Quadratic forms and spaces

F = field, $\mathrm{char}(F) \neq 2$ $\quad (\Leftrightarrow\ 2 \in F^\times)$

Quadratic form over F of dim $= n \geq 0$: homogeneous polynomial of deg $= 2$ in n variables $x_1, \dots, x_n$:

$$f(x) = \sum_{i,j=1}^{n} A_{ij} x_i x_j = {}^t x A x, \quad A_{ij} = A_{ji} \in F, \quad A = {}^t A = (A_{ij}) \in M_n(F), \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

f is **nondegenerate** (or **regular**) if $d(f) := \det(A) \neq 0$

Symmetric bilinear form attached to f:

$$B(x,y) = \sum_{i,j=1}^{n} A_{ij} x_i y_j = B(y,x) = {}^t x A y = \frac{1}{2}\left(f(x+y) - f(x) - f(y)\right)$$

$A_{ij} = B(e_i, e_j)$, $e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i^{\text{th}}$ row $\Rightarrow$ A is determined by $f: F^n \longrightarrow F$

Orthogonal direct sum of $\left.\begin{aligned} f = f(x) &= f(x_1, \dots, x_m) \\ g = g(y) &= g(y_1, \dots, y_n) \end{aligned}\right\}$: $f \perp g = \underbrace{f(x) + g(y)}_{m+n \text{ variables}}$

Diagonal quadratic forms: for $a \in F$: $\langle a \rangle := ax^2$ $\quad (\dim = 1)$

$$\langle a_1, \dots, a_n \rangle := \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle = a_1 x_1^2 + \cdots + a_n x_n^2$$

Change of variables: $x = Px'$, $P \in GL_n(F)$

$$f' = f|P, \quad f'(x') := f(Px') = {}^t x' \underbrace{{}^t P A P}_{A'} x', \quad \underline{d(f') = d(f) \det(P)^2}$$

f, f' are equivalent (over F) (notation: $f \sim f'$) if $f' = f|P$ for some $P \in GL_n(F)$

Completing the squares $\Rightarrow$ every f is equivalent to some $\langle a_1, \dots, a_n \rangle$

Notation: (a) $\underline{d_\pm(f) := (-1)^{\left[\frac{n}{2}\right]} d(f) = (-1)^{\binom{n}{2}} d(f)}$

(b) for $d \in F^\times$, let $\overline{d}$ be its image in $F^\times / F^{\times 2}$

Note: (1) f regular and $f \sim f' \Rightarrow f'$ regular and $\overline{d(f)} = \overline{d(f')} \in F^\times / F^{\times 2}$.

---

(2) $d(f \perp g) = d(f)\, d(g)$

(3) $d_\pm(f \perp g) = d_\pm(f)\, d_\pm(g)\, (-1)^{\dim(f)\dim(g)}$

(4) $f \sim f'$, $g \sim g' \Rightarrow f \perp g \sim f' \perp g'$

Geometric formulation

V = F-vector space, $\dim_F(V) = n \geq 0$

$B: V \times V \longrightarrow F$ symmetric bilinear form, $f(u) := B(u,u)$

$f: V \longrightarrow F$ is a quadratic form and $B(u,v) = \frac{1}{2}(f(u+v) - f(u) - f(v))$

(V, f) is a <u>quadratic space</u> over F

choice of a basis $\{e_i\}$ of V: $f\left(\sum_{i=1}^{n} x_i e_i\right)$ will be a quadratic form (as a polynomial in $\{x_i\}$). Another basis $\{e_i'\}$ of V: $f\left(\sum_{i=1}^{n} x_i' e_i'\right)$ will be equivalent to $f\left(\sum_{i=1}^{n} x_i e_i\right)$.

<u>Orthogonality</u>: B induces a linear map

$$\begin{array}{ccc} \widetilde{B}: V & \longrightarrow & V^* \\ \cup & & \cup \\ v_1 & \longmapsto & (v_2 \longmapsto B(v_1, v_2)) \end{array}$$

equal to its dual $\widetilde{B}^*: V \simeq V^{**} \longrightarrow V^*$.

($A = {}^tA$ = the matrix of $\widetilde{B}$ w.r.t. $\{e_i\}$ and $\{e_i^*\}$)

For an F-vector subspace $U \subset V$,

$$U^\perp := \{v \in V \mid \forall u \in U \quad B(u,v) = 0\} = \mathrm{Ker}\left(V \xrightarrow{\widetilde{B}} V^* \xrightarrow{\text{res}} U^*\right)$$

<u>Note</u>: (a) (V, f) is <u>regular</u> (or nondegenerate) $\Longleftrightarrow$ $\widetilde{B}$ is an isomorphism $\Longleftrightarrow$ $V^\perp = \{0\}$.

(b) If (V, f) is <u>regular</u>, then (for each subspace $U \subset V$)

$$\dim(U^\perp) = \underbrace{\dim(V^*)}_{\dim(V)} - \underbrace{\dim(U^*)}_{\dim(U)} \quad \text{(since res is surjective)}$$

$$\Rightarrow \dim((U^\perp)^\perp) = \dim(U) \Rightarrow \underline{U = (U^\perp)^\perp} \quad (\text{since } U \subset (U^\perp)^\perp).$$

<u>Def</u>: $(V, f) \perp (W, g) := (V \oplus W, \; f(v) + g(w))$

<u>Prop</u>. If $U \subset (V, f)$ is a subspace such that $(U, f|_U)$ is <u>regular</u>, then $\underline{V = U \perp U^\perp}$.

<u>Pf</u>. $\forall v \in V$ the linear form $\begin{array}{ccc} U & \longrightarrow & F \\ \cup & & \cup \\ u & \longmapsto & B(v,u) \end{array}$ is of the form

$u \longmapsto B(\mathrm{pr}(v), u)$ for unique $\mathrm{pr}(v) \in U \Rightarrow$ for each $u \in U$

$B(v - \mathrm{pr}(v), u) = 0 \Rightarrow v - \mathrm{pr}(v) \in U^\perp \Rightarrow v = \underset{\cup}{\mathrm{pr}(v)} + \underset{\cup U^\perp}{(v - \mathrm{pr}(v))} \Rightarrow$

$\Rightarrow V = U + U^\perp$. But $U \cap U^\perp = \{0\}$, since $f|_U$ is regular, hence $V = U \oplus U^\perp$. As $U \perp U^\perp \Rightarrow V = U \perp U^\perp$.

<u>Cor 1</u>. If $v \in V$, $a := f(v) \neq 0 \Rightarrow (F \cdot v, f|_{F \cdot v})$ is regular $\Rightarrow V = \underbrace{(F \cdot v)}_{\langle a \rangle} \perp (F \cdot v)^\perp$

<u>Cor 2</u>. $(V, f) = \underbrace{\langle a_1, \ldots, a_m \rangle}_{\neq 0 \text{ regular}} \perp \underbrace{\langle 0, \ldots, 0 \rangle}_{\dim = n - m}$

$V^\perp$.

Def. (V,f) **represents** $a \in F$ if $\exists\, v \in V \setminus \{0\}$ $\quad f(v) = 0$

(V,f) is **universal** if it represents all $a \in F$

Def. Regular (V,f) is **isotropic** if $\exists\, v \in V \setminus \{0\}$ $\quad f(v) = 0$

(**anisotropic** otherwise) $\qquad$ v is an **isotropic vector**

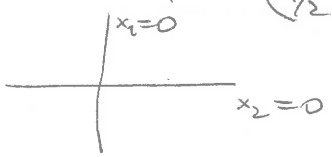
$C(f) := \{v \in V \mid f(v) = 0\} \subset V$ the **isotropic cone** of f

Ex 1. The **hyperbolic plane** H: $f(x_1, x_2) = x_1 x_2$, $A = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

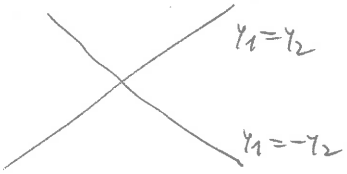
$f \sim y_1^2 - y_2^2 = \langle 1, -1 \rangle = f'$

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

$C(f)$:

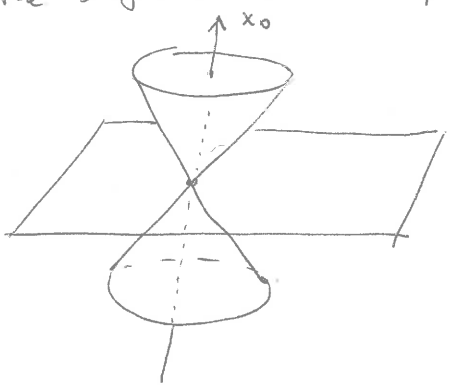


$C(f')$:



Ex 2. $F = \mathbb{R}$, $f = x_0^2 - x_1^2 - x_2^2 - x_3^2$

$C(f)$ = the light cone in special theory of relativity



Prop. Regular (V,f) is **isotropic** $\iff \exists\, H = \langle 1, -1 \rangle \subset V$ $\quad (\Rightarrow V = H \perp H^{\perp}$, $\Rightarrow V$ is **universal**)

Pf: $\Leftarrow$ OK; $\Rightarrow$ $\exists\, v_1 \in V \setminus \{0\}$ $\quad f(v_1) = 0$.

V regular $\Rightarrow$ $\exists\, u \in V$ $\quad B(u, v_1) = 1$. For any $t \in F$,

$B(v_1, u + t v_1) = 1$, $\quad f(u + t v_1) = f(u) + 2t$. Take $t := -\frac{f(u)}{2}$;

then $\quad H = (F v_1 \oplus F(u + t v_1)) \subset V$.

Cor 1. $\forall\, a \in F^{\times}$ $\quad \langle a, -a \rangle \sim H = \langle 1, -1 \rangle$

Cor 2. (V,f) regular, $\dim(V) = n \Rightarrow$ $\quad f \perp (-f) \sim nH = \underbrace{H \perp \dots \perp H}_{n \text{ times}}$

$(V \sim \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle$, $\quad \langle a_i \rangle \perp \langle -a_i \rangle \sim H)$

Cor 3. Regular (V,f) of $\dim(V) = 2$ is **isotropic** $\iff \overline{d(f)} = \overline{-1}$

Pf: $\Rightarrow$ f isotropic $\Rightarrow H \subset (V,f) \Rightarrow H \sim (V,f) \Rightarrow \overline{d(f)} = \overline{-1}$

$\Leftarrow$ $f \sim \langle a_1, a_2 \rangle$. If $\overline{a_1 a_2} = \overline{-1} \Rightarrow f \sim \langle a_1, -a_1 \rangle \sim H$.

Cor 4. Regular (V,f) of $\dim(V)=3$ is isotropic $\Leftrightarrow$ f represents $-d(f)$.

Pf: $\Rightarrow$ regular + isotropic $\Rightarrow$ universal

$\Leftarrow$ if $\exists v\in V$ $f(v)=-d(f)$, then $V=\underbrace{(F\cdot v)}_{\langle d(f)\rangle}\perp\underbrace{(F\cdot v)^{\perp}}_{\sim\langle a,b\rangle}$

$\overline{d(f)}=\overline{-d(f)}\cdot\bar{a}\cdot\bar{b}\Rightarrow\bar{b}=\overline{-a}\Rightarrow\langle a,b\rangle\sim\langle a,-a\rangle\sim H\Rightarrow V$ isotropic

---

Prop. (important!) Let $f(x_1,\dots,x_m)$, $g(y_1,\dots,y_n)$ be regular quadratic forms

Then: $f\perp(-g)=\underbrace{f(x_1,\dots,x_m)-g(y_1,\dots,y_n)}_{m+n\text{ variables}}$ is isotropic $\Leftrightarrow$ $\exists a\in F^{\times}$ represented by both f and g.

Pf: $\Leftarrow$ If $a=f(u)=g(v)\Rightarrow\underset{\uparrow F^m}{u},\underset{\uparrow F^n}{v}\neq 0$, $(f\perp(-g))\binom{u}{v}=f(u)-g(v)=0$.

$\Rightarrow$ $\exists\binom{u}{v}\neq 0\in F^{m+n}$ $f(u)-g(v)=0$. Say, $u\neq 0\in F^m$. If $f(u)\neq 0$, take $a:=f(u)=g(v)$. If $f(u)=0$, then f is isotropic $\Rightarrow$ f represents any non-zero value of g.

Cor. If f is regular and $a\in F^{\times}$, then:

f represents $a\Leftrightarrow f\perp\langle -a\rangle$ is isotropic

$\Updownarrow$

$f\sim\langle a\rangle\perp g$ for some g

Isometries (abstract version of equivalences)

Def. An isometry between quadratic spaces (V_1,f_1) and (V_2,f_2) is an isomorphism of F-vector spaces $\alpha:V_1\xrightarrow{\sim}V_2$ such that

$\forall v_1\in V_1$ $f_1(v_1)=f_2(\alpha(v_1))$ $\left(\Leftrightarrow\forall u_1,v_1\in V_1\quad B_1(u_1,v_1)=B_2(\alpha(u_1),\alpha(u_2))\right)$

Def. If (V,f) is regular, its auto-isometries $\alpha:(V,f)\xrightarrow{\sim}(V,f)$ form the orthogonal group $O(V,f)$. In matrix form:

$V=F^n$, $f(x)={}^tx\,A\,x$, $A={}^tA\in M_n(F)$

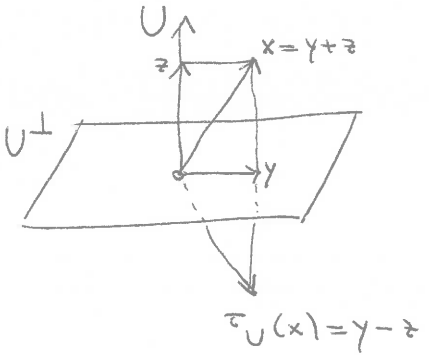
$O(V,f)=\{U\in GL_n(F)\mid {}^tUAU=A\}$ $\quad(\Rightarrow\det(U)=\pm 1)$.

$=\underbrace{O^+(V,f)\amalg O^-(V,f)}_{SO(V,f)}$ $\quad\det(O^{\pm}(V,f))=\pm 1$

Orthogonal symmetries

Given: $U \subset (V, f)$ such that $(U, f|_U)$ is regular $\Longrightarrow V = U \perp U^\perp$

$x = z + y$



$$\tau_U : V = \begin{pmatrix} U \\ \oplus \\ U^\perp \end{pmatrix} \longrightarrow V = \begin{pmatrix} U \\ \oplus \\ U^\perp \end{pmatrix}$$

$$x = \begin{pmatrix} z \\ y \end{pmatrix} \longmapsto \begin{pmatrix} -z \\ y \end{pmatrix} =: \tau_U(x)$$

symmetry with respect to $U^\perp$

$\tau_U|_U = -id$, $\tau_U|_{U^\perp} = id$

Reflection (w.r.t. the hyperplane $u^\perp$): if $u \in V$, $f(u) \neq 0$, $U = F \cdot u$

$$\boxed{\tau_u(x) = x - \frac{2B(u,x)}{f(u)}\, u}$$

$\det(\tau_u) = -1$

$\det(\tau_U) = (-1)^{\dim(U)}$

Witt's theorems

Witt's Cancellation Thm: $\left.\begin{array}{l} f_1 \sim f_2 \text{ regular} \\ f_1 \perp g_1 \sim f_2 \perp g_2 \end{array}\right\} \Longrightarrow g_1 \sim g_2$.

Geometric version: Given subspaces $U_1, U_2 \subset (V, f)$ with U_1 regular, every isometry $(U_1, f|_{U_1}) \xrightarrow{\sim} (U_2, f|_{U_2})$ extends to an isometry $\sigma : (V, f) \xrightarrow{\sim} (V, f)$ $(\sigma \in O(V, f))$.

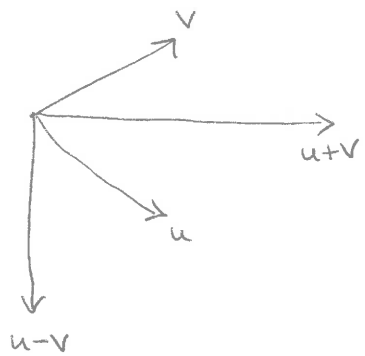
Cor: $U_1^\perp$ is isometric to $U_2^\perp$ (by σ) $\Longrightarrow$ Cancellation Thm

---

Pf of the geometric version: enough to prove the following

Special case: if $u, v \in V$, $f(u) = f(v) \neq 0 \Longrightarrow \exists \sigma \in O(V, f)$ $\sigma(u) = v$

($U_1 = F \cdot u$, $U_2 = F \cdot v$), and then argue by induction on $\dim(U_1)$.



If $f(u-v) \neq 0 \Longrightarrow \tau_{u-v} : u \longmapsto v$ $(\sigma = \tau_{u-v})$

If $f(u+v) \neq 0 \Longrightarrow \tau_{u+v} : u \longmapsto -v \xrightarrow{\tau_v} v$ $(\sigma = \tau_v \tau_{u+v})$

Note: $f(u+v) + f(u-v) = 2(f(u)+f(v)) = 4f(u) \neq 0$,

so $f(u+v) \neq 0$ or $f(u-v) \neq 0$.

Totally isotropic subspaces

Def. A (vector) subspace $U \subset (V,f)$ is **totally isotropic** if $f|_U = 0$
($\iff U \subset C(f) \iff B|_{U\times U} = 0 \iff U \subset U^\perp$).

Note. If (V,f) is **regular**, then the inclusion $U \subset U^\perp$ implies that
$2\dim(U) \le \dim(U) + \dim(U^\perp) = \dim(V)$.

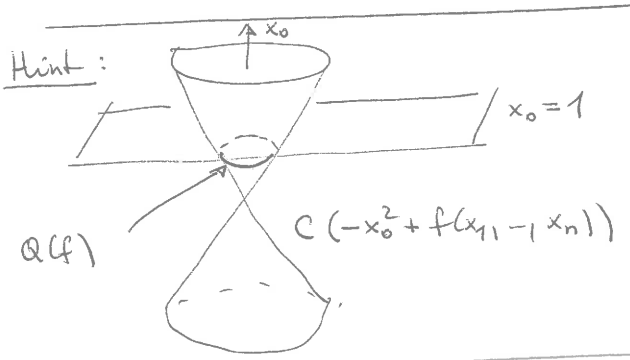
Ex: $\Delta(W) = \{(w,w) \mid w \in W\}$ is totally isotropic in
$(W,g) \perp (W,-g)$ [if $g \sim \langle a_1,\dots,a_n\rangle$ is regular, then
$g \perp (-g) \sim \langle a_1,-a_1\rangle \perp \dots \perp \langle a_n,-a_n\rangle = nH$]

Exercise. If (V,f) is **regular**, then
$\max\{\dim(U) \mid U \subset (V,f)$ totally isotropic$\} = \max\{r \ge 0 \mid rH \subset (V,f)\}$

Exercise (a) Describe a relation between affine subspaces $W \subset (V,f)$ contained in the affine quadric $Q(f) = \{v \in V \mid f(v) = 1\}$ and totally isotropic subspaces of $(V,f) \perp \langle -1\rangle$.

(b) Determine $\max\{\dim(W) \mid W \subset \mathbb{R}^{m+n}$ affine subspace contained in $\{x \in \mathbb{R}^{m+n} \mid x_1^2 + \dots + x_m^2 - x_{m+1}^2 - \dots - x_{m+n}^2 = 1\}\}$

Hint:



Def. Regular (V,f) is **split** if there exists totally isotropic $U \subset (V,f)$ of maximal possible dimension $\dim(U) = [\dim(V)/2]$

$\Updownarrow$

$V \simeq nH$ or $V \sim nH \perp \langle a\rangle$

Equivalences between diagonal forms

Note: $A, B \in F^\times$, $A+B \neq 0 \Rightarrow \langle A, B\rangle \sim \langle A+B, \frac{AB}{A+B}\rangle$ (*)

$\Rightarrow$ if $A_i \in F^\times$, $\forall j \le m$ $\sum_{i=1}^{j} A_i \neq 0 \Rightarrow \langle A_1,\dots,A_m\rangle \sim \langle A_1+A_2, A_3, \frac{A_1A_2}{A_1+A_2},\dots\rangle \sim \dots \sim \langle A_1+\dots+A_m, \dots\rangle$.

Prop. If $\langle a_1,\dots,a_n\rangle \sim \langle b_1,\dots,b_n\rangle$, then there is a chain of equivalences in between of the form $\langle c_1,\dots,c_i,\dots,c_n\rangle \sim \langle c_1,\dots,t^2c_i,\dots,c_n\rangle$ or $\langle c_1,\dots,c_i,\dots,c_j,\dots,c_n\rangle \overset{(*)}{\sim} \langle c_1,\dots,c_i+c_j,\dots,\frac{c_ic_j}{c_i+c_j},\dots,c_n\rangle$ } "elementary equivalences"

Pf: $\exists$ minimal $m \ge 1$, $I \subset \{1,\dots,n\}$, $|I| = m$, $b_1 = \sum_{i\in I} a_i t_i^2$, $t_i \in F^\times$
Say, $I = \{1,\dots,m\}$. If $m = 1$ $\overset{\text{Witt}}{\Longrightarrow} \langle a_2,\dots,a_n\rangle \sim \langle b_2,\dots,b_n\rangle \Leftarrow$ apply induction.
By the above, get a chain of elementary equivalences
$\langle a_1,\dots,a_n\rangle \sim \dots \sim \langle b_1, a_2', \dots, a_n'\rangle \overset{\text{Witt}}{\Longrightarrow} \langle a_2',\dots,a_n'\rangle \sim \langle b_2,\dots,b_n\rangle$.

Rmks: (1) f represents $a \in k^\times \iff f \sim \langle a \rangle \perp g \iff f \perp \langle -a \rangle$ is isotropic (diagonalisation)

Pf (of the nontrivial implication): if $\begin{pmatrix} x \\ t \end{pmatrix} \in k^{n+1} \setminus \{0\}$ and $f(x) - at^2 = 0$, then either $t \neq 0$ ($\Rightarrow f(t^{-1}x) = a$), or $t = 0 \Rightarrow x \in k^n \setminus \{0\}$, $f(x) = 0 \Rightarrow f$ is isotropic $\Rightarrow$ f represents a.

---

(2) Every regular f is equivalent to $f \sim \underbrace{H \perp \dots \perp H}_{m\,H} \perp f_{an}$, where $m \in \mathbb{N}$ and f_{an} is anisotropic ($f_{an} = 0$ of $\dim = 0$ is allowed).

We say that f_{an} is the anisotropic kernel of f.

Witt's cancellation thm implies: f, g regular, $f \sim g \Rightarrow f_{an} \sim g_{an}$.

Ex: ($k = \mathbb{R}$), $f \sim r\langle 1 \rangle \perp s\langle -1 \rangle = \begin{cases} \underbrace{(r-s)\langle 1 \rangle}_{f_{an}} \perp sH & \text{if } r \geq s \\ \underbrace{(s-r)\langle -1 \rangle}_{f_{an}} \perp rH & \text{if } r \leq s. \end{cases}$

Def: regular f, g are Witt-equivalent if $\exists m, n \in \mathbb{N}$ $f \perp mH \sim g \perp nH$ ($\iff f_{an} \sim g_{an}$). The Witt-equivalence classes (= the equivalence classes of isotropic forms) of regular quadratic forms over k form a commutative ring $W(k)$ (the Witt ring of k).

sum $\longleftrightarrow \perp$, product $\longleftrightarrow \otimes$, inverse $\longleftrightarrow (f \mapsto -f)$.

Ex: ($k = \mathbb{R}$) (classes of) anisotropic forms: $r\langle 1 \rangle$, 0, $s\langle -1 \rangle$ $(r, s \in \mathbb{N}_+)$

Witt-equiv class of $(r\langle 1 \rangle \perp s\langle -1 \rangle) \in W(\mathbb{R})$

$\downarrow$ $\qquad\qquad$ $\downarrow$ signature

$r - s \in \mathbb{Z}$

$r \mapsto r$, $0 \mapsto 0$, $s\langle -1 \rangle \mapsto -s$

($k = \mathbb{C}$) (classes of) anisotropic forms: 0, $\langle 1 \rangle$

$\dim \pmod 2 : W(\mathbb{C}) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$

$\langle 1, 1 \rangle \sim H$

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

Let $k = \mathbb{F}_p$, $p \neq 2$ prime, $a_i \in \mathbb{F}_p^\times$ $(i \geq 1)$. We know that:

(A) $\forall a_1, a_2, a_3 \in \mathbb{F}_p^\times \quad \exists x, y \in \mathbb{F}_p \quad a_1x^2 + a_2y^2 = a_3$

(B) $\mathbb{F}_p^\times / \mathbb{F}_p^{\times 2} = \{\overline{1}, \overline{u}\}$, for any $u \in \mathbb{F}_p^\times$ such that $\left(\frac{u}{p}\right) = -1$

Note: $\overline{-1} = \begin{cases} \overline{1} & \text{if } p \equiv 1 [4] \\ \overline{u} & \text{if } p \equiv 3 [4] \end{cases}$

Below: f regular quadratic form of $\dim(f) = n \geq 1$ over $\mathbb{F}_p$.

Consequences: (i) $n \geq 3 \Rightarrow f$ is isotropic

(ii) $n = 2 \Rightarrow f$ represents every element of $\mathbb{F}_p^\times \Rightarrow$

$\Rightarrow \forall a_1, a_2, a_3 \in \mathbb{F}_p^\times \quad \langle a_1, a_2 \rangle \sim \left\langle a_3, \frac{a_1 a_2}{a_3} \right\rangle \Rightarrow \langle a_1, a_2 \rangle \sim \langle 1, a_1 a_2 \rangle$.

(iii) Induction ($\forall n \geq 2$): $\forall a_1, \dots, a_n \in \mathbb{F}_p^\times \ \forall b_1, \dots, b_{n-1} \in \mathbb{F}_p^\times$

$$f = \langle a_1, \dots, a_n \rangle \sim \langle \underbrace{1, \dots, 1}_{n-1}, \underbrace{a_1 \cdots a_n}_{d(f)} \rangle \sim$$

$$\sim \langle b_1, \dots, b_{n-1}, d(f)/(b_1 \cdots b_{n-1}) \rangle$$

(iv) Special case: $\forall k \geq 2$

$$\langle a_1, \dots, a_{2k-1} \rangle \sim \underbrace{\langle 1, -1 \rangle \perp \dots \perp \langle 1, -1 \rangle}_{(k-1)H} \perp \langle \underbrace{(-1)^{k-1} a_1 \cdots a_{2k-1}}_{d_\pm(f)} \rangle$$

$$\langle a_1, \dots, a_{2k} \rangle \sim \underbrace{\langle 1, -1 \rangle \perp \dots \perp \langle 1, -1 \rangle}_{} \perp \langle -1, \underbrace{(-1)^k a_1 \cdots a_{2k}}_{d_\pm(f)} \rangle$$

(v) Anisotropic forms: $\underbrace{0}$, $\underbrace{\langle 1 \rangle, \langle u \rangle}$, $\underbrace{\langle 1, -u \rangle}$ $\sim \langle -1, u \rangle$

(equivalence classes of) $\dim = 0$, $\dim = 1$, $\dim = 2$

(vi) If $2 \nmid \dim(f) \Rightarrow f_{an} = \langle d_\pm(f) \rangle$

If $2 \mid \dim(f) \Rightarrow f_{an} = \begin{cases} 0, & \text{if } \overline{d_\pm(f)} = \overline{1} \\ \langle 1, -u \rangle, & \text{if } \overline{d_\pm(f)} = \overline{u}. \end{cases}$

(vii) $\{\text{regular quadratic forms over } \mathbb{F}_p \text{ of } \dim > 0\} / \text{equivalence} \xrightarrow{\sim} \mathbb{N}_+ \times \{\pm 1\}$ bijection

$$f \longmapsto \left(\dim(f), \left(\frac{d(f)}{p}\right)\right)$$

$$\langle \underbrace{1, 1, \dots, 1}_{n \geq 1} \rangle \longmapsto (n, +1)$$

$$\langle \underbrace{1, \dots, 1}_{n-1}, u \rangle \longmapsto (n, -1)$$

(viii) $\langle 1, 1 \rangle \sim \begin{cases} H, & p \equiv 1 [4] \\ \langle 1, -u \rangle, & p \equiv 3 [4] \end{cases} \Rightarrow \left(W(\mathbb{F}_p), +\right) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, & p \equiv 1 [4] \\ \mathbb{Z}/4\mathbb{Z}, & p \equiv 3 [4] \end{cases}$

Exercise. What is the product structure of $W(\mathbb{F}_p)$?

Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

Any regular quadratic form f over $\mathbb{Q}_p$ is equivalent to

$$f \sim \underbrace{\langle a_1, \dots, a_m \rangle}_{f_0} \perp \underbrace{\langle pb_1, \dots, pb_n \rangle}_{pf_1}, \quad \text{where } a_i, b_j \in \mathbb{Z}_p^\times. \quad (f_1 = \langle b_1, \dots, b_n \rangle) \qquad (*)$$

From now on: $p \neq 2$, $a_i, b_j \in \mathbb{Z}_p^\times$. Notation: $\mathbb{Q}_p^\times \longrightarrow \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$, $a \longmapsto \overline{a}$

Recall: $\mathbb{Z}_p^\times / \mathbb{Z}_p^{\times 2} \xrightarrow{\sim} \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2}$. Fix $u \in \mathbb{Z}_p^\times$ such that $\left(\frac{u \pmod p}{p}\right) = -1$. Then $\mathbb{Z}_p^\times / \mathbb{Z}_p^{\times 2} = \{\overline{1}, \overline{u}\}$ and $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} = \{\overline{1}, \overline{u}, \overline{p}, \overline{pu}\}$.

Again, $\overline{-1} = \begin{cases} \overline{1}, & p \equiv 1 \ [4] \\ \overline{u}, & p \equiv 3 \ [4] \end{cases}$.

Hensel's lemma implies (see Prop. ... above):

(A) f is anisotropic over $\mathbb{Q}_p \iff f_0 \pmod p$ and $f_1 \pmod p$ are anisotropic over $\mathbb{F}_p$.

(B) f_0 represents $a \in \mathbb{Z}_p^\times$ over $\mathbb{Q}_p \iff$ $f_0 \pmod p$ represents $a \pmod p$ over $\mathbb{F}_p$. (always true if $\dim(f_0) \geq 2$.)

Consequences (as over $\mathbb{F}_p$, $p \neq 2$): below, a_i, b_j, f, f_0, f_1 are as in $(*)$

(i) $\dim(f_j) \geq 3$ $(j = 0, 1) \Rightarrow f_j$ is isotropic over $\mathbb{Q}_p$.

(ii) f_j $(j = 0, 1)$ is anisotropic $\iff f_j \sim \begin{cases} 0 \\ \langle 1 \rangle \\ \langle u \rangle \\ \langle 1, -u \rangle \end{cases}$

(iii) f is anisotropic $\iff f \sim \begin{cases} 0 \\ \langle 1 \rangle \\ \langle u \rangle \\ \langle 1, -u \rangle \end{cases} \perp \begin{cases} 0 \\ \langle p \rangle \\ \langle pu \rangle \\ \langle p, -pu \rangle \end{cases}$ $2^4 = 16$ classes (distinct! – exercise) of such forms

dim	0	1	2	3	4	≥ 5
anisotropic f	0	$\langle 1 \rangle$	$\langle 1, p \rangle$	$\langle 1, p, -pu \rangle$	$\langle 1, -u, p, -pu \rangle$	
		$\langle u \rangle$	$\langle 1, pu \rangle$	$\langle u, p, -pu \rangle$		
		$\langle p \rangle$	$\langle u, p \rangle$	$\langle 1, -u, p \rangle$		
		$\langle pu \rangle$	$\langle u, pu \rangle$	$\langle 1, -u, pu \rangle$		
			$\langle 1, -u \rangle$			
			$\langle p, -pu \rangle$			

(iv) $\dim(f) \geq 5 \Rightarrow f$ is isotropic over $\mathbb{Q}_p$.

($\Longleftarrow \dim(f_0) \geq 3$ or $\dim(f_1) \geq 3$ $\Uparrow$ (B))

(v) $f_{an} = (f_0)_{an} \perp p(f_1)_{an}$ (by (A))

(vi) (As over $\mathbb{F}_p$, $p \neq 2$) $\langle a_1, a_2 \rangle \sim \langle a_3, \frac{a_1 a_2}{a_3} \rangle$, $f_0 \sim \langle \underbrace{1, \dots, 1}_{m-1}, \underbrace{a_1 \cdots a_m}_{d(f_0)} \rangle$

$$(f_j)_{an} = \begin{cases} \langle d_\pm(f_j) \rangle, & \text{if } 2 \nmid \dim(f_j) \\ 0, & \text{if } 2 \mid \dim(f_j) \text{ and } \overline{d_\pm(f_j)} = \overline{1} \\ \langle -1, d_\pm(f_j) \rangle \sim \langle 1, -u \rangle & \text{if } 2 \mid \dim(f_j) \text{ and } \overline{d_\pm(f_j)} = \overline{u}. \end{cases}$$

$(j = 0, 1)$

(vii) Classification : assume $f \sim f_0 \perp p f_1$, $f' \sim f_0' \perp p f_1'$ are regular

$f \sim f' \iff \dim(f) = \dim(f')$ AND $f_{an} \sim f'_{an}$

$\iff$ ——— " ——— AND $\overline{d(f)} = \overline{d(f')}$

Lemma. If $\dim(f) = \dim(f')$ and $\overline{d(f)} = \overline{d(f')}$, then:

(1) $\left[\forall j = 0,1 \quad \dim(f_j) \equiv \dim(f_j') \pmod 2\right]$, (2) $\overline{d_\pm(f_0) d_\pm(f_1)} = \overline{d_\pm(f_0') d_\pm(f_1')}$.

(3) $(f_0)_{an} \sim (f_0')_{an} \iff \overline{d_\pm(f_0)} = \overline{d_\pm(f_0')} \overset{(2)}{\iff} \overline{d_\pm(f_1)} = \overline{d_\pm(f_1')} \iff (f_1)_{an} \sim (f_1')_{an}$.

Pf. Exercise.

Cor. $f \sim f' \iff \dim(f) = \dim(f')$ AND $\overline{d(f)} = \overline{d(f')} \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ AND

$\overline{d_\pm(f_0)} = \overline{d_\pm(f_0')} \in \mathbb{Z}_p^\times / \mathbb{Z}_p^{\times 2} \xrightarrow{\sim} \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2} \xrightarrow{\sim} \{\pm 1\}$.

(equivalently, $\overline{d_\pm(f_1)} = \overline{d_\pm(f_1')}$)

Exercise : $d_\pm(f \perp g) = d_\pm(f)\, d_\pm(g)\, (-1)^{\dim(f)\dim(g)}$

Exercise : compute the Hasse invariant $c_p(f)$ in terms of f_0 and f_1.

Answer : $c_p(f) = \left(\frac{d_\pm(f_1)}{p}\right) \left(\frac{d(f_0) d(f_1)}{p}\right)^{\dim(f_1)} = \left(\frac{d_\pm(f_1)}{p}\right) \left(\frac{d(f) p^{-v_p(d(f))}}{p}\right)^{v_p(d(f))}$

(viii) $(W(\mathbb{Q}_p), +) \xrightarrow{\sim} (W(\mathbb{F}_p), +)^{\oplus 2}$

$[f_{an}] \longmapsto [(f_0)_{an}], [(f_1)_{an}]$

Classification of quadratic forms (up to equivalence) over fields of small arithmetic complexity

Notation: F field, $\mathrm{char}(F) \neq 2$; all quadratic forms below will be regular (in particular, if $f = \langle a_1, \dots, a_n \rangle$, then $\forall i \ \ a_i \in F^\times$) $\quad d(f) = a_1 \cdots a_n$

$F^\times \longrightarrow F^\times / F^{\times 2}$, $a \longmapsto \overline{a}$

---

dim = 1: $\quad \langle a \rangle \sim \langle b \rangle \iff ab^{-1} \in F^{\times 2}$, and so

$$\{ f \mid \dim(f) = 1 \} / \sim \ \longleftrightarrow \ F^\times / F^{\times 2} \qquad \text{bijection}$$
$$f = \langle a \rangle \ \longmapsto \ \overline{a} = \overline{d(f)}$$

---

dim = 2: **Prop.** $\underbrace{\langle a, b \rangle}_{f} \sim \underbrace{\langle a', b' \rangle}_{f'} \iff \underbrace{\overline{d(f)}}_{\overline{ab}} = \underbrace{\overline{d(f')}}_{\overline{a'b'}}$ and

a' is represented by $\langle a, b \rangle$

$(\iff 1$ is represented by $\langle a/a', b/a' \rangle \sim \langle aa', ba' \rangle)$

Pf: $(\Rightarrow)$ automatic

$(\Leftarrow)$ if $a' \in F^\times$ is represented by $\langle a, b \rangle$, then the diagonalisation procedure (completing the square) gives $\langle a, b \rangle \sim \langle a', b' \rangle$, for some $b' \in F^\times$. Necessarily, $\overline{ab} = \overline{a'b'}$.

Need to analyse: the condition "a' is represented by $\langle a, b \rangle$"

$(\iff 1$ ——— " ——— $\langle aa', ba' \rangle)$

Recall: If f, f' are regular quadratic forms over F and $a \in F^\times$, then:

(1) f is isotropic $\iff f \sim g \perp \langle 1, -1 \rangle$ for some g.

(2) f represents $a \iff f \sim \langle a \rangle \perp g$ for some g

$\iff f \perp \langle -a \rangle$ is isotropic

(3) f, f' represent the same $b \in F^\times \iff f \perp (-f')$ is isotropic

---

Cor 1. If $\dim(f) = 2$, then: f is isotropic $\iff \overline{-d(f)} = \overline{1}$

Pf: $(\Rightarrow)$ (1) above; $(\Leftarrow)$ $f \sim \langle a, b \rangle$, $-ab = c^2 \Rightarrow \overline{b} = \overline{-a}$, $f \sim \langle a, -a \rangle$ isotropic

Cor 2. For $a, b \in F^\times$, it is equivalent:

the equation $ax^2 + by^2 = z^2$ has a solution $(x, y, z) \in F^3 - \{(0,0,0)\}$

$\Updownarrow$

$\langle 1, -a, -b \rangle$ is isotropic $\iff \langle a, b \rangle$ represents 1

$\Updownarrow$

$\langle 1, -a \rangle$ represents b

$\Updownarrow$

$\langle 1, -b \rangle$ represents a

Summary: in order to determine $\{f \mid \dim(f)=2\}/\sim$, we need to understand, for each $b \in F^\times$, the set

$$\boxed{\begin{aligned} H_b &:= \{ a \in F^\times \mid a \text{ is represented by } \langle 1, -b\rangle \} \\ &= \{ \text{—"—} \mid \exists\, x,y \in F \quad a = x^2 - by^2 \} \end{aligned}}$$

Prop. (1) $H_b \subset F^\times$ is a subgroup containing $F^{\times 2}$.

(2) H_b depends only on $\overline{b} \in F^\times/F^{\times 2}$; denote by $\overline{H}_b \subset F^\times/F^{\times 2}$ the quotient group $H_b/F^{\times 2}$.

(3) If $b = c^2$ $(c \in F^\times)$, then $x^2 - by^2 = (x+cy)(x-cy)$

$\Rightarrow H_b = F^\times$ $\quad (\overline{b} = \overline{1} \Rightarrow H_b = H_1 = F^\times)$.

Pf. Need to show: H_b is a group (the rest is automatic)

in the case $b \notin F^{\times 2}$

Then $F(\sqrt{b}) = \{x + y\sqrt{b} \mid x,y \in F\}$ is a field,

$\alpha \longmapsto \alpha' = x - y\sqrt{b}$ is a field automorphism and the norm

$N(\alpha) = \alpha\alpha' = x^2 - by^2$ is a group homomorphism

$N: F(\sqrt{b})^\times \longrightarrow F^\times \Longrightarrow$ its image $\mathrm{Im}(N) = H_b \subset F^\times$ is a subgroup

---

This argument works for any $b \in F^\times$, if we replace $F(\sqrt{b})$ by $F_1 := F[T]/(T^2 - b)$ and $\sqrt{b}$ by $\overline{T} = T \pmod{(T^2-b)} \in F_1$.

(if $b = c^2$, $c \in F^\times$, then $T^2 - b = (T-c)(T+c)$ and

$$F_1 \xrightarrow{\sim} F[T]/(T-c) \times F[T]/(T+c) \xrightarrow{\sim} F \times F$$

$$P(T) \pmod{(T^2-c^2)} \longmapsto P(c), P(-c)$$

The involution on $F \times F$ is $(u,v)' = (v,u)$ and $N((u,v)) = uv$.

Summary: $\boxed{1 \text{ is represented by } \langle a, b\rangle \Longleftrightarrow a \in H_b \Longleftrightarrow b \in H_a}$

Cor. a' is represented by $\langle a, b\rangle \Longleftrightarrow aa'$ is represented by $\langle 1, a'b\rangle$

$\Longleftrightarrow aa' \in H_{-a'b} \Longleftrightarrow a' \in a\, H_{-ab}$.

Prop. Given $d \in F^\times$, there is a bijection

$$\begin{array}{ccc} \{f \mid \dim(f) = 2,\ \overline{d(f)} = \overline{d}\} & \longleftrightarrow & F^\times/H_{-d} \\ \Psi & & \downarrow \\ \langle a, d/a\rangle & \longmapsto & a\, H_{-d} \end{array}$$

(f is isotropic $\Longleftrightarrow \overline{-d} = \overline{1}$)

Ex. (1) If $F^\times = F^{\times 2}$ (e.g., if $F=\mathbb{C}$), then $\forall b \in F^\times \quad H_b = F^\times$

(2) If $F=\mathbb{R}$, then $\mathrm{sgn}: F^\times/F^{\times 2} \xrightarrow{\sim} \{\pm 1\}$, $H_b = \begin{cases} \mathbb{R}^\times & b>0 \\ \mathbb{R}^\times_{>0} & b<0 \end{cases}$

(3) If $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $p\neq 2$ prime, then $\forall a,b \in F^\times \quad a = x^2 - by^2$ a une solution $x,y \in \mathbb{F}_p \Rightarrow \forall b \in F^\times \quad H_b = F^\times$.

The same holds for $F=\mathbb{F}_{p^r}$ if $p\neq 2$, $r\geq 1$ ($F^\times$ is cyclic of order $q-1$, p^r-1 (even))

$\Rightarrow F^\times/F^{\times 2} = \{\pm 1\}$, $|F^{\times 2}| = \frac{q-1}{2}$, $|\{x^2 \mid x\in F\}| = |\{a+by^2 \mid y\in F\}| = \frac{q+1}{2}$.

Fields F such that $\forall b \in F^\times \quad H_b = F^\times$

($\Leftrightarrow$ every regular f of $\dim = 2$ represents every $a \in F^\times$)

($\Leftrightarrow$ every regular f $\dim = 3$ is isotropic)

Basic example: $F=\mathbb{F}_q$, $q=p^r$, $p\neq 2$ ($\Rightarrow F^\times/F^{\times 2} \xrightarrow{\sim} \{\pm 1\}$)

By definition, $\forall a,b,c \in F^\times \quad \langle a,b\rangle \sim \langle c, \frac{ab}{c}\rangle$

Therefore: if $f \sim \langle a_1, \dots, a_n\rangle$, $\overline{d(f)} = \overline{a_1 \cdots a_n}$, then

$$f \sim \langle \underbrace{1, \dots, 1}_{n-1}, d(f)\rangle$$

Prop: $\forall n \geq 1$

$$\{f \mid \dim(f)=n\}/\sim \;\longleftrightarrow\; F^\times/F^{\times 2} \quad \text{bijection}$$
$$f \;\longmapsto\; \overline{d(f)}$$
$$\langle 1,1,\dots,1,d\rangle \;\longleftarrow\; \bar{d}$$

Anisotropic forms: $\dim = 0$: $f=0$

$\dim = 1$: $f=\langle a\rangle$, $\bar{a} \in F^\times/F^{\times 2}$

$\dim = 2$: $f=\langle 1,-a\rangle$, $\bar{a} \in F^\times/F^{\times 2} \setminus \{\bar{1}\}$

Recall: for f of $\dim(f)=n$, the sign-determinant of f is defined as

$$d_\pm(f) := (-1)^{\binom{n}{2}} d(f) = (-1)^{\left[\frac{n}{2}\right]} d(f).$$

Then $d_\pm(f \perp g) = d_\pm(f)\, d_\pm(g)\, (-1)^{\dim(f)\dim(g)}$

Anisotropic kernels:

$n = \dim(f) = 2k+1$ $(k\geq 0)$: $f \sim \langle 1,-1,\dots,1,-1\rangle \perp \langle (-1)^k d(f)\rangle$

$\sim k\langle 1,-1\rangle \perp \langle d_\pm(f)\rangle$, $f_{an} = \langle d_\pm(f)\rangle$

$n = \dim(f) = 2k+2$ $(k\geq 0)$: $f \sim \underbrace{\langle 1,-1,\dots,1,-1\rangle}_{k\langle 1,-1\rangle} \perp \underbrace{\langle 1, (-1)^k d(f)\rangle}_{\sim \langle -1, (-1)^{k+1} d(f)\rangle}$

$(-1)^{k+1} d(f) = d_\pm(f)$

- If $\overline{d_\pm(f)} = \bar{1}$ $\Rightarrow$ $f \sim (k+1)\langle 1,-1\rangle$, $f_{an}=0$
- If $d_\pm(f) \neq \bar{1}$ $\Rightarrow$ $f_{an} = \langle 1, -d_\pm(f)\rangle$

[redacted]. Fields such that $F^{\times 2} \neq F^\times$ and

$$\forall b \in F^\times \quad (F^\times : H_b) = \begin{cases} 1, & b \in F^{\times 2} \\ 2, & b \notin F^{\times 2} \end{cases} \tag{H}$$

Ex: $F = \mathbb{R}, \mathbb{Q}_p$ (proof: later)

Prop. (1) If $b \notin F^{\times 2}$, then $\exists\, a \notin H_b$. For any such $a \in F^\times$, $b \notin H_a$ and

$$F^\times = H_b \amalg aH_b = H_a \amalg bH_a .$$

(2) $\bigcap_{a \in F^\times} H_a = F^{\times 2}$.

(3) $H_b = H_{b'} \iff \overline{b} = \overline{b'} \in F^\times / F^{\times 2}$.

(4) $aH_b \cap a'H_{b'} = \emptyset \iff \overline{b} = \overline{b'} \neq \overline{1}$ and $a'/a \notin H_b = H_{b'}$.

Pf. (1) automatic. (2) follows from (1).

(3) $\Leftarrow$ — ; $\Rightarrow$ If $H_b = H_{b'}$, then $\forall a \in F^\times$

$$\begin{cases} \text{either} & a \in H_b = H_{b'} \Rightarrow b, b' \in H_a \Rightarrow b'/b \in H_a \\ \text{or} & a \notin H_b, a \notin H_{b'} \Rightarrow b, b' \notin H_a \Rightarrow bH_a = F^\times \setminus H_a = b'H_a \Rightarrow b'/b \in H_a \end{cases}$$

so $b'/b \in \bigcap_{a \in F^\times} H_a \overset{(2)}{=} F^{\times 2}$.

(4) $\Leftarrow$ automatic; $\Rightarrow$ $aH_b \cap a'H_{b'} = \emptyset \Rightarrow \overline{b}, \overline{b'} \neq \overline{1}$ and

$$F^\times = aH_b \amalg acH_b = a'H_{b'} \amalg a'c'H_{b'} \quad \text{for any } c \notin H_b,\ c' \notin H_{b'}$$

$$\Rightarrow a'H_{b'} \subset acH_b \overset{1 \in H_{b'}}{\Longrightarrow} a'/ac \in H_b \Rightarrow acH_b = a'H_b \Rightarrow H_{b'} \subset H_b .$$

By symmetry, $H_b \subset H_{b'} \Rightarrow H_b = H_{b'} \overset{(3)}{\Longrightarrow} \overline{b} = \overline{b'}$ and $a'/a \in H_b = H_{b'}$.

We need to understand: when is $\langle a_1, \dots, a_n \rangle$ isotropic and when does $\langle a_1, \dots, a_n \rangle$ represent a ($\Leftrightarrow \langle a_1, \dots, a_n, -a \rangle$ isotropic).

dim = 2: we know that, $\forall d \in F^\times$,

$$\{ f \mid \dim(f) = 2,\ \overline{d(f)} = \overline{d} \} / \sim \overset{\text{bijection}}{\longleftrightarrow} F^\times / H_{-d} \quad \left(\simeq \begin{cases} \{1\}, & \overline{-d} = \overline{1} \\ \{\pm 1\}, & \overline{-d} \neq \overline{1} \end{cases} \right.$$

f isotropic $\Leftrightarrow \overline{-d} = \overline{1}$

Conclusion: (a) for each $\overline{d} \in F^\times / F^{\times 2} \setminus \{\overline{-1}\}$ there are two classes of f with $\dim(f) = 2$, $\overline{d(f)} = \overline{d}$, both anisotropic.

(b) there is one class with $\dim(f) = 2$, $\overline{d(f)} = \overline{-1}$, isotropic ($\sim \langle 1, -1 \rangle$)

Goal: given $f = \langle a_1, \dots, a_n \rangle$ $(a_i \in F^\times,\ d(f) = a_1 \cdots a_n)$ and $a \in F^\times$, decide between the following alternatives:

$$\left\{\begin{array}{ll} f\ (IS) & f \text{ isotropic} \\ f\ (AN) & f \text{ anisotropic} \end{array}\right\} \quad | \quad \left\{\begin{array}{ll} f\ R(a) & f \text{ represents } a \\ f\ NR(a) & f \text{ does not represent } a \end{array}\right\}$$

For F arbitrary:

(1) $f\ R(a) \iff (f \perp \langle -a \rangle)\ (IS)$

(2) $n=1$: $f\ R(a) \iff \overline{a} = \overline{a_1}$

(3) $n=2$: $f\ (IS) \iff \underbrace{\overline{-d(f)}}_{d_\pm(f)} = \overline{1}$

(4) $n=3$: $f\ (IS) \iff f\ R(\underbrace{-d(f)}_{d_\pm(f)})$

(5) $n=3$: $f\ (AN) \iff -a_1a_3 \notin H_{-a_1a_2}$ $\left(\iff -a_1a_2 \notin H_{-a_1a_3}\right)$

For F satisfying (H):

(6) $n=4$: $f\ (AN) \iff \left[\underbrace{\overline{d(f)} = \overline{1}}_{d_\pm(f)} \text{ and } \underbrace{-a_1a_3 \notin H_{-a_1a_2}}_{\langle a_1, a_2, a_3 \rangle\ (AN)}\right]$

Pf: $\langle a_1, a_2, a_3, a_4 \rangle\ (AN) \iff \left[\forall\, b \in F^\times \quad \underbrace{\langle a_1, a_2 \rangle\ NR(b)}_{b \notin a_1 H_{-a_1a_2}} \text{ or } \underbrace{\langle -a_3, -a_4 \rangle\ NR(b)}_{b \notin (-a_3) H_{-a_3a_4}}\right]$

$\iff a_1 H_{-a_1a_2} \cap (-a_3) H_{-a_3a_4} = \emptyset \iff \left[\underbrace{\overline{-a_1a_2} = \overline{-a_3a_4}}_{\overline{d(f)} = \overline{1}} \text{ and } -a_1a_3 \notin H_{-a_1a_2} = H_{-a_3a_4}\right]$

Using (1)–(6), we can complete the beginning of the following table (for a field F satisfying (H)) and $f = \langle a_1, \dots, a_n \rangle$:

$\dim(f)$	f isotropic	f anisotropic	f represents $a \in F^\times$	f does not represent a
$n=1$	$\emptyset$	always	$\overline{a} = \overline{a_1}$	$\overline{a} \neq \overline{a_1}$
$n=2$	$\overline{-d(f)} = \overline{1}$	$\overline{-d(f)} \neq \overline{1}$	$aa_1 \in H_{-a_1a_2}$ $(\iff a \in a_1 H_{-d(f)})$	$a \notin a_1 H_{-d(f)}$
$n=3$	$-a_1a_3 \in H_{-a_1a_2}$	$-a_1a_3 \notin H_{-a_1a_2}$	$-a_1a_3 \in H_{-a_1a_2}$ $(f\ (IS))$ or $\overline{a} \neq \overline{-d(f)}$	$-a_1a_3 \notin H_{-a_1a_2}$ $(f\ (AN))$ and $\overline{a} = \overline{-d(f)}$
$n=4$	$\overline{d(f)} \neq \overline{1}$ or $\underbrace{-a_1a_3 \in H_{-a_1a_2}}_{\langle a_1, a_2, a_3 \rangle\ (IS)}$	$\overline{d(f)} = \overline{1}$ and $-a_1a_3 \notin H_{-a_1a_2}$		

What about the two missing entries (and the case of $\dim(f)>4$)?

Prop 1. If F satisfies (H) and $|F^\times/F^{\times 2}|>2$, then every (regular) f of $\dim(f)>4$ over F is isotropic, and every (regular) f of $\dim(f)=4$ represents all $a\in F^\times$.

Pf. Enough to show: any $f=\langle a_1,a_2,a_3,a_4,a_5\rangle$ is isotropic.
Let $g=\langle a_1,a_2,a_3\rangle$, $h=\langle -a_4,-a_5\rangle$; then $f=g\perp(-h)$.
If f is anisotropic, then so is g, and

$$\phi=\underbrace{\{b\in F^\times \text{ represented by } g\}}_{F^\times\setminus(-a_1a_2a_3)F^{\times 2}}\cap\underbrace{\{b\in F^\times \text{ represented by } h\}}_{a_4\,H_{-a_4a_5}}$$

which is impossible. ($a_4 H_{-a_4a_5}$: disjoint union of $\frac{1}{2}|F^\times/F^{\times 2}|>1$ cosets of $F^{\times 2}$)

Prop. 2 If F satisfies (H) and $|F^\times/F^{\times 2}|=2$, then F behaves like $\mathbb{R}$:

(1) $F^\times=F^{\times 2}\amalg(-F^{\times 2})$; (2) Every f is equivalent to $n_+\langle 1\rangle\perp n_-\langle -1\rangle$

(3) $\forall x,y\in F\ \exists z\in F\ x^2+y^2=z^2$ ($\Leftrightarrow -1\neq$ sum of squares in F);

(4) There is a bijection

$$\{\text{(regular) } f \text{ over } F\}/\sim \ \longleftrightarrow\ \mathbb{N}_+\times\mathbb{N}_+$$
$$\big[n_+\langle 1\rangle\perp n_-\langle -1\rangle\big]\ \longleftrightarrow\ (n_+,n_-)$$

(5) $\{\text{anisotropic (regular) } f \text{ over } F\}/\sim\ \longleftrightarrow\ \mathbb{Z}$

$$\big[|n|\langle \operatorname{sgn}(n)\rangle\big]\ \longleftrightarrow\ n$$

Pf. $\exists u\in F^\times\setminus F^{\times 2}$ $F^\times=F^{\times 2}\amalg uF^{\times 2}$. As $F^{\times 2}\subset H_u\subset F^\times$ and
$(F^\times:H_u)=2=(F^\times:F^{\times 2})\Rightarrow H_u=F^{\times 2}\Rightarrow u\notin \pm H_u\Rightarrow\langle 1,-u,-u\rangle$ anisotropic
$\Rightarrow\langle 1,1\rangle$ anisotropic $\Rightarrow -1\notin F^{\times 2}\Rightarrow F^\times\overset{(3)}{=}F^{\times 2}\amalg(-F^{\times 2})$ ($\Leftrightarrow$ (1) $\not\Rightarrow$ (2)).
(3) follows from $H_{-1}=F^{\times 2}$, the rest is as in the case $F=\mathbb{R}$.

Completing the table for F satisfying (H) and $|F^\times/F^{\times 2}|>2$:

$\dim(f)$	f isotropic	f anisotropic	f represents $a\in F^\times$	f does not represent $a\in F^\times$
$n=4$			always	$\emptyset$
$n>4$	always	$\emptyset$	always	$\emptyset$

Prop 3. For each $d \in F^\times$, $\{ f \mid \dim(f)=3,\ \overline{d(f)} = \overline{d} \}/\sim$ has two elements, one isotropic, one anisotropic.

Pf. If f is isotropic $\Rightarrow$ $f \sim \langle 1, -1, -d \rangle$. If not, fix $a \in F^\times$ such that $\overline{a} \neq \overline{-d}$ (it exists); then $f \sim \langle a \rangle \perp f_1$ (since f represents a), where $\dim(f_1)=2$, $\overline{d(f_1)} = \overline{ad} \neq \overline{-1}$ ($\Rightarrow f_1$ anisotropic, as it should be) and f_1 does not represent $-a$. There is precisely one class of such f_1, namely that of $\langle b, abd \rangle$, where $b \in F^\times \smallsetminus (-aH_{-ad})$. Conversely, for any $a, b \in F^\times$ such that $\overline{a} \neq \overline{-d}$ and $f := \langle a, b, abd \rangle$ is anisotropic (since $-b \cdot abd \notin H_{-ab}$) and $\overline{d(f)} = \overline{d}$.

Prop 4. For $a, b \in F^\times$, let $N_{a,b} := \langle 1, -a, -b, ab \rangle$ be the norm form of the quaternion algebra $H_{a,b} = \{ \xi = x + yi + zj + tk \mid x, y, z, t \in F \}$, $(i^2 = a,\ j^2 = b,\ ij = -ji = k,\ k^2 = ab)$, $\overline{\xi} = x - yi - zj - tk$, $N(\xi) = \xi\overline{\xi} = x^2 - ay^2 - bz^2 + abt^2$.

(1) $N_{a,b}$ is isotropic $\iff$ $\langle 1, -a, -b \rangle$ is isotropic $\iff$ $a \in H_b \iff b \in H_a$.

(2) $N_{a,b} \sim N_{c,d}$ $\overset{\text{Witt}}{\iff}$ $\underbrace{\langle -a, -b, ab \rangle}_{\overline{d} = \overline{1}} \sim \underbrace{\langle -c, -d, cd \rangle}_{\overline{d} = \overline{1}}$ $\overset{\text{Prop. 3}}{\iff}$ $\langle -a, -b, ab \rangle$ and $\langle -c, -d, cd \rangle$ are simultaneously isotropic or anisotropic

$$\iff \left\{ \begin{array}{l} (a \in H_b \text{ and } c \in H_d) \\ \text{or} \\ (a \notin H_b \text{ and } c \notin H_d) \end{array} \right\}$$

Pf (1) $x^2 - bz^2 = a(y^2 - bt^2)$ for $(x, y, z, t) \in F^4 \smallsetminus \{(0,0,0,0)\}$

$$\iff \left\{ \begin{array}{ll} \text{either} & x^2 - bz^2 = y^2 - bt^2 = 0 \Rightarrow b \in F^{\times 2} \Rightarrow N_{a,b} \sim 2\langle 1, -1 \rangle \\ \text{or} & a = (x^2 - bz^2)/(y^2 - bt^2) \in H_b \end{array} \right\}.$$

Cor. If $|F^\times / F^{\times 2}| > 2$, then

$\{ f \mid \dim(f)=4,\ \overline{d(f)} = \overline{1} \}/\sim = \{ N_{a,b} \}/\sim$ has two elements: the (isotropic) class of $N_{a,b} \sim 2\langle 1, -1 \rangle$ for any $a, b \in F^\times$ with $a \in H_b$ and the (anisotropic) class of $N_{a,b}$ for any $a, b \in F^\times$ with $a \notin H_b$.

Pf: $|F^\times / F^{\times 2}| > 2 \overset{\text{Prop. 1}}{\Longrightarrow} f$ represents $1 \Longrightarrow f \sim \langle 1, -a, -b, \overline{ab\,d(f)} \rangle \sim N_{a,b}$ for some $a, b \in F^\times$. Appl Prop. 4.

Prop. 5. If $\overline{d} \neq \overline{1}$, then

$\{ f \mid \dim(f)=4,\ \overline{d(f)} = \overline{d} \}/\sim$ has two elements, both isotropic; represented by $\langle 1, -1 \rangle \perp f_1$, where f_1 represents the two (anisotropic) classes of $\dim(f_1)=2$, $\overline{d(f_1)} = \overline{-d}$ $(\neq \overline{-1})$.

Pf: $\overline{d(f)} \neq 1 \Rightarrow f$ isotropic $\Rightarrow f \sim \langle 1, -1 \rangle \perp f_1$.

Classification thm. Assume that $|F^\times/F^{\times 2}| > 2$ and $\forall\, b \in F^\times \setminus F^{\times 2}$ $(F^\times : H_b) < \infty$. Then, for each $n \geq 1$ and $d \in F^\times$,

(1) $\{ f \mid \dim(f) = n,\ \overline{d(f)} = \overline{d} \} / \sim$ has two elements, except for $\left(\begin{matrix} n=2 \\ \overline{d} = \overline{-1} \end{matrix}\right)$, when there is only one (isotropic) class.

(2) $\{ f \mid f \text{ anisotropic},\ \dim(f) = n,\ \overline{d(f)} = \overline{d} \} / \sim$ contains

$$\begin{cases} 2 \text{ elements} & \text{if} \quad n = 2,\ \overline{d} \neq \overline{-1} \\ 1 \text{ element} & \text{if} \quad n = 3 \quad \text{or} \quad \text{if } (n = 4 \text{ and } \overline{d} = \overline{1}) \\ 0 \text{ elements} & \text{otherwise.} \end{cases}$$

They are represented, respectively, by

$\langle a_1, a_2 \rangle$ $\qquad \overline{a_1 a_2} = \overline{d} \neq \overline{-1}$

$\langle a_1, a_2, a_3 \rangle$ $\qquad -a_1 a_3 \notin H_{-a_1 a_2}$, $\qquad \overline{a_1 a_2 a_3} = \overline{d}$

$\langle a_1, a_2, a_3, a_4 \rangle$ $\qquad -a_1 a_3 \notin H_{-a_1 a_2}$, $\qquad \overline{a_1 a_2 a_3 a_4} = \overline{1}$

---

(3) the total number of anisotropic classes (if $2 < |F^\times/F^{\times 2}| < \infty$):

$\dim(f) =$	0	1	2	3	4
$\lvert \{ \text{anisotropic } f \} / \sim \rvert$	1	$\lvert F^\times/F^{\times 2} \rvert$	$2(\lvert F^\times/F^{\times 2} \rvert - 1)$	$\lvert F^\times/F^{\times 2} \rvert$	1

$$4\,|F^\times/F^{\times 2}|$$

Pf: This has been proved if $n \leq 4$. If $n > 4$, then f [is isotropic, hence represents] each $b \in F^\times \Rightarrow f \sim \langle 1 \rangle \perp g$, $d(f) = d(g)$, $\dim(g) = n - 1$.
As $[\langle 1 \rangle \perp g \sim \langle 1 \rangle \perp g' \overset{\text{Witt}}{\iff} g \sim g']$, (1) follows by induction.

The Hilbert symbol

Assume: F = field of $\mathrm{char}(F) \neq 2$ satisfying

(H) $F^\times / F^{\times 2} \neq \{1\}$ and $\forall b \in F^\times \setminus F^{\times 2}$ $\quad (F^\times : H_b) = 2$

Def. The **Hilbert symbol** over F is the map

$$\begin{array}{ccc} F^\times \times F^\times & \longrightarrow & \{\pm 1\} \\ \downarrow \quad \downarrow & & \downarrow \\ a, b & \longmapsto & (a,b)_F = \begin{cases} 1, & a \in H_b \\ -1, & a \notin H_b \end{cases} \end{array}$$

(*note*: similarity to the legendre symbol $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$, $(p \neq 2)$, $a \longmapsto \begin{cases} 1, & a \in \mathbb{F}_p^{\times 2} \\ -1, & a \notin \mathbb{F}_p^{\times 2} \end{cases}$)

Properties of the Hilbert symbol: (0) $(a,b)_F = (b,a)_F$

(1) $(aa', b)_F = (a,b)_F (a',b)_F$

(2) $(a, bb')_F = (a,b)_F (a,b')_F$ } bimultiplicativity

(3) $(a, 1-a)_F = 1 \quad (a \in F^\times \setminus \{1\})$ Steinberg relation

(4) $(a,b)_F$ depends only on $\bar{a}, \bar{b} \in F^\times / F^{\times 2}$

(5) If $\bar{b} \neq \bar{1}$, then $\exists\ a \in F^\times$ $(a,b)_F \neq 1$

(6) $(a, -a)_F = 1$.

Pf: (0), (3), (4), (5), (6) are automatic; (2) follows from (0) and (1). Finally, (1) follows from

Lemma. If G is a group and H a subgroup of index $(G:H) = 2$, then the map $G = H \amalg g_0 H \xrightarrow{\alpha} \{\pm 1\}$, $H \longmapsto 1$, $G \setminus H = g_0 H \longmapsto -1$ ($g_0 H = G \setminus H$, for any $g_0 \in G \setminus H$) is a group homomorphism with kernel H, inducing an isomorphism $G/H \xrightarrow{\sim} \{\pm 1\}$.

Ex: (a) $G = \mathbb{F}_p^\times$, $H = \mathbb{F}_p^{\times 2}$ $(p \neq 2)$, α = the legendre symbol

(b) $G = F^\times$, $H = H_b$ $(b \in F^\times \setminus F^{\times 2})$, $\alpha(a) = (a,b)_F$.

Ex: $F = \mathbb{R}$; for $b \in \mathbb{R}^\times$, $H_b = \left\{ \begin{array}{ll} \mathbb{R}^\times, & b > 0 \\ \mathbb{R}^\times_{>0}, & b < 0 \end{array} \right\}$, hence $\mathbb{R}^\times / \mathbb{R}^{\times 2} = \mathbb{R}^\times_{<0}$

$$(a,b)_{\mathbb{R}} = \left\{ \begin{array}{ll} 1, & a > 0 \text{ or } b > 0 \\ -1, & a, b < 0 \end{array} \right\} = (-1)^{\frac{\mathrm{sgn}(a)-1}{2} \cdot \frac{\mathrm{sgn}(b)-1}{2}}.$$

Prop. $\forall v \in Pl\{\infty\}$, $\mathbb{Q}_v$ satisfies (H) $(\mathbb{Q}_\infty = \mathbb{R})$.
Therefore the Hilbert symbol $(\ ,\ )_v = (\ ,\ )_{\mathbb{Q}_v} : \mathbb{Q}_v^\times \times \mathbb{Q}_v^\times \to \{\pm 1\}$ is defined.

Pf. We have checked this for $v = \infty$. For $v = p$, we use the following facts:

(1) $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} = p^{\mathbb{Z}}/p^{2\mathbb{Z}} \times \mathbb{Z}_p^\times / \mathbb{Z}_p^{\times 2}$, $\mathbb{Z}_p^\times / \mathbb{Z}_p^{\times 2} \xrightarrow{\sim} \begin{cases} \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2}, & p \neq 2 \\ (\mathbb{Z}/8\mathbb{Z})^\times, & p = 2 \end{cases}$

$$\Rightarrow \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} = \begin{cases} \{\overline{1}, \overline{u}, \overline{p}, \overline{pu}\}, \ u \in \mathbb{Z}_p^\times, \left(\frac{u \pmod p}{p}\right) = -1; & p \neq 2 \\ \{\overline{\pm 1}, \overline{\pm 5}, \overline{\pm 2}, \overline{\pm 10}\}; & p = 2. \end{cases}$$

[if $p \equiv 3\ [4]$, one can take $u = -1$]

---

(2) $\forall b \in \mathbb{Q}_p^\times$ $H_b \subset \mathbb{Q}_p^\times$ is a subgroup containing $\mathbb{Q}_p^{\times 2}$; it depends only on $\overline{b} \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ and contains $\overline{1}, \overline{-b}, \underbrace{\overline{1-b}, \overline{-b(1-b)}}_{\text{if } b \neq 1}$.

---

(3) Define, for any commutative ring A and $b \in A^\times$,
$H_b(A) := \{x^2 - by^2 \mid x, y \in A\} \cap A^\times$. This is a subgroup of $A^\times$ containing $A^{\times 2}$ and, for any ring homomorphism

$$\left\{ \alpha : A \to A' \text{ such that } \alpha(A^\times) \subset \alpha(A)^\times \right\}, \quad \alpha(H_b(A)) = H_{\alpha(b)}(\alpha(A)) \subset H_{\alpha(b)}(A').$$

$$\Rightarrow \forall p \neq 2 \quad \forall b \in \mathbb{Z}_p^\times$$

$\alpha : \mathbb{Z}_p \to \mathbb{F}_p$, $a \mapsto a \pmod p$

$$\begin{array}{ccc} \mathbb{Z}_p^\times & & H_b(\mathbb{Z}_p) = H_{\alpha(b)}(\mathbb{F}_p) = \mathbb{F}_p^\times \\ \cup & & \\ \mathbb{Z}_p^{\times 2} & & \end{array}$$

$$\Rightarrow H_b(\mathbb{Z}_p)/\mathbb{Z}_p^{\times 2} \subset \mathbb{Z}_p^\times / \mathbb{Z}_p^{\times 2}$$

surjective $\Downarrow \alpha$

$$\mathbb{F}_p^\times / \mathbb{F}_p^{\times 2}$$

$$\Rightarrow \underline{H_b(\mathbb{Z}_p) = \mathbb{Z}_p^\times} \Rightarrow \underline{H_u \supset \mathbb{Z}_p^\times}$$

---

(4) If $a, b \in \mathbb{Z}_p^\times$ $(p \neq 2)$, $x_1, x_2, x_3 \in \mathbb{Z}_p$, $\left(\frac{a \pmod p}{p}\right) = -1$ and $x_1^2 - ax_2^2 - pbx_3^2 \equiv 0\ [p^2]$, then $x_1, x_2, x_3 \in p\mathbb{Z}_p$.

Cor: $\langle 1, -a, -pb \rangle$ is anisotropic over $\mathbb{Q}_p \Rightarrow a \notin H_{pb}$, $pb \notin H_a$.

Pf: $x_1^2 \equiv a x_2^2\ [p] \Rightarrow x_2 \in p\mathbb{Z}_p \Rightarrow x_1 \in p\mathbb{Z}_p \Rightarrow x_3 \in p\mathbb{Z}_p$.

Therefore: $\overline{H_u} \subset \{\overline{1}, \overline{u}, \overline{p}, \overline{pu}\}$ contains $\underbrace{\overline{1}, \overline{u}}_{\text{by (3)}}$, but not $\overline{p}, \overline{pu}$.

$\overline{1}, \overline{-p} \in \overline{H_p} \not\ni \overline{u} \Rightarrow \underline{\overline{H_p} = \{\overline{1}, \overline{-p}\}}$ ($\overline{1}, \overline{-p}$ distinct)

$\Downarrow$

$\underline{\overline{H_u} = \{\overline{1}, \overline{u}\}}$

Finally, $\underbrace{\overline{1}, \overline{-pu}}_{\text{distinct}} \in \overline{H_{pu}} \not\ni \overline{u} \Rightarrow \underline{\overline{H_{pu}} = \{\overline{1}, \overline{-pu}\}}$.

Prop. holds for $p \neq 2$.

(5) If $a_i \in 1+4\mathbb{Z}_2$, $x_i \in \mathbb{Z}_2$ $(1\le i\le 3)$ and

$p=2$ $\quad a_1x_1^2+a_2x_2^2+a_3x_3^2 \equiv 0\ [2^2]$, then $x_i \in 2\mathbb{Z}_2$ $(1\le i\le 3)$

$(\Rightarrow \langle a_1,a_2,a_3\rangle$ is isotropic over $\mathbb{Q}_2)$.

Pf: $a_ix_i^2 \equiv \begin{cases} 0 \ [2^2] & \text{if } 2\mid x_i \\ 1 \ [2^2] & \text{if } 2\nmid x_i \end{cases}$.

therefore $\langle 1,1,1\rangle$, $\langle 1,1,5\rangle$, $\langle 1,5,5\rangle$ are isotropic over $\mathbb{Q}_2$

$\Rightarrow$ $\overline{-1},\overline{-5} \notin H_{-1}\cup H_{-5}$ $\quad (*)$

By (2), $\overline{1}, \overline{5}, \overline{1+5}=\overline{-10} \in \overline{H_{-5}}$ $\overset{(*)}{\Rightarrow}$ $\overline{-1},\overline{-5},\overline{10},\overline{2} \notin \overline{H_{-5}}$

$(\Rightarrow \overline{-10}/\overline{5}=\overline{-2}\ \Psi)$ $\Rightarrow$ $\overline{H_{-5}}=\{\overline{1},\overline{-2},\overline{5},\overline{-10}\}$

$\mathbb{Z}_2^*/\mathbb{Z}_2^{*2} = \{\overline{1},\overline{-5},\overline{1-5}=\overline{-1}\} \in \overline{H_5}$ $(\Rightarrow \overline{-5}\cdot\overline{-1}=\overline{5}\ \Psi)$

$\overline{H_5}=\{\pm\overline{1},\pm\overline{5}\}=\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}$

$\overline{2} \notin \overline{H_5}$

$\overline{1},\overline{-2},\overline{1-2}=\overline{-1}\ (\Rightarrow \overline{2}) \in \overline{H_2} \not\ni \overline{-5}$ $\Rightarrow$ $\overline{H_2}=\{\pm\overline{1},\pm\overline{2}\} \not\ni \overline{5}$

$\overline{H_5} \not\ni \overline{-2} \in \overline{H_{-5}},\overline{H_2}$ $\Rightarrow$ $\overline{1},\overline{2},\overline{-5},\overline{-10} \in \overline{H_{-2}} \not\ni \overline{5}$ $\Rightarrow$ $\overline{H_{-2}}=\{\overline{1},\overline{2},\overline{-5},\overline{-10}\}$

$\overline{H_{-5}} \not\ni \overline{-1} \in \overline{H_2},\overline{H_5}$ $\Rightarrow$ $\overline{H_{-1}}=\{\overline{1},\overline{2},\overline{5},\overline{10}\}$

$\overline{H_{-1}} \not\ni \overline{-10} \in \overline{H_{-2}},\overline{H_{-5}}$ $\Rightarrow$ $\overline{H_{10}}=\{\overline{1},\overline{-2},\overline{-5},\overline{10}\}$

$\overline{H_5} \not\ni \overline{10} \in \overline{H_{-1}},\overline{H_{-10}}$ $\Rightarrow$ $\overline{H_{10}}=\{\overline{1},\overline{-1},\overline{10},\overline{-10}\}$

Prop. holds for $p=2$

Formulas: $p\neq 2$ $\quad \overline{H_1}=\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}=\{\overline{1},\overline{u},\overline{p},\overline{pu}\}$, $\overline{H_u}=\{\overline{1},\overline{u}\}=\mathbb{Z}_p^*/\mathbb{Z}_p^{*2}$

$\overline{H_p}=\{\overline{1},\overline{-p}\}$, $\overline{H_{pu}}=\{\overline{1},\overline{-pu}\}$

$\overline{-1}=\begin{cases}\overline{1}, & p\equiv 1\ [4]\\ \overline{u}, & p\equiv 3\ [4]\end{cases}$

So: (1) $a,b\in\mathbb{Z}_p^* \Rightarrow a\in H_b \Rightarrow (a,b)_p=1$.

(2) $\overline{1}\in\overline{H_p}\not\ni\overline{u} \Rightarrow \forall a\in\mathbb{Z}_p^*$ $(a,p)_p=\left(\frac{a}{p}\right)=\begin{cases}1, & \overline{a}=\overline{1}\\ -1, & \overline{a}=\overline{u}\end{cases}$

(3) $(p,-p)_p=-1 \Rightarrow (p,p)_p=\underbrace{(p,-p)_p}_{1}\underbrace{(p,-1)_p}_{\left(\frac{-1}{p}\right)}=\left(\frac{-1}{p}\right)$.

$\Rightarrow$ $\forall a,b\in\mathbb{Z}_p^*$ $(\underbrace{p^ma}_{x},\underbrace{p^nb}_{y})_p=\underbrace{(p,p)_p^{mn}}_{\left(\frac{-1}{p}\right)^{mn}}\cdot\underbrace{(p,b)_p^{m}}_{\left(\frac{b}{p}\right)^{m}}\cdot\underbrace{(a,p)_p^{n}}_{\left(\frac{a}{p}\right)^{n}}\underbrace{(a,b)_p}_{1}=\left(\frac{T(x,y)}{p}\right)$, where

$\underbrace{T(x,y)}_{\text{the tame symbol}} := \underbrace{(-1)^{v_p(x)v_p(y)}}_{(-1)^{mn}}\left(\underbrace{\frac{x^{v_p(y)}}{y^{v_p(x)}}}_{a^n/b^m\in\mathbb{Z}_p^*}\right) \pmod p \in \mathbb{F}_p^*$

Formulas for $p=2$: (a) $\overline{H_5} = \mathbb{Z}_2^\times / \mathbb{Z}_2^{\times 2} \Rightarrow \forall a,b \in \mathbb{Z}_2^\times \quad (a,5)_2 = (5,b)_2 = 1$

$\overline{a} = \overline{5}^m \underbrace{\overline{\pm 1}}_{a \bmod 4}$ $(m=0,1) \Rightarrow (a,b)_2$ depends only on $\left.\begin{matrix} a \pmod 4 \\ b \pmod 4 \end{matrix}\right\} \in \underbrace{(\mathbb{Z}/4\mathbb{Z})^\times}_{\pm 1}$

$\overline{-1} \notin \overline{H_{-1}} \Rightarrow (-1,-1)_2 = -1$. Therefore

$\forall a,b \in \mathbb{Z}_2^\times \quad (a,b)_2 = \left\{ \begin{matrix} 1, & a \equiv 1 \,[4] \text{ or } b \equiv 1 \,[4] \\ -1, & a \equiv b \equiv -1 \,[4] \end{matrix} \right\} = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$

(b) $\forall a \in \mathbb{Z}_2^\times \quad (-1,a)_2 = \left\{ \begin{matrix} 1, & a \equiv 1 \,[4] \\ -1, & a \equiv -1 \,[4] \end{matrix} \right\} = (-1)^{\frac{a-1}{2}} =: \chi_{-4}(a)$

(c) $\overline{H_2} = \{\overline{\pm 1}, \overline{\pm 2}\} \Rightarrow \forall a \in \mathbb{Z}_2^\times \quad (2,a)_2 = \left\{ \begin{matrix} 1, & a \equiv \pm 1 \,[8] \\ -1, & a \equiv \pm 5 \,[8] \end{matrix} \right\} =: \chi_8(a)$

$(-2,a)_2 = (-1,a)_2 (2,a)_2 = \left\{ \begin{matrix} 1, & a \equiv 1,3 \,[8] \\ -1, & a \equiv -1,-3 \,[8] \end{matrix} \right\} =: \chi_{-8}(a)$

(d) $(2,2)_2 = \underbrace{(2,-1)_2}_{1} \underbrace{(2,-2)_2}_{1} = 1$

(e) $\forall a,b \in \mathbb{Z}_2^\times \quad (2^m a, 2^n b)_2 = \underbrace{(2,2)_2^{mn}}_{1} (a,2)_2^n (2,b)_2^m (a,b)_2$

Hilbert's formulation of QRL

Thm (Hilbert) $\boxed{\forall\, a,b \in \mathbb{Q}^\times \qquad \prod_{v \in \text{Puts}} (a,b)_v = 1}$

Pf: Factorise $a = \pm \prod p^{v_p(a)}$, $b = \pm \prod p^{v_p(b)}$

Bimultiplicativity of $(a,b)_v \Rightarrow$ enough to consider $a = \begin{cases} -1 \\ \text{prime} \end{cases}$, $b = \begin{cases} -1 \\ \text{prime} \end{cases}$

① $\underline{(-1,-1)}$: $\underbrace{(-1,-1)_\infty}_{-1}\ \underbrace{(-1,-1)_2}_{-1} = 1$

② $\underline{(-1,2)}$: $\underbrace{(-1,2)_\infty}_{1}\ \underbrace{(-1,2)_2}_{1} = 1$ (Steinberg)

③ $(-1,p)$: $(p \neq 2)$ $\underbrace{(-1,p)_\infty}_{1}\ \underbrace{(-1,p)_p}_{\left(\frac{-1}{p}\right)}\ \underbrace{(-1,p)_2}_{\chi_{-4}(p)} = 1 \quad \left(\Leftrightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}\right)$

④ $\underline{(2,2)} = (2,-2)\cdot(2,-1)$: Steinberg

⑤ $\underline{(2,p)}$: $(p \neq 2)$ $\underbrace{(2,p)_\infty}_{1}\ \underbrace{(2,p)_p}_{\left(\frac{2}{p}\right)}\ \underbrace{(2,p)_2}_{\chi_8(p)} = 1 \quad \left(\Leftrightarrow \left(\frac{2}{p}\right) = \chi_8(p)\right)$

⑥ $\underline{(p,2)}$: $(p \neq 2 \neq 2)$ $\underbrace{(p,2)_2}_{\left(\frac{p}{2}\right)}\ \underbrace{(p,2)_p}_{\left(\frac{2}{p}\right)}\ \underbrace{(p,2)_2}_{(-1)^{\frac{p-1}{2}\cdot\frac{2-1}{2}}} = 1 \quad \left(\Leftrightarrow \left(\frac{p}{2}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{2-1}{2}}\right)$

Cor: $\forall\ a,b,c \in \mathbb{Q}^\times \quad \forall\ v_0 \in \text{Puts}$,

$\left[ax^2+by^2+cz^2 = 0 \text{ has a solution in } \mathbb{Q}_v\ \forall\, v \neq v_0 \Rightarrow \text{also for } v = v_0 \right]$

$\Updownarrow$ (nontrivial)

$(-b/a, -c/a)_v = 1$

Thm (Aubry–Cassels–Davenport)

let $f(X) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$ $\quad a_{ij} = a_{ji} \in \frac{1}{2}\mathbb{Z}$, $a_{ii} \in \mathbb{Z}$. Assume that

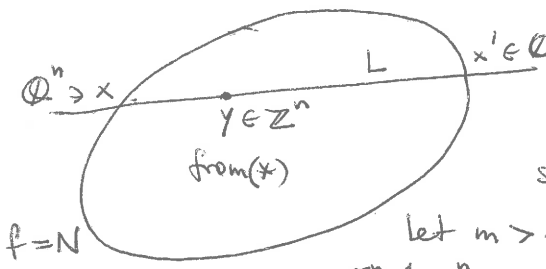
(*) $\forall x \in \mathbb{R}^n \setminus \mathbb{Z}^n \quad \exists y \in \mathbb{Z}^n \quad 0 < |f(x-y)| < 1$.

Then $f(\mathbb{Q}^n) \cap \mathbb{Z} = f(\mathbb{Z}^n) \cap \mathbb{Z}$.

Ex: $f = X_1^2 + X_2^2$, $X_1^2 + X_1X_2 \pm X_2^2$, $X_1^2 \pm 2X_2^2$, $X_1^2 + X_2^2 + X_3^2$, $X_1^2 - 3X_2^2$, $X_1^2 + X_2^2 - 3X_3^2$

Pf: Assume that $x \in \mathbb{Q}^n \setminus \mathbb{Z}^n$, $f(x) = N \in \mathbb{Z}$. We construct $x' \in \mathbb{Q}^n$ with $f(x') = f(x) = N$ and a smaller denominator than x as follows:

$\{x, x'\}$ = (the line L through x and y from (*)) $\cap$ (the quadric $f = N$)



Indeed f and the corresponding bilinear form $B(X,Y) = B(Y,X) = \sum_{i,j=1}^{n} a_{ij} X_i Y_j$ satisfy: $f(\mathbb{Z}^n) \subset \mathbb{Z}$, $2B(\mathbb{Z}^n, \mathbb{Z}^n) \subset \mathbb{Z}$.

let $m > 1$ be the denominator of x ($mx \in \mathbb{Z}^n$, $m \in \mathbb{Z}_{>1}$, m minimal)

Set $z := x - y \in \frac{1}{m}\mathbb{Z}^n$ and consider the polynomial

$P(t) := f(y + t(x-y)) = f(y + tz) = at^2 + bt + c$ (t = an affine coordinate on the line L)

We have:
- $x = y + 1 \cdot z$, $x' = y + \lambda \cdot z$ for some $\lambda \in \mathbb{Q} \setminus \{1\}$
- $a = f(z) \in \mathbb{Q}$, $0 < |a| < 1$ (by (*))
- $c = P(0) = f(y) \in \mathbb{Z}$ (since $y \in \mathbb{Z}^n$)
- $P(1) = a+b+c = f(x) = f(x') = P(\lambda) = a\lambda^2 + b\lambda + c \in \mathbb{Z}$
- $mb = 2B(y, mz) \in \mathbb{Z}$

Therefore $a+b = a\lambda^2 + b\lambda \in \mathbb{Z}$, $\lambda \neq 1$ $\Rightarrow$ $m' := ma \in \mathbb{Z}$, $0 < |m'| < |m| = m$

$a(\lambda+1) + b = 0 \Rightarrow a\lambda \in \mathbb{Z}$

$m'(x' - y) = ma\lambda z \in \mathbb{Z}^n$

$\Rightarrow$ $\underline{m'x' \in \mathbb{Z}^n}$

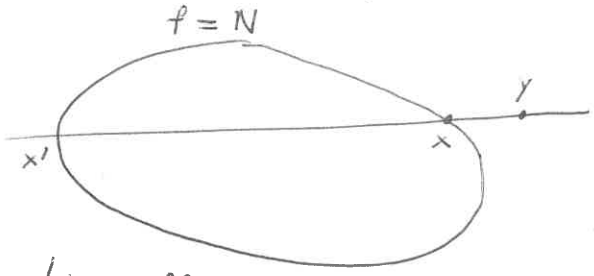
this proves that the denominator of x' is strictly smaller than that of x. After finitely many steps, we obtain a point in $(f = N) \cap \mathbb{Q}^n$ with denominator equal to 1, i.e., a point in $(f = N) \cap \mathbb{Z}^n$.

Cor. (Gauss) $\{x_1^2 + x_2^2 + x_3^2 \mid x_i \in \mathbb{Z}\} = \mathbb{Z} \cap \{x_1^2 + x_2^2 + x_3^2 \mid x_i \in \mathbb{Q}\}$

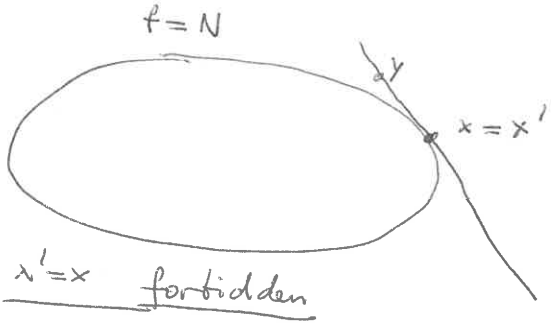
$= \{n \in \mathbb{Z} \mid n \geq 0,\ n \neq 4^k(8m-1)\}$

Aubry – (Cassels – Davenport) (bis)

There was a gap in the proof of the theorem.



$x' \neq x$ allowed



$x' = x$ forbidden

We need to show that $x' \neq x$.

Recall: $x \in \mathbb{Q}^n \setminus \mathbb{Z}^n$, $y \in \mathbb{Z}^n$, $f(x) = N \in \mathbb{Z}$, $0 < |f(x-y)| < 1$, $f(\mathbb{Z}^n) \subset \mathbb{Z}$

$f(x+y) - f(x) - f(y) = 2B(x,y)$, $\{x, x'\} = \{f = N\} \cap (\text{the line } \overleftrightarrow{xy})$

We have: $x' = x \iff \overleftrightarrow{xy}$ is tangent to $\{f = N\}$ at $x \iff B(x, y-x) = 0$

$\iff B(x,y) = f(x)$.

But $f(x-y) = f(x) + f(y) - 2B(x,y)$, so $\left[x' = x \Rightarrow f(x-y) = -f(x) + f(y) \in \mathbb{Z} \right]$

($f(x) \in \mathbb{Z}$, $f(y) \in \mathbb{Z}$)

contradiction with $0 < f(x-y) < 1$

Sums of 4 squares

Notation : $r_4(n) := \left| \{ x = (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = n \} \right|$ $(n \in \mathbb{N}$

Exercise : $r_4(2n) = r_4(n) \cdot \begin{cases} 3, & 2 \nmid n \\ 1, & 2 \mid n \end{cases}$ **Hint :** $\left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$

$= \frac{x_1^2 + x_2^2 + x_3^2 + x_4^2}{2}$

Numerical data for $2 \nmid n$:

	n	x	$r_4(n)/8$		factorised form of n	$r_4(n)/8$
	1	$(0,0,0,1)$	1			
*	3	$(0,1,1,1)$	4		p	$p+1$
	5	$(0,0,1,2)$	6		p	$p+1$
	7	$(1,1,1,2)$	8		p	$p+1$
	9	$(0,1,2,2)$	12	13	p^2	p^2+p+1
		$(0,0,0,3)$	1			
	11	$(0,1,1,3)$	12		p	$p+1$
	13	$(0,0,2,3)$	6	14	p	$p+1$
		$(1,2,2,2)$	8			
	15	$(1,1,2,3)$	24		pq	$pq+p+q+1 = (p+1)(q+1)$
	17	$(0,0,1,4)$	6	18	p	$p+1$
		$(0,2,2,3)$	12			
	19	$(0,1,3,3)$	12	20	p	$p+1$
		$(1,1,1,4)$	8			
	21	$(0,1,2,4)$	24	32	pq	$(p+1)(q+1)$
		$(2,2,2,3)$	8			
	23	$(1,2,3,3)$	24		p	$p+1$
	25	$(0,0,0,5)$	1	31	p^2	p^2+p+1
		$(0,0,3,4)$	6			
		$(1,2,2,4)$	24			
	27	$(0,1,1,5)$	12	40	p^3	p^3+p^2+p+1
		$(1,1,3,4)$	24			
		$(0,3,3,3)$	4			
	45	$(0,0,3,6)$	6	78	$p^2 q$	$(p^2+p+1)(q+1)$
		$(1,2,2,6)$	24			
		$(0,2,4,5)$	24			
		$(2,3,4,4)$	24			

It seems : $2 \nmid n \Rightarrow r_4(n) \overset{?}{=} 8 \sigma_1(n) = 8 \sum_{d \mid n} d$

Lemma $\Rightarrow$ $\boxed{\forall n \geq 1 \quad r_4(n) \overset{?}{=} 8 \sum_{4 \nmid d \mid n} d}$