Recall: We're proving the Hasse-Minkowski Thm over a global field F:

local-global principle for isotropy of quadratic forms over F:

q isotropic/every $F_v \Rightarrow q$ isotropic $/F$

We proved this for $\dim q < 5$. Now show H-M for $\dim \geq 5$, by induction on $\dim q$.

Write $q = \langle \underbrace{a, b}_{q_1}, \underbrace{c, d, e, \ldots}_{q_2} \rangle$ isotropic$/F_v$ $\forall v$

possibly more entries

regular, so entries all $\neq 0$

Let $S = \{v \mid q_2 \text{ isotropic on } F_v\}$.

$T = \{v \mid q_2 \text{ anisotropic on } F_v\}$.

Claim T is finite. I.e.: all but finitely many $v \in S$.

Proof of claim:

these are all but finitely many v on F

For v non-archimedean, have

valuation ring R_v (local ring)

$\cup$

maximal ideal m_v ; $R_v/m_v = k_v$ finite field

$c, d, e \in R_v$ for all but finitely many v;

c, d, e lie in only finitely many $\mathfrak{m}_v$;

& only finitely many $\mathfrak{m}_v$ have char $k_v = 2$.

(We're assuming char $F \neq 2$)

Exclude these. Then $c, d, e \overset{\in R_v}{\notin} \mathfrak{m}_v$, so

$\bar{c}, \bar{d}, \bar{e} \neq 0$ in k_v; $\langle \bar{c}, \bar{d}, \bar{e}, \ldots \rangle$ isotropic$/k_v$

c, d, e units

& then $\langle c, d, e, \ldots \rangle$ isotropic$/F_v$. $\quad u(k_v) = 2$

So all but finitely many v lie in S; i.e. q_2 isotropic$/F_v$. This proves the claim. ✓

Returning to the main pf of H-M:

Have $q = \langle \underbrace{a, b}_{q_1}, \underbrace{c, d, e, \ldots}_{q_2\text{, isotropic over all but fin many } F_v} \rangle$ isotropic$/$all F_v

regular; entries $\neq 0$

(q_1, q_2 regular)

Claim: Let $v \in T$, i.e. q_2 anisotropic $/F_v$. Then $\exists\, z_v \in F_v^\times$ st

$$z_v \in D_{F_v}(q_1),\ -z_v \in D_{F_v}(q_2).$$

Pf of claim: By assumption,

q isotropic $/F_v$.

So $\exists\, x \overset{\neq 0}{\in} F_v^n$ st $q(x) = 0$

Write $x = (x_1, x_2)$ in F_v^{n-2}
in F_v^2

$q(x) = q_1(x_1) + q_2(x_2)$

Case 1: $x_2 = 0 \in F_v^{n-2}$.

$x \neq 0 \Rightarrow x_1 \neq 0$.

b/c $q_2(x_2) = 0$

So $0 = q(x) = q(x_1, x_2) = q_1(x_1)$

So q_1 is isotropic $/F_v$ & regular;
$\therefore$ universal $/F_v$.

Also q_2 regular, $\Rightarrow \exists\, y_2 \overset{\neq 0}{\in} F_v^{n-2}$ st $q_2(y_2) \neq 0$.

q_1 universal $\Rightarrow \exists\, y_1 \in F_v^2$ st $q_1(y_1) = -q_2(y_2) \neq 0$

Take $z_v = q_1(y_1) = -q_2(y_2)$. So $z_v \in F_v^\times$
and $z_v \in D_{F_v}(q_1)$, $-z_v \in D_{F_v}(q_2)$,
giving the claim in this case.

Case 2: $x_2 \neq 0 \in F_v^{n-2}$.

$v \in T$; i.e. q_2 anisotropic/ F_v.

So $q_2(x_2) \neq 0$. But since $x_2 \neq 0$

$0 = q(x_1, x_2) = q_1(x_1) + q_2(x_2)$

So take $z_v = q_1(x_1) = -q_2(x_2) \in F_v^\times$

with $z_v \in D_{F_v}(q_1)$, $-z_v \in D_{F_v}(q_2)$. ✓

So the claim is proved; i.e.

$\forall v \in T \; \exists z_v \in F_v^\times$ with $z_v \in D_{F_v}(q_1)$, $-z_v \in D_{F_v}(q_2)$.

Take $v \in T$.

Since $z_v \in D_{F_v}(q_1)$, we may write 2 dim'l form, $\langle a, b \rangle$.

$z_v = q_1(x_v, y_v)$ with $x_v, y_v \in F_v$

$0 \neq \; = a x_v^2 + b y_v^2$ not both 0.

If $x, y \in F_v$ are suff. close to x_v, y_v resp., wrt $|\cdot|_v$, then $z := ax^2 + by^2 = q_1(x, y) \neq 0$ (being suff. close to $z_v \neq 0$).

Also, z_v/z suff close to 1, so in $F_v^{\times 2}$; so z, z_v in same square class in F_v.

Since there are only finitely many such $v \in T$, Weak Approx $\Longrightarrow$

$\exists\, x, y \in F$ that are suff. close to x_v, y_v resp for all $v \in T$.

So $z = ax^2 + by^2 = q_1(x, y) \in F^\times$.

So q_1 represents z over F.

So $q_1 \cong \langle z, w \rangle$ for some $w \in F^\times$.

Let $q' = \langle z \rangle \perp q_2$. So $q \cong q' \perp \langle w \rangle$.

By def of S, q_2 is isotropic $/F_v$ for all $v \in S$.

Hence $q' = \langle z \rangle \perp q_2$ is isotropic $/F_v$ for all $v \in S$.

For $v \notin S$ (i.e. $v \in T$), q_2 reps. $-z_v / F_v$.

Since $-z, -z_v$ are in the same square class $/F_v$,

q_2 also reps $-z / F_v$.

$\therefore q' = \langle z \rangle \perp q_2$ is isotropic $/F_v$ for all $v \notin S$.

Thus q' is isotropic $/F_v$ for all v.

But $q \cong q' \perp \langle w \rangle$, so $\dim q' = \dim q - 1$.

So by induction hypothesis, H-M holds for q'.

$\therefore$ q' is isotropic $/F$. But $q \cong q' \perp \langle w \rangle$

So q is isotropic $/F$.

This completes the proof of Hasse-Minkowski.

Back to Galois cohomology

— via group cohomology.

Recall: if Γ is a finite group or a profinite group $\varprojlim \Gamma_j$, finite gp

and Γ acts on an abelian group A, we can define $H^i(\Gamma, A)$:

$$C^i(\Gamma, A) = \{\text{cont. maps } \Gamma^i \to A\}$$ i-cochains

$$\cup\!|$$

$$Z^i(\Gamma, A) = \ker d : C^i(\Gamma, A) \to C^{i+1}(\Gamma, A)$$ i-cocycles

$$\cup\!|$$

$$B^i(\Gamma, A) = \operatorname{im} d : C^{i-1}(\Gamma, A) \to C^i(\Gamma, A)$$

i-coboundaries

where $d : C^i(\Gamma, A) \to C^{i+1}(\Gamma, A)$

is defined by

group action

$$df(\gamma_1, \ldots, \gamma_{i+1}) = \gamma_1 \cdot f(\gamma_2, \ldots, \gamma_{i+1}) + \sum_{j=1}^{i} (-1)^j f(\gamma_1, \ldots, \gamma_{j-1}, \underbrace{\gamma_j \gamma_{j+1}}_{\text{mult in } \Gamma}, \gamma_{j+2}, \ldots, \gamma_{i+1}) + (-1)^{i+1} f(\gamma_1, \ldots, \gamma_i)$$

Here $d^2 : C^i(\Gamma, A) \longrightarrow C^{i+2}(\Gamma, A)$

is the zero map, so $B^i(\Gamma, A) \subseteq Z^i(\Gamma, A)$

and we can take $H^i(\Gamma, A) = Z^i(\Gamma, A) / B^i(\Gamma, A)$.

= gp of coho classes of i-cocycles.

Ex. $H^0(\Gamma, A) = A^\Gamma$

$$:= \left\{ a \in A \,\middle|\, \begin{array}{l} a \text{ is fixed under the} \\ \text{action of } \Gamma \end{array} \right\}$$

If the action is trivial, $H^0(\Gamma, A) = A$.

Ex. $H^1(\Gamma, A)$

$$= \{ f \overset{\text{cont}}{:} \Gamma \to A : f(\gamma\gamma') = \gamma \cdot f(\gamma') + f(\gamma) \}$$

the set of (continuous) crossed homomorphisms from Γ to A (wrt the action).

If the action is trivial, then $H^1(\Gamma, A) = \mathrm{Hom}(\Gamma, A)$ (usual hom's)

Ex. $H^2(\Gamma, A) =$ gp of coho. classes of factor systems f, i.e. cont. maps $f : \Gamma \times \Gamma \to A$ such that

$$\gamma \cdot f(\gamma', \gamma'') - f(\gamma\gamma', \gamma'') + f(\gamma, \gamma'\gamma'') - f(\gamma, \gamma') = 0$$

If A is finite, $H^2(\Gamma, A)$ classifies the set of iso. classes of group extensions $1 \to A \to \Delta \to \Gamma \to 1$ st the given action of Γ on A is the one obtained by lifting $\gamma \in \Gamma$ to some $\delta \in \Delta$ and conjugating A. (Well defined b/c A is abelian)

Can also define group cohomology via derived functors:
Let $H^i(\Gamma, A)$ be the i^{th} right derived functor of the functor $A \mapsto A^\Gamma$.
So $H^0(\Gamma, A) = A^\Gamma = \mathrm{Hom}_\Gamma(\mathbb{Z}, A)$

Hom as Γ-modules, i.e. as $\mathbb{Z}[\Gamma]$-modules

So $H^i(\Gamma, \cdot) = i^{th}$ rt derived functor of $\mathrm{Hom}_\Gamma(\mathbb{Z}, \cdot)$

$$= \mathrm{Ext}^i_\Gamma(\mathbb{Z}, \cdot)$$

So $H^i(\Gamma, A) = \mathrm{Ext}^i_{\mathbb{Z}[\Gamma]}(\mathbb{Z}, A)$.

Can use this to rewrite the cocycle definition (See Serre, Local Fields, Ch. VII, §2-3)

As expected with cohomology, given a s.e.s. $0 \to A \to B \to C \to 0$ of Γ-modules, there's a l.e.s.

$$\begin{array}{ccccccc} & A^\Gamma & & B^\Gamma & & C^\Gamma & \\ & \| & & \| & & \| & \\ 0 \to & H^0(\Gamma, A) & \to & H^0(\Gamma, B) & \to & H^0(\Gamma, C) & \to \\ & H^1(\Gamma, A) & \to & H^1(\Gamma, B) & \to & H^1(\Gamma, C) & \to \cdots \end{array}$$

If $H^i(\Gamma, \cdot) = 0$ for all $i \gg 0$, can work backwards to compute H^0, H^1.

What if we want to form $H^i(\Gamma, G)$ for a nonabelian group G on which Γ acts?
(Serre, Galois Cohomology, Chap I, §5)

Difficulty: $Z^i(\Gamma, G)$ is not a group.

We can still define the set

$$Z^1(\Gamma, G) = \left\{ f \in C^1(\Gamma, G) \;\middle|\; f(\gamma\gamma') = f(\gamma)\,(\gamma \cdot f(\gamma')) \right\}$$

but we can't take Z^1/B^1 for H^1.

Instead, define an equivalence relation on $Z^1(\Gamma, G)$ (being "cohomologous"):

$f_1 \sim f_2$ if $\exists g \in G$ st $\forall \gamma \in \Gamma$,

$$f_2(\gamma) = g^{-1} f_1(\gamma)\,(\gamma \cdot g).$$

So $f \sim 1$ (trivial elt of Z^1) iff

$$\exists g \in G \text{ st } \forall \gamma \in \Gamma,\ f(\gamma) = g^{-1}(\gamma \cdot g)$$

(so specializes to the old B^1 if G abelian).

We then define $H^1(\Gamma, G)$ to be the set of cohomology classes in $Z^1(\Gamma, G)$. Not a group; just a <u>pointed set</u> (set with a distinguished element) like Z^1.

Ex. Say Γ acts <u>trivially</u> on G. Then

$$Z^1(\Gamma, G) = \left\{ f \in C^1(\Gamma, G) \middle| f(\gamma\gamma') = f(\gamma) f(\gamma') \right\}$$

$$= \mathrm{Hom}(\Gamma, G),$$

as in the abelian case.

But $\underbrace{\mathrm{Hom}(\Gamma, G)}_{= Z^1(\Gamma, G)}$ is not a group, just a pointed set.

Category of pointed sets: $(S, s_0) \to (T, t_0)$, $s_0 \longmapsto t_0$

inj $\Rightarrow$ trivial ker; <u>not</u> conversely

$H^0(\Gamma, G) = G^\Gamma$ as before; a group

$H^i(\Gamma, G)$: not defined for $i \geq 2$.

If $1 \to N \to G \to H \to 1$ is a s.e.s with compatible actions of Γ, get a 6-term exact sequence

$$\begin{tikzcd} 1 \arrow[r] & H^0(\Gamma, N) \arrow[r] & H^0(\Gamma, G) \arrow[r] & H^0(\Gamma, H) \arrow[dll, out=0, in=180] \\ & H^1(\Gamma, N) \arrow[r] & H^1(\Gamma, G) \arrow[r] & H^1(\Gamma, H) \end{tikzcd}$$

in category of pointed sets

(i.e. ker = im of prev. map)

If $N \subset Z(G)$ (so N is abelian), get a 7^{th} term:

$$\begin{tikzcd} 1 \arrow[r] & H^0(\Gamma, N) \arrow[r] & H^0(\Gamma, G) \arrow[r] & H^0(\Gamma, H) \arrow[dll, out=0, in=180] \\ & H^1(\Gamma, N) \arrow[r] & H^1(\Gamma, G) \arrow[r] & H^1(\Gamma, H) \arrow[dll, out=0, in=180] \\ & H^2(\Gamma, N) & & \end{tikzcd}$$

Galois cohomology: Case where

Γ is a Galois group.

Previously discussed: F a field, $\Gamma = \mathrm{Gal}(F) := \mathrm{Gal}(F^{sep}/F)$.

Write $H^i(F,G)$ for $H^i(\Gamma,G)$

(G not nec. abelian if $i=0,1$)

More generally, say E/F is a Galois extension, & let $\Gamma = \mathrm{Gal}(E/F)$.

Write $H^i(E/F,G)$ for $H^i(\Gamma,G)$

Before we considered $G=\mathbb{Z}/\ell$. More genlly, can let G be a linear algebraic group, i.e. a Zariski closed subgroup of GL_n.

Again, need G abelian, unless $i=0,1$.

Case of GL_n itself, over F:

View GL_n as the Zariski closed subset of $\mathbb{A}_F^{n^2+1}$

n^2+1 dim'l affine space; coordinates x_{ij} $(1 \leq i \leq n)$ and y st

$$y \underbrace{\det(x_{ij})}_{\text{Poly of deg } n \text{ in the } x_{ij}} - 1 = 0$$

Write $\mathbb{G}_m := GL_1$: multiplicative group.

Ex The invertible $n \times n$ diagonal matrices form a group $\cong \mathbb{G}_m^n$.

Ex $SL_n \subset GL_n$, given by $\det(x_{ij}) - 1$.

Ex $SO_n(q) \subset O_n(q) \subset GL_n$, q : q.f. $/F$

Ex. The group of matrices of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ is isomorphic to the additive group $\mathbb{G}_a$.

If G is a linear alg. gp defined $/F$, then $\Gamma := Gal(F) = Gal(F^{sep}/F)$ acts on the group $G(F^{sep})$ of F^{sep}-points on G.

Define $H^i(F, G) := H^i(\Gamma, G(F^{sep}))$

($i = 0, 1$, unless G is commutative)

And for E/F Galois, define

$H^i(E/F, G) := H^i(Gal(E/F), G(E))$

Ex. F a field, G a finite group, take trivial action of $\underset{\Gamma}{\underset{\shortparallel}{Gal(F)}}$ on G.

Then $H^1(\Gamma, G) = Hom(\Gamma, G)/\sim$

$= \{$iso. classes of G-Galois algebras $/F\}$

Galois fld extens, + $\oplus$'s of such.

conjugacy in G

E.g. $F = \mathbb{Q}$, $G = \mathbb{Z}/2$: $\mathbb{Q}(i)$, also $\mathbb{Q} \oplus \mathbb{Q}$.

Ex. (as on PS 4) L/K a Galois field extension $\Rightarrow$

$$H^1(\mathrm{Gal}(L/K), L^\times) \text{ is trivial}$$

"Hilbert's Theorem 90"

Can write as: $H^1(L/K, \mathbb{G}_m) = 1$.

Can take $\varprojlim_{L/K}$ and get $H^1(K, \mathbb{G}_m) = 1$.

More generally: $H^1(L/K, GL_n) = 1$

(by a generalization of the proof — Serre, Local Fields, Chap X, §1, Prop 3)