Recall: Given a linear algebraic group $G \subseteq GL_n$ over a field F, we have Galois cohomology $H^i(F, G)$ (for all $i \geq 0$ if G comm; $i = 0, 1$ in general).

A G-torsor X over F (princ. hom. space) is an F-variety with a simply transitive right action of G on X.

Equiv:
$$X \times G \xrightarrow{\sim} X \times X$$
$$(x, g) \longmapsto (x, x \cdot g)$$

A G-torsor X over F is trivial iff it is iso to G itself.

Equiv: X has an F-point.

We saw:

$$H^1(F, G) \overset{\text{bij}}{\longleftrightarrow} \left\{ \begin{array}{l} \text{iso classes of} \\ G\text{-torsors } / F \end{array} \right\}$$

More generally, for E/F Galois,

$$H^1(E/F, G) \overset{\text{bij}}{\longleftrightarrow} \left\{ \begin{array}{l} \text{iso classes of} \\ G\text{-torsors } /F \\ \text{that are trivial } /E \end{array} \right\}$$

Another interpretation of H^1:

Consider an algebraic structure Δ over F: consisting of F^n together with additional functorial structure

Ex. q.f. $/ F$ (i.e. (V, q)) $V = F^n$

Ex c.s.a. $/ F$ (F^{n^2} with add'l struc)

General principle: If $G = \mathrm{Aut}(\Delta)$ lin. alg gp.

$$H^1(E/F, G) \overset{\text{bij}}{\longleftrightarrow} \left\{ \begin{array}{l} \text{iso cl's of forms } /F \\ \text{of } \Delta, \text{ iso to } \Delta \text{ over } E \end{array} \right\}$$

Using this, we get in particular:

$$H^1(E/F, O(q)) \xleftrightarrow{\text{bij}} \left\{\begin{array}{l}\text{isom. classes of qf}/F \\ \text{that become iso to} \\ q \text{ over } E\end{array}\right\}$$

reg qf/F

As a special case, taking $E = F^{sep}$, $q = \langle 1, 1, \dots, 1\rangle$:

$$H^1(F, O_n) \xleftrightarrow{\text{bij}} \left\{\begin{array}{l}\text{isom. classes of} \\ \text{qf}/F \text{ of dim } n\end{array}\right\}$$

To prove the general principle, for E/F, Δ, $G = \mathrm{Aut}(\Delta)$:

let $X = \{\text{objects}/E \text{ iso to } \Delta \text{ over } E\}$.

So $\Gamma := \mathrm{Gal}(E/F)$ acts on X, and

$$X^\Gamma = \{\text{objects}/F \text{ iso to } \Delta \text{ over } E\}.$$

We saw:

Compatible Γ-actions

$$X \xleftrightarrow{\text{bij}} GL_n(E)/G(E)$$

So $1 \to G(E) \to GL_n(E) \to X(E) \to 1$, a s.e.s. of ptd. sets with Γ-actions, gives a 5-term exact coho sequence.

$$1 \to H^0(\Gamma, G(E)) \to H^0(\Gamma, \overset{\overset{GL_n(F)}{\shortparallel}}{GL_n(E)}) \to \overset{\overset{H^0(\Gamma, X) = X^\Gamma}{\shortparallel}}{H^0}(\Gamma, GL_n(E)/G(E)) \to$$

$$\to H^1(\Gamma, G(E)) \to \underset{\underset{1 \;(\text{Hilbert } 90)}{\shortparallel}}{H^1(\Gamma, GL_n(E))}$$

So:

$$H^1(\Gamma, G(E)) \cong X^\Gamma / GL_n(F)$$

$$\shortparallel \qquad\qquad\qquad \cong$$

$$H^1(E/F, G) \qquad \{GL_n(F) \text{ orbits in } X^\Gamma\}$$

$$\shortparallel \qquad\qquad\qquad \cong$$

$$H^1(E/F, \mathrm{Aut}(\Delta)) \cong \left\{ \begin{array}{l} \text{iso classes of objects}/F \text{ that} \\ \text{are iso to } \Delta \text{ over } E \end{array} \right\}$$

as asserted.

This proves the general principle.

This then justifies the assertion about q.f.'s, that

$$H^1(E/F, O(q)) \xleftrightarrow{\text{bij}} \left\{ \begin{array}{l} \text{iso cl's of qf}/F \\ \text{that become iso} \\ \text{to } q\ /E \end{array} \right\}$$

& in particular

$$H^1(F, O(\underset{\text{reg, dim } n}{q})) \leftrightarrow \left\{ \begin{array}{l} \text{iso cl's of reg qf's} \\ /F \text{ of dim } n \end{array} \right\}$$

$$\updownarrow$$

$$\{\text{iso cl's of } O(q)\text{-torsors}/F\}$$

As another example, take csa's.

$$H^1(E/F, \mathrm{Aut}(A)) \leftrightarrow \left\{ \begin{array}{l} \text{iso cl's of csa's } /F \\ \text{that become iso} \\ \text{to } A/E \end{array} \right\}$$

some csa $/F$, deg n.

and

$$H^1(F, \mathrm{Aut}(A)) = \left\{ \begin{array}{l} \text{iso cl's of csa's} \\ /F \text{ of deg } n \end{array} \right\},$$

Since all csa's of deg n $/F$ become iso $/F^{sep}$ (to M_n).

In particular, take $A = M_n(F)$.

What is $\mathrm{Aut}(A)$?

Recall: By the Skolem-Noether Thm on csa's, every endomorphism f of a csa A/F is an inner aut; i.e. $\exists\, s \in A^\times$ st $\forall a \in A$, $f(a) = s^{-1} a s$.

What are the inner aut's of $A = M_n(F)$?

Each is given by conjugation by some elt of $A^\times = GL_n(F)$:

$$GL_n(F) \twoheadrightarrow \mathrm{Aut}(M_n(F))$$

$$\text{Kernel} = Z(GL_n(F)) = \overset{\text{non-0}}{\text{constant}} \text{ mx's.}$$

So: get $\mathrm{Aut}(M_n(F)) \cong GL_n(F)/F^\times$

$$=: PGL_n(F)$$

Note: Here $\mathrm{Aut}(M_n(F))$ means as an algebra $/F$.

We can also consider a larger group,

$\mathrm{Aut}_{vs}(\underbrace{M_n(F)}_{\text{as a } F\text{-vs}, \ \cong F^{n^2}})$ of aut's as a vs$/F$.

so $\cong GL_{n^2}(F)$.

So $\underset{\text{as } F\text{-alg}}{\mathrm{Aut}(M_n(F))} \underset{\text{subgp}}{\subset} GL_{n^2}(F)$,

is a linear alg. group;

& this is $PGL_n(F)$.

defined as a quotient of GL_n; but now also a subgp of GL_{n^2}.

Conclusion:

$$\left\{\begin{array}{c}\text{iso cl's of}\\ \text{csa's }/F\\ \text{of deg } n\end{array}\right\} \xleftrightarrow{\text{bij}} H^1(F, PGL_n).$$

$$\updownarrow \text{bij}$$

$$\left\{\begin{array}{c}\text{iso cl's of}\\ PGL_n\text{-torsors }/F\end{array}\right\}$$

In the examples w/ q.f.'s & csa's, we used that we had a structure consisting of a f.d.v.s. with some additional (functorial) data.

What about the simplest such objects wrt f.d.v.s's $/F$?

If V is an n-dim'l vs$/F$, then $\mathrm{Aut}(V) = GL_{n,F}$.

So

$$\begin{tikzcd}
\left\{\begin{matrix}\text{iso cl's of} \\ GL_n\text{-torsors}/F\end{matrix}\right\} \arrow[r, leftrightarrow, "\text{bij}"] & H^1(F, GL_n) \arrow[dl, leftrightarrow] \\
\left\{\begin{matrix}\text{iso cl's of} \\ n\text{-dim'l vs's}/F\end{matrix}\right\} &
\end{tikzcd}$$

This is trivial by Hilbert 90.

This is trivial by classification of fdvs's.

So this is also trivial: every GL_n-torsor is trivial; i.e., is iso to GL_n itself, over F.

Some <u>other</u> algebraic structures?

Ex. Octonion algebras $/F$.
"
Cayley algebras

These generalize the usual Cayley numbers $/\mathbb{R}$ (an 8-dim'l non-associative algebra whose non-0 elts are invertible).

(For more, see Chap VIII, §33.C of "The Book of Involutions" (BOI), by Knus, Merkurjev, Rost, Tignol)

For such an alg A, $\mathrm{Aut}(A)$ is a linear algebraic group "of type G_2"

in classification in Lie theory, re Dynkin diagrams

So $\{$iso cl's of octonion alg's $/F\}$

$\updownarrow$

$\left\{\begin{array}{l}\text{iso cl's}\\ \text{of } G\text{-torsors}\end{array}\right\} \longleftrightarrow H^1(F, G)$

of type G_2

Ex. Albert algebras / F:

27-dim'l exceptional Jordan algebras

a type of non-assoc. alg;
a variant on Lie algebras

$\mathrm{Aut}(A)$ is a group of "type F_4" in the
classification in Lie theory

an Albert algebra

So $\{$iso cl's of Albert algebras/$F\}$

$\updownarrow$ bij

of type F_4

$H^1(F, G) \longleftrightarrow \left\{\begin{array}{l}\text{iso classes}\\ \text{of } G\text{-torsors}\end{array}\right\}$

(See BOI, Chap IX, §37)

Ex F of char $\neq 2$, $n > 0$, $\delta \in F^\times$

Quadratic forms q of dim n over F
with $\det q = \delta \in F^\times / F^{\times 2}$.

Iso classes of these

$\Big\updownarrow$ bij

$$H^1(F, SO(q))$$

some particular qf of det $= \delta$

(Proof via Clifford algebras; see BOI, Ch VII, 29.29.)

(Or via l.e.s. in cohomology from s.e.s.

$$1 \to SO(q) \to O(q) \to \{\pm 1\} \to 1.\ )$$

For other related examples, see BOI, Chap VII, §29

Those are deduced there from an abstract result presenting the general principle, but phrased in terms of groupoids — see BOI, Prop 29.1.

In all these examples, the objects of a given sort are classified by the H^1 of some linear alg. gp. G, which also classifies G-torsors.

This is useful in studying local-global principles.

Say we have a type of algebraic structure, over a global field F.

LGP says: trivial (split) $/F \iff$ trivial$/F_v$ $\forall v$.

Ex LGP for quadratic forms to be iso to a given q.f. (e.g. $\langle 1, \ldots, 1\rangle$, or nh)

Ex. LGP for csa's to split (Thm of Albert-Brauer-Hasse-Noether)

Using torsors to get such LGP's:

Recall: A variety V over a global field F satisfies a LGP if $V(F_v) \neq \emptyset$ for all $v \Rightarrow V(F) \neq \emptyset$.

In the case that V is G-torsor $/F$,
for some linear algebraic group G,
for E/F, $\quad V(E) \neq \emptyset \Leftrightarrow V$ is trivial $/E$

i.e. $\cong G$ over E

If Δ is a alg. structure classified
by G-torsors for some G, then
Δ has a LGP $/F \Leftrightarrow$
G-torsors satisfy a LGP $/F$

i.e. trivial $/F \Leftrightarrow$ trivial $/$ each F_v

So: for the lin. alg groups G arising
in the above examples, do G-torsors
satisfy a LGP?

Equiv: Consider the natural map

$$\alpha: H^1(F, G) \longrightarrow \prod_v H^1(F_v, G)$$

induced by the inclusions $F \hookrightarrow F_v$.

On the level of torsors, α assigns to each G-torsor $/F$ the corresp G-torsor$/F_v$.
The distinguished element of $H^1(F, G)$ corresp to the trivial G-torsor G: the unique G-torsor $/F$ with an F-point.

$$\ker\alpha \longleftrightarrow \left\{ \begin{array}{l} \text{iso classes of } G\text{-torsors}/F \\ \text{that become trivial}/\text{each } F_v \end{array} \right\}$$

LGP $\Leftrightarrow$ $\ker\alpha$ is trivial.

Tate-Shafarevich set

Write $Ш(F, G) = \ker\alpha \subseteq H^1(F, G)$ the obstruction to the LGP.
i.e. $Ш(F, G) = 1 \Leftrightarrow$ have LGP for G-torsors$/F$.

a ptd set; a group if G commutative

In general, whether LGP holds depends on G and F.

A key property that G may have: being a rational variety.

We say an irreducible variety V/F is rational if its function field is purely transcendental over F.

Equiv: V has a Zariski dense open subset U that is iso to a Zariski dense open subset of $\mathbb{A}^n_F$.

$n = \dim V$

Ex $SO(q)$ is rational (PS#1)

Note: A lin. alg. gp. is smooth, so it is irreducible $\Longleftrightarrow$ connected.

Thm (Sansuc, Chernousov)

Let F be a number field, and let G be a connected linear algebraic group $/F$. Suppose that G is rat'l as an F-variety. Then $Ш(F,G) = 1$. I.e. we have a LGP for G-torsors $/F$.

So in this situation, if

Aut of the structure

$$H^1(F,G) \longleftrightarrow \left\{\begin{array}{l}\text{Iso classes of alg.}\\ \text{structures } /F\\ \text{of type} \ldots\end{array}\right\}$$

then two such objects are iso $/F$ $\iff$ they are iso $/F_v$ for all v.

Ex Let q be a qf / a #fld F of even dim $n = 2r$. If q is hyperbolic over F_v for each v, then $\det q = \det rh = (-1)^r$.

But the qf's of dim n and $\det = (-1)^r$ are classified by $H^1(F, SO(q))$, and $SO(q)$ is a rational connected F-variety.

So LGP holds for this H^1.

$\therefore$ $q \cong rh$ over F.

I.e. q hyperbolic / all $F_v \Rightarrow q$ hyperbolic $/F$.

— gives another pf. (We have that this also follows from Hasse-Minkowski PS#5)

Note: One can also consider algebraic groups that aren't linear alg. gps, i.e. not affine (& not closed subsets of GL_n).

Key example: elliptic curves E:

a smooth projective curve of genus 1 over F, with an F-pt O. This has a group law, with identity O, and

not affine

E is an algebraic group $/F$.

Tate-Shafarevich Conjecture:

Ш(F, E) is finite if F is a # fld.

Tate-Shafarevich group (since E is commutative)

Open in general. Stronger Conjecture: Conjecture of Birch & Swinnerton-Dyer: Predicts $|$Ш$(F,E)|$ in terms of quantities including the L-function associated to E, the regulator of E, and the # of torsion points in $E(F)$. — a Millennium Problem

For a linear algebraic group G
over a # field F, it's a thm
of Borel-Serre that $Ш(F, G)$ is finite.

so finite obstruction to LCP

Also true / global function fields:
more recent; due to a number of authors,
culminating w B. Conrad.