Recall: $R \subset F$, $m = (\pi) \subset R$
cdvr cdvf $R/m = k$
char $\neq 2$

$$(i, j) : W(k) \oplus W(k) \xrightarrow{\sim} W(F).$$

Inverse

$$(\partial_1, \partial_2) : W(F) \xrightarrow{\sim} W(k) \oplus W(k)$$

$$u(F) = 2u(k)$$

So if F is a local field, $u(F) = 4$, & also $|W(F)| = 16$.

For F local, have Hilbert symbol:

$$(a, b)_F = \pm 1, = 1 \iff \left(\frac{a, b}{F}\right) \text{ splits,}$$
$$\iff \langle a, b \rangle \text{ reps } 1.$$

The next result is useful in understanding the Hilbert symbol — in particular showing that it is a non-degenerate pairing:

Prop Let $q = \langle a, b, c \rangle$ be an anisotropic q.f. $/F$ of dim 3, & $\delta := \det q$.

Then: i) q does not represent $-\delta$.

ii) q represents the other square classes.

Proof. Re (i): We'll prove the contrapositive: That if (i) fails then q is isotropic.

So suppose q represents $-\delta = -abc$.

Then $\langle a, b, c, abc \rangle$ is isotropic; & so it contains a hyperbolic plane $h = \langle 1, -1 \rangle$;

i.e. $\langle a, b, c, abc \rangle \cong \langle 1, -1, \underbrace{d, e}_{\text{in } F^\times} \rangle$

$\det = 1 \in F^\times / F^{\times 2}$ $=$ $\det = -de$

So $e = -d \in F^\times / F^{\times 2}$

and $\langle d, e \rangle \cong \langle d, -d \rangle \cong h$

$\cong \langle -abc, abc \rangle$

So $\langle a, b, c, abc \rangle \cong \langle 1, -1, -abc, abc \rangle$

With Cancellation $\Rightarrow$ $\underset{q}{\underset{\shortparallel}{\langle a, b, c \rangle}} \cong \underbrace{\langle 1, -1, -abc \rangle}_{\text{isotropic}}$

✓

Re (ii): Say w is in a <u>different</u> square class than $-\delta = -abc$.

WTS: $q = \langle a, b, c \rangle$ represents w.

$$\underset{\text{in } F^\times/F^{\times 2}}{w \neq -\delta} \Rightarrow \underset{\det(\langle a,b,c,-w\rangle)}{\underset{\parallel}{(-\delta)w}} \neq (-\delta)^2 = 1 \in F^\times/F^{\times 2}$$

: not a square.

But $\langle 1, -u, -\pi, u\pi \rangle$ has square det

the only anisotropic form of dim 4 (up to isometry)

$\therefore \langle a, b, c, -w \rangle$ is isotropic.

So $q = \langle a, b, c \rangle$ represents w. ✓

Applying this, we get

<u>Cor</u> The Hilbert symbol is a non-degenerate pairing: no nontrivial class always pairs trivially.

I.e.: $\forall y \in F^\times \setminus F^{\times 2}$,

$\exists z \in F^\times$ st $(y, z)_F = -1$.

i.e. the quaternion alg $\left(\frac{y, z}{F}\right)$ is not split

Proof Since $\langle 1, -u, -\pi, u\pi \rangle$ is anisotropic,
so is the subform $q := \langle -u, -\pi, u\pi \rangle$.
$\det q = 1 \in F^\times / F^{\times^2}$, so the prop. shows
q reps every square class except -1.
Since y is not a square, $y \neq 1 \in F^\times / F^{\times^2}$,
so $-y \neq -1 \in F^\times / F^{\times^2}$, so q reps. $-y$.
$\therefore q \cong \langle -y \rangle \perp q'$. But $\det q = 1$.
$\therefore \det q' = -y \in F^\times / F^{\times^2}$; $\Rightarrow q' \cong \langle -z, yz \rangle$
$\dim q = 3 \Rightarrow \dim q' = 2$ $\Rightarrow$ $(z \in F^\times)$

So $\langle -u, -\pi, u\pi \rangle = q \cong \langle -y \rangle \perp q' \cong \langle -y, -z, yz \rangle$
So $\underbrace{\langle 1, -u, -\pi, u\pi \rangle}_{\text{norm form of } \left(\frac{u,\pi}{F}\right)} \cong \underbrace{\langle 1, -y, -z, yz \rangle}_{\text{norm form of } \left(\frac{y,z}{F}\right)}$

$\therefore \left(\frac{y,z}{F}\right) \cong \left(\frac{u,\pi}{F}\right)$; so $(y,z)_F = (u,\pi)_F = -1$.

Above results assumed $\operatorname{char} k \neq 2$.
But if $F = \mathbb{Q}_2$ or a finite extension,
then $\operatorname{char} F = 0$ but $\operatorname{char} k = 2$.
Can carry over these results to this situation, though proofs are more complicated.

Lam, Chap VI: In above situation

Thm 2.10: $\exists!$ quaternion div. alg. $/F$,

viz. $\left(\frac{\pi, u}{F}\right)$ for a suitable unit u.

Have $R \subset F$, with uniformizer π. (Ex. $\pi = 2$ if $R = \mathbb{Z}_2$, $F = \mathbb{Q}_2$)

As in #thy, $\exists!$ degree 2

unique ext of k of deg 2 unramified extension K/F,

i.e. π is again a uniformizer for K.

$K = F(\sqrt{u})$; use this u. (If $F = \mathbb{Q}_2$, $u = 5$)

Kummer extension

Thm 2.12: $u(F) = 4$.

Cor 2.15: (1) $\exists!$ 4-dim'l anisotropic qf $/F$,

viz $\langle 1, -u, -\pi, u\pi \rangle$

(2) If q is anisotropic $/F$ of dim 3, then it does not represent $-\det F$, but it does represent every other square class

Thm 2.16 The Hilbert symbol $/F$ is non-degenerate.

Some things are different: Before we had

$1, u, \pi, u\pi$ $|F^\times / F^{\times 2}| = 4$, for res. char. $\neq 2$. But

for res char $= 2$, $|F^\times / F^{\times 2}| > 4$:

Ex. In $\mathbb{Q}_2$, there are eight square classes, forming $(\mathbb{Z}/2)^3$; given by $(-1)^i 2^j 5^k$, $i,j,k \in \{0,1\}$. (Lam, Ch VI, Cor 2.24)

More generally, for a finite extension $F/\mathbb{Q}_2$, let $s = v(2) \geq 1$ (2 is not nec. a uniformizer)

Let $q = |k|$; a power of 2. (Lam, Ch VI, Th. 2.22)

Then $|F^\times / F^{\times 2}| = 4q^s \geq 8$. $= 2^{n+2}$ if $[F:\mathbb{Q}_2] = n$

res. degree

$(q = 2^f,\ s = e,\ \text{so } q^s = 2^{ef} = 2^n)$

ram. index

Re Hilbert symbol: (Lam, Ch VI, Cor 2.28)

If $x, y \in U = \mathbb{Z}_2^\times$, then

$(x,y)_2 = (-1)^{\frac{x-1}{2}\frac{y-1}{2}}$, $(2,y)_2 = (-1)^{\frac{y^2-1}{8}}$.

(Compare to quadratic reciprocity)

Also get structure of $W(F)$ for 2-adic fields F

(Lam, Ch VI, Thm 2.29):

Say $\begin{array}{c} F \\ | \\ \mathbb{Q}_2 \end{array}$ degree n extension

Recall $|F^\times/F^{\times^2}| = 2^m$, $\underset{n+2}{\overset{\shortparallel}{m}} \geq 3$. Then as a group,

1) If $-1 \in F^{\times^2}$, then $W(F) \cong (\mathbb{Z}/2)^{m+2}$.

2) Say $-1 \notin F^{\times^2}$.

a) If -1 is a sum of two squares, then

$$W(F) \cong (\mathbb{Z}/4)^2 \oplus (\mathbb{Z}/2)^{m-2}$$

b) Otherwise, $W(F) = \mathbb{Z}/8 \oplus (\mathbb{Z}/2)^{m-1}$

In each case, $|W(F)| = 2^{m+2}$
$= 2^{n+4}$

So 2^{n+4} anisotropic q.f.'s in F, up to isometry.

Local-global principles for global fields: esp. Hasse-Minkowski Theorem

F a global field, q a q.f./F.

Thm: q isotropic/F $\iff$ q isotropic/every F_v.

local field

Equivalently:

q anisotropic/F $\iff$ q anisotropic/some F_v.

Ex. $F = \mathbb{Q}$. Completions: $\mathbb{Q}_p$ $\forall$ primes p, and $\mathbb{R}$

wrt $|\cdot|_p$ — wrt $|\cdot|_\infty$ (usu abs val)

Ex. $F = \mathbb{F}_p(t)$ = rat'l fns on projective t-line over $\mathbb{F}_p$.

Completions: F_f, wrt $|\cdot|_f$, & wrt $|\cdot|_\infty$

irreducible

point on t-line $\longleftrightarrow$ monic poly/$\mathbb{F}_p$;

pt at ∞ on $\mathbb{P}^1_{\mathbb{F}_p}$

Eg. For $f = t$, $F_f = \mathbb{F}_p((t))$;

$|t^2 + t^3|_f = \frac{1}{p^2}$ $\leftarrow$ in $(t)^2$ but not (t^3)

For $f = \infty$, $F_f = \mathbb{F}_p((t^{-1}))$;

$|t^2 + t^3|_\infty = p^3$ $\leftarrow$ deg 3; pole of order 3 at ∞

This theorem is special for quadratic forms.

Fails for cubic forms.

Ex. $3x^3+4y^3+5z^3$ is isotropic $/\mathbb{R}$ and $/$all $\mathbb{Q}_p$

but is anisotropic $/\mathbb{Q}$.

(Selmer curve)

Fails for quartic forms.

Ex. $(3x^2-yz)^2+5(y^2-zx)^2-2(z^2-3xy)^2$

is isotropic $/\mathbb{R}$ and all $\mathbb{Q}_p$,

but anisotropic $/\mathbb{Q}$. (See Lang p. 170)

Related to observation:

A q.f. q of dim n $\rightsquigarrow$ a quadric hypersurface $Q\subset\mathbb{P}^{n-1}$ given by $q=0$;

a homogeneous space under the group $O(q)$.

Some consequences of Hasse-Minkowski:

Cor For a q.f. q $/$ global field F,

q is hyperbolic $/F \iff q$ is hyperbolic $/$each F_v.

Pf is by induction, using H-M, Witt decomposition, & Witt Cancellation.

Cor $i_W(q) = \min_v i_W(q_v)$

Witt index of q over F

(# of h's in Witt decomp)

q.f./F

Witt index of q / F_v

q viewed as q.f. / F_v

(These corollaries will be on the next problem set.)

Cor If $a \in F^\times$, then

q represents a over F $\iff$

q represents a over each F_v.

Pf. q reps a over F

$\iff q \perp \langle -a \rangle$ is isotropic /F

$\iff q \perp \langle -a \rangle$ — — — — — — — /all F_v

$\iff q$ reps a over all F_v. ✓

q.f.'s /F

Cor $q \cong q'$ over $F \iff q \cong q'$ over all F_v.

Pf. Either side implies $\dim q = \dim q'$.

If this holds, then:

$q \cong q' \,/F$

$\iff$ q, q' define the same class in $W(F)$

$\iff$ $q \perp \langle -1 \rangle q'$ is trivial in $W(F)$, i.e. is hyperbolic $/F$

$\iff$ $q \perp \langle -1 \rangle q'$ is hyperbolic $/$ all F_v

prev Cor

$\iff$ $q \cong q' \,/$ all F_v. ✓

Cor Given $q, q' \,/F$,

$q \cong q' \,/F \iff$

(i) $\dim q = \dim q'$

(ii) $\det q = \det q' \in F^\times / F^{\times 2}$

(iii) (a) $s(q_v) = s(q'_v)$ for every discrete valuation v on F.

Hasse invariant:
For $q = \langle a_1, \ldots, a_n \rangle$,
$s(q) = \prod_{i<j} \left(\frac{a_i, a_j}{F} \right) \in Br(F)$

(b) $\operatorname{sign}(q_v) = \operatorname{sign}(q'_v)$ for every real abs val on F

signature of a real form.

Pf. $(\Rightarrow)$ is trivial. For $(\Leftarrow)$:

(i), (ii), (iii)(a) $\Rightarrow$ $q \cong q' / F_v$ for v any discrete valuation (previous result)

(i), (iii)(b) $\Rightarrow$ $q \cong q' / F_v \cong \mathbb{R}$ ← real completion by Sylvester's Law of Inertia for real qf's.

At complex completions, any two regular qf's of the same dim are isometric.

So: $q \cong q'$ in every F_v.

So done by previous Cor.

Cor Let F be a finite extension of $\mathbb{F}_p(x)$. Then $u(F) = 4$.

global fn. fld

$p \neq 2$

Pf Say q is a qf/F. If $\dim q > 4$, then q is isotropic / all F_v, since $u(F_v) = 4$. $\therefore$ q is isotropic/F.

Thus $u(F) \leq 4$. WTS $=$.

For this, want an anisotropic qf over F of $\dim = 4$.

First case: $F = \mathbb{F}_p(x)$.

Since $u(\mathbb{F}_p) = 2$, $\exists$ anisotropic qf q_0 of dim 2 over $\mathbb{F}_p$.

Let $q = q_0 \perp \langle x \rangle q_0$, q.f. $/F$.

c.d.v.f. (local fld)

uniformizer

Let $v \leftrightarrow (x)$; $F_v = F_x = \mathbb{F}_p((x))$.

As a q.f. over F_v, $\partial_1(q) = \partial_2(q) = q_0$.

These are anisotropic $/\mathbb{F}_p$, so q is anisotropic $/F_v$.

$\therefore q$ is anisotropic over $F \subset F_v$. ✓

General case: F is a finite extension of $\mathbb{F}_p(x)$; $F = \operatorname{frac} R$ for R a finite extension of $\mathbb{F}_p[x]$.

Ded. dom.

Proceed similarly wrt a max'l ideal $m \subset R$ with uniformizer π, and finite residue field R/m.

What about $u(F)$ for F a # field ?

It depends on whether there is a real completion of F, or if all archimedean completions are complex. assoc to $F \hookrightarrow \mathbb{C}$

Ex. $F = \mathbb{Q}$, one arch. abs. value,
Completion $= \mathbb{R}$.

Ex. $F = \mathbb{Q}(\sqrt{2})$, two arch. abs. values,
corresp to $\sqrt{2} \mapsto 1.414213\ldots$, $\sqrt{2} \mapsto -1.414213\ldots$
Each has completion $= \mathbb{R}$.

Ex. $F = \mathbb{Q}(\sqrt{-2})$. One arch abs value,
Completion $= \mathbb{C}$. Similarly for $\mathbb{Q}(i)$.

Ex. $F = \mathbb{Q}(\sqrt[3]{2})$. Two arch abs values
One with completion $= \mathbb{R}$
(use real $\sqrt[3]{2}$),
One with completion $= \mathbb{C}$

Over $\mathbb{R}$, $\langle 1, \ldots, 1 \rangle$ is anisotropic; pos. def.
So $u(\mathbb{R}) = \infty$.
So $u(F) = \infty$ if $F \hookrightarrow \mathbb{R}$;
So if a # fld F has a real completion

What if F has <u>no</u> real completions?

— F is a "totally imaginary # field"

— e.g. $\mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\zeta_5)$ or "totally complex"

<u>Cor</u> If F is a totally imaginary # field then $u(F) = 4$.

Pf is as for the global function field case, but for archimedean absolute values, use $F_v \cong \mathbb{C}$, & $u(\mathbb{C}) = 1 < 4$.

For other # fields, including $\mathbb{Q}$:

<u>Cor</u> Say $\dim q > 4$. Then:

q is isotropic $/F \iff$

$\forall v$ st $F_v \cong \mathbb{R}$, the image of q under $F \hookrightarrow F_v \cong \mathbb{R}$ is indefinite

Same pf using: $q/\mathbb{R}$ is isotropic $\iff q$ is indefinite.

Case of $\mathbb{Q}$: If $\dim q > 4$ then q is isotropic$/\mathbb{Q} \iff q$ is indefinite $/\mathbb{R}$.

To handle the case of # flds that are not totally imaginary, and some other fields that have $u(F) = \infty$:

There's a variant of u:
the Elman-Lam invariant $u'(F)$:
the sup of the dims of anisotropic q.f.'s /F that correspond to torsion elements of $W(F)$.

For $\mathbb{Q}$, this eliminates pos def qf's & neg. def. qf's. And then get $u'(\mathbb{Q}) = 4$. More generally, $u'(F) = 4$ for all global fields.

In general, $u'(F) = u(F)$ for any field F with no embedding $F \hookrightarrow \mathbb{R}$.
(See Lam, Appendix to §6 of Chap XI.)

Question: Which rational #s are the sum of three squares?

Equiv: What is $D(\langle 1,1,1\rangle)$ over $\mathbb{Q}$?

Since we can multiply by squares & clear denominators, it suffices to determine which integers are in this set.

Use Cor of Hasse-Minkowski:

q reps a in $\mathbb{Q} \iff q$ reps a in $\mathbb{R}$ & all $\mathbb{Q}_p$.

To rep a in $\mathbb{R}$: $\iff a>0$.

To rep a in $\mathbb{Q}_p$, p odd:

Every elt in $\mathbb{Z}/p$ is a sum of two squares, hence also in $\mathbb{Q}_p$, since p is odd.

For $\mathbb{Q}_2$: recall: If F is a non-archimedean local field, & $q=\langle a,b,c\rangle$ is an anisotropic q.f. $/F$ of dim 3, then q represents all the square classes of F other than $-\det q$.

Apply this to $q = \langle 1,1,1\rangle$ over $\mathbb{Q}_2$:

get q reps every square class other than -1.

A unit in $\mathbb{Z}_2^\times$ is a square iff it is $\equiv 1 \pmod 8$,

so a general element of $\mathbb{Q}_2^\times$ is a square

iff it is $2^{2a}(\text{unit} \equiv 1 \pmod 8)$.

So: $n \in \mathbb{Z}$ is in $D(q)$

$\Longleftrightarrow$ $n > 0$ and $-n \neq 4^a(8b+1)$.

Equiv: $n > 0$ and $n \neq 4^a(8b-1)$, $a,b \in \mathbb{Z}$.

Ex. Which non-0 elements in $\mathbb{Q}$ are

sums of 4 squares?

Again reduce to $\mathbb{Z}$. OK / $\mathbb{Q}_p$ for $p \neq 2$.

For $\mathbb{R}$: OK iff positive

For $\mathbb{Q}_2$: if $\neq 4^a(8b-1)$, then

in $D(\langle 1,1,1\rangle) \subseteq D(\langle 1,1,1,1\rangle)$.

If $4^a(8b-1)$, then $4^a(8b-2) + 4^a$

sum of 3 squares square

So yes for all pos. integers.

To prove Hasse-Minkowski:

WMA q regular (otherwise isotropic /F)

Proceed by induction on dim q.

Prove cases of dim $q = 1, 2, 3, 4$ separately,

& then start induction with dim = 5.

For dim $q=1$: $q = \langle a \rangle$, $a \neq 0$.

Then q anisotropic /F and over F_v ✓

Higher dimensional cases:

To be discussed.