, a_2, a_3, \dots, a_n\rangle \sim \langle a_1', a_2', a_3, \dots, a_n\rangle = f'$ (and permutations)

$\langle a_1, a_2\rangle \overset{\text{Witt}}{\sim} \langle a_1', a_2'\rangle \Rightarrow \overline{a_1 a_2} = \overline{a_1' a_2'}$, $(a_1, a_2)_p = (a_1', a_2')_p$

$$\frac{c(f')}{c(f)} = \frac{(a_1', a_2')_p}{(a_1, a_2)_p} \frac{(a_1' a_2', a_3 \cdots a_n)_p}{(a_1 a_2, a_3 \cdots a_n)_p} = 1.$$

Prop. $d(f \perp g) = d(f)\, d(g)$, $\quad c(f \perp g) = c(f)\, c(g)\, (d(f), d(g))_p$

Prop. $f = \langle a, b, c\rangle$ is isotropic $\iff$ $c(f) = (-1, -d(f))_p$

Pf: ——— " ——— $\iff \left(\frac{a}{-c}, \frac{b}{-c}\right)_p = 1$, but $\left(-\frac{a}{c}, -\frac{b}{c}\right)_p = (a,b)_p (a,c)_p (b,c)_p (-1, -abc)_p$

Cor: If $\dim(f) = 3$ and $c(f) = (-1, -d(f))_p \Rightarrow f$ represents all elements of $\mathbb{Q}_p^*$.

Goal: Classification Theorem. Let f, f' be non-degenerate quadratic forms over $\mathbb{Q}_p$. Then:

$$f \sim f' \iff \dim(f) = \dim(f'),\ d(f) = d(f'),\ c(f) = c(f').$$

Prop. ($\dim = 4$) $f \sim \langle a_1, a_2\rangle \perp \langle -b_1, -b_2\rangle$ is anisotropic $\iff$ ($d(f) = \overline{1}$ and $c(f) = -(-1,-1)_p$)
($\iff$ $f \sim \langle 1, -a_1, -b_1, ab\rangle$, $(a,b)_p = -1$). [Note: $(-1,-1)_p = \begin{cases} 1 & p \neq 2 \\ -1 & p = 2 \end{cases}$]

Pf: f isotropic $\iff \exists\, e \in \mathbb{Q}_p$ represented by both $\langle a_1, a_2\rangle$ and $\langle b_1, b_2\rangle$
$\iff \exists\, e \in \mathbb{Q}_p^*$ ——— " ———

$(e, -a_1a_2)_p = (a_1, a_2)_p$ and $(e, -b_1b_2)_p = (b_1, b_2)_p$

f anisotropic $\iff \overline{-a_1a_2} \neq 1 \neq \overline{-b_1b_2}$ and has no solution $e \in \mathbb{Q}_p^*$

$\Updownarrow$

——— " ——— and $\underbrace{\overline{-a_1a_2} = \overline{-b_1b_2}}_{d(f) = \overline{1}}$, $\underbrace{(a_1,a_2)_p = -(b_1,b_2)_p}$

$c(f) = (a_1,a_2)_p(-b_1,-b_2)_p(b_1b_2, b_1b_2)_p =$

$= \underbrace{(a_1,a_2)_p(b_1,b_2)_p}_{-1}(-1,-1)_p$

Cor. If $\dim(g) = 3$ and $a \in \mathbb{Q}_p^*$ (g non-degenerate), then:
g does not represent $a \iff f = g \perp \langle -a\rangle$ is anisotropic
$\iff \left[d(g) = \overline{-a} \text{ and } -(-1,-1)_p = c(f) = c(g)(d(g), -a)_p = c(g)(d(g), -1)_p \right]$ ($\iff c(g) = -(-d(g), -1)_p$)

Cor. $\dim(g) = 3$: $c(g) = (-d(g), -1)_p \iff g$ isotropic $\Rightarrow g$ represents all $a \in \mathbb{Q}_p^*$
$c(g) = -(-d(g), -1)_p \Rightarrow g$ represents $\mathbb{Q}_p^* \setminus (-d(g)\,\mathbb{Q}_p^{*2})$

Prop. $\dim(g) \geq 5 \Rightarrow g$ is isotropic

Pf: $g \sim h_3 \perp (-h_2) \perp g'$, $\dim(h_i) = i$

h_3 represents all but possibly one class in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$

h_2 represents $\geq \frac{1}{2}|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}| \geq 2$ classes in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \Rightarrow \exists\, e \in \mathbb{Q}_p^*$ represented by both h_3 and $h_2 \Rightarrow g$ is isotropic.

(we already know this if $p \neq 2$)
$\Uparrow$
g or $pg \sim \langle a_1, -, a_n\rangle$, $a_1, a_2, a_3 \in \mathbb{Z}_p^*$
$\Rightarrow \left(-\frac{a_1}{a_3}, -\frac{a_2}{a_3}\right)_p = 1 \Rightarrow \langle a_1, a_2, a_3\rangle$ isotropic

---

Cor. $\dim(f) = 4 \Rightarrow f$ represents every $a \in \mathbb{Q}_p^*$

Pf. $f \perp \langle -a\rangle$ is isotropic.

Cor. $\dim(f) = 4$, f anisotropic $\iff \underbrace{f \sim \langle 1, -a_1, -b_1, ab\rangle}$, $(a,b)_p = -1$

Pf: ($\Rightarrow$): f represents 1 and $d(f) = \overline{1} \Rightarrow$; $c(f) = (-a_1,-b)_p(-b_1,ab)_p(-a_1,ab)_p =$
$= (a,b)_p(-1,-1)_p$

Number of anisotropic classes: let $N := |\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}| = \begin{cases} 4 & p \neq 2 \\ 8 & p = 2 \end{cases}$

$\dim(f) = n$	0	1	2	3	4	≥ 5
$\lvert\{f \text{ anisotropic}, \dim(f) = n\}/\sim\rvert$	1	N	2N−2	N	1	0

$4N = 2 \cdot N \cdot 2$

Summary : if $\dim(f)=\dim(f')$, $d(f)=d(f')$, $c(f)=c(f')$, then:

$[f$ represents $a\in\mathbb{Q}_p^* \iff f'$ represents $a]$ (by the above analysis according to the value of dim)

Writing $f\sim\langle a_1\rangle\perp g \Rightarrow f$ represents $a_1 \Rightarrow f'$ represents $a_1 \Rightarrow f'\sim\langle a_1\rangle\perp g'$, then $d(g)=d(g')$, $c(g)=c(g')$. Repeating this procedure, we obtain

$f\sim\langle a_1,\dots,a_n\rangle\sim f'$, proving the Classification Theorem

---

Rks : • If $\dim(f)=1 \Rightarrow c(f)=1$

• If $\dim(f)=2$ and $d(f)=\overline{-1} \Rightarrow c(f)=1$.

• these are the only constraints on possible values of $(\dim, d, c)$

Ex : (1) $5x_1^2-3x_2^2-x_3^2$ is isotropic over $\mathbb{Q}_p \iff (5,-3)_p=1$

$p\neq 2,3,5 \Rightarrow 5,-3\in\mathbb{Z}_p^* \Rightarrow (5,-3)_p=1$

$(5,-3)_5=\left(\frac{-3}{5}\right)=-1$, $(5,-3)_3=(5,3)_3=\left(\frac{5}{3}\right)=-1$, $(5,-3)_2=(-1)^{\frac{5-1}{2}\cdot\frac{-3-1}{2}}=1$

(2) $f=x_1^2+x_2^2+x_3^2+x_4^2$, $g=af$, $a\in\mathbb{Q}_p^* \Rightarrow \dim(f)=\dim(g)=4$, $d(g)=\overline{a^4}\,d(f)=d(f)$

$c(f)=1$, $c(g)=(a,a)_p^6=1 \Rightarrow f\sim g$ (over all $\mathbb{Q}_p$).

---

(3) $x_1^2+x_2^2$ represents $n\in\mathbb{Z}\setminus\{0\}$ over $\mathbb{Q}_p \iff \langle 1,1,-n\rangle$ is isotropic over $\mathbb{Q}_p$

$\iff 1=(-1,n)_p$. Write $n=p^{v_p(n)}n'$ $(\Rightarrow p\nmid n')$. Then

$$(-1,p)_p^{v_p(n)}(-1,n')_p=\begin{cases}(-1)^{\frac{p-1}{2}\cdot v_p(n)} & p\neq 2\\ (-1,n')_2=(-1)^{\frac{n'-1}{2}} & p=2\end{cases}$$

Cor. $x_1^2+x_2^2$ represents $n\in\mathbb{Z}\setminus\{0\}$ over all $\mathbb{Q}_p \iff \left\{2\mid v_p(n) \text{ for all } p\equiv 3 \pmod 4\right\}$

$n>0 \iff n'\equiv 1 \pmod 4$

---

(4) $x_1^2+x_2^2+x_3^2$ represents $n\in\mathbb{Z}\setminus\{0\}$ over $\mathbb{Q}_p \iff \langle 1,1,1,-n\rangle$ is isotropic over $\mathbb{Q}_p$

isotropic over $\mathbb{Q}_p$ if $p\neq 2$ $\Rightarrow$ — " — ok if $p\neq 2$.

$f=\langle 1,1,1,-n\rangle$ is not isotropic over $\mathbb{Q}_2 \iff \left[d=\underbrace{\overline{-n}=\overline{1}}_{1} \wedge \underbrace{c(f)=-(-1,-1)_2}_{1}\right]$

$\exists a \quad 4^a\cdot n\equiv 7 \pmod 8 \iff -n\in\mathbb{Z}_2^{*2}\cdot 4^{\mathbb{Z}}$

Cor : $x_1^2+x_2^2+x_3^2$ represents $n\in\mathbb{Z}\setminus\{0\}$ over all $\mathbb{Q}_p$

$\iff n\neq 4^a m$, $m\equiv 7 \pmod 8$

---

5) Back to $\mathbb{Q}_\infty=\mathbb{R}$: one can define $d(f)$, $c(f)$ by the same formula; if

$f\sim n_+\langle 1\rangle\perp n_-\langle -1\rangle$, then $d(f)=(-1)^{n_-}$ and $c(f)=(-1,-1)_\infty^{n_-(n_--1)/2}=(-1)^{n_-(n_--1)/2}$

$(n_++n_-=n)$ determine $n_- \pmod 4$. As a result, $(\dim, d(f), c(f))$ determine f only for $n\leq 3$.

Generalised quaternion algebras

K = field such that $2 \in K^*$, $a, b \in K^*$

Def: $\left(\frac{a,b}{K}\right) = \left(\frac{a,b}{K}\right)_2 = \mathbb{H}_{a,b} = K\cdot 1 \oplus K\cdot i \oplus K\cdot j \oplus K\cdot k = \{x = x_0 + x_1 i + x_2 j + x_3 k \mid x_0, x_1, x_2, x_3 \in K\}$

$\forall z \in K \quad zi = iz, \ zj = jz$ $\quad i^2 = a, \ j^2 = b, \ k = ij = -ji$ $\quad (\Rightarrow jk = -kj = -bi, \ ki = -ik = -aj, \ k^2 = -ab)$

Ex: $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)_2$ the classical quaternions

Properties: (1) the centre $Z(\mathbb{H}_{a,b}) = \{x \mid \forall y \ xy = yx\} = K$

(2) Main involution: $x = x_0 + x_1 i + x_2 j + x_3 k \Rightarrow \overline{x} = x_0 - x_1 i - x_2 j - x_3 k$; $\overline{xy} = \overline{y}\,\overline{x}$

(3) Reduced trace and norm: $\mathrm{Trd}(x) = x + \overline{x} = 2x_0 \in K$, $\mathrm{Nrd}(x) = N(x) = x\overline{x} = \overline{x}x =$ $\boxed{x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \in K}$

(4) $N(xy) = xy\,\overline{xy} = x\underbrace{y\,\overline{y}}_{\text{centre}}\,\overline{x} = x\overline{x}\,y\overline{y} = N(x)N(y)$

(5) the quadratic form $N(x)$ is anisotropic (over K) $\Leftrightarrow$ $aX^2 + bY^2 - Z^2$ is anisotropic.
(since $\{z^2 - by^2 \mid y, z \in K\} \cap K^*$ is a subgroup of K^*).

(6) If $aX^2 + bY^2 - Z^2$ is anisotropic over K $\Rightarrow$ $N(x) \neq 0$ if $x \neq 0$ $\Rightarrow \forall x \neq 0$ $x^{-1} := N(x)^{-1}\overline{x}$ satisfies $xx^{-1} = x^{-1}x = 1$

$\Rightarrow \mathbb{H}_{a,b}$ is a skew-field (= a division algebra): every non-zero element has an inverse.

---

(7) If $aX^2 + bY^2 - Z^2$ is isotropic over K: $\exists u, v \in K$ $au^2 + bv^2 = 1$ $(\Rightarrow (ui + vj)^2 = 1)$.

$\exists$ isomorphism of K-algebras $\left(\frac{a,b}{K}\right) \xrightarrow{\sim} M_2(K)$ such that $1 \mapsto \begin{pmatrix}1 & \\ & 1\end{pmatrix}$, $ui + vj \mapsto \begin{pmatrix}1 & \\ & -1\end{pmatrix}$

$(\Rightarrow i \mapsto \begin{pmatrix}au & av \\ bv & -au\end{pmatrix}$, $j \mapsto \begin{pmatrix}bv & -au \\ -bu & -bv\end{pmatrix})$ $\quad k \mapsto \begin{pmatrix}0 & -a \\ b & 0\end{pmatrix}$

the main involution corresponds to $\begin{pmatrix}A & B \\ C & D\end{pmatrix} \mapsto \begin{pmatrix}D & -B \\ -C & A\end{pmatrix}$, Trd to Tr, Nrd to det.

---

(8) **Ex:** If $K = \mathbb{Q}_v$ $(v \in P \cup \{\infty\})$, $a, b \in \mathbb{Q}_v^*$, then $\left(\frac{a,b}{\mathbb{Q}_v}\right) \simeq$ division algebra, $(a,b)_v = -1$; $M_2(\mathbb{Q}_v)$, $(a,b)_v = 1$

---

(9) If $K = \mathbb{Q}$, $a, b \in \mathbb{Q}^*$ the product formula $\prod_v (a,b)_v = 1 \Rightarrow$

$\{v \in P \cup \{\infty\} \mid \left(\frac{a,b}{\mathbb{Q}_v}\right) \neq M_2(\mathbb{Q}_v)\}$ has even cardinality.

Ex: $a = b = -1$, $(-1,-1)_v = \begin{cases} -1, & v = 2, \infty \\ 1, & v = p \neq 2 \end{cases}$

---

(10) $\mathbb{H}_{a,b}^{\mathrm{Trd}=0} = \{x_1 i + x_2 j + x_3 k\} \subset \mathbb{H}_{a,b}$ is stable under the adjoint action of $\mathbb{H}_{a,b}^* = \{q \mid N(q) \neq 0\}$: $\mathrm{Ad}(q): x \mapsto qxq^{-1} = N(q)^{-1}(qx\overline{q})$

$[\overline{x} = -x \Rightarrow \overline{qx\overline{q}} = \overline{q}\,\overline{x}\,\overline{q} = -qx\overline{q}]$ and $N(qxq^{-1}) = N(q)N(x)N(q^{-1}) = N(x)$

$\Rightarrow$ $\mathrm{Ad}: \mathbb{H}_{a,b}^* \longrightarrow O(\mathbb{H}_{a,b}^{\mathrm{Trd}=0}, N)$ (the orthogonal group)

In fact, $\det(\mathrm{Ad}(q)) = +1 \Rightarrow$ $\mathrm{Ad}: \mathbb{H}_{a,b}^* \longrightarrow SO(\mathbb{H}_{a,b}^{\mathrm{Trd}=0}, N)$

$\cup$

$\mathbb{H}_{a,b}^{N=1}$ $\quad$ 2-fold covering

Ex: $K = \mathbb{R}$, $a = b = -1$: $SU(2) \longrightarrow SO(3)$ — " —