<u>Recall</u>: Given a field F,

- quadratic forms$/F \rightsquigarrow W(F), I(F), I^n(F)$
- csa's$/F \rightsquigarrow Br(F)$
- $K_2^M(F) = F^\times \otimes_{\mathbb{Z}} F^\times / \left(\begin{matrix} a \otimes (1-a), \\ 1 \neq a \in F^\times \end{matrix} \right)$

$h_2^M(F) = K_2(F)/2.$

Can relate these objects via a commutative diagram

$$\begin{tikzcd}
 & h_2(F) \arrow[dl, "\alpha"', "\sim"] \arrow[dr, "\beta", "\sim"'] & \\
I^2(F)/I^3(F) \arrow[rr, "\gamma", "\sim"'] & & Br(F)[2]
\end{tikzcd}$$

$$[a,b] \mapsto \langle 1,-a,-b,ab \rangle, \qquad [a,b] \mapsto \left(\frac{a,b}{F}\right), \qquad q \mapsto C(q)$$

To generalize this:

Use that K_2 is part of a <u>collection</u> of groups K_n, due to Milnor:

Define the $\mathbb{N}$-graded $\mathbb{Z}$-algebra

$$K_*^M(F) = T^*(F^\times) / \left(\begin{matrix} a \otimes (1-a), \\ 1 \neq a \in F^\times \end{matrix} \right)$$

Here, the nth graded piece $K_n^M(F)$ is the image of $T^n(F^\times)$ (written additively); the "mult" is from $\otimes$.

So $K_2^M(F)$ is as above,

$K_1^M(F) = F^\times$, $\quad K_0^M(F) = \mathbb{Z}$.

or view as Grothendieck group of f.d. v.s.'s/F.
(For a ring R, take fin. gen. proj. modules/R).

(Later, Quillen defined other K-groups, $K_n^Q(F)$.
Have $K_n^M(F) \hookrightarrow K_n^Q(F)$ iso if $n \le 2$.)

We had an iso

$$k_2(F) \xrightarrow[\alpha]{\sim} I^2(F)/I^3(F)$$

$$[a,b] \longmapsto \langle 1, -a, -b, ab \rangle = \langle 1, -a \rangle \otimes \langle 1, -b \rangle$$

Can this be generalized to $n \ge 2$?

Define $k_n(F) = K_n^M(F)/2$.

For $a_1, \dots, a_n \in F^\times$, write

$$\langle\langle a_1, \dots, a_n \rangle\rangle := \langle 1, a_1 \rangle \otimes \cdots \otimes \langle 1, a_n \rangle \quad \text{in } I^n(F)$$

"n-fold Pfister form"

So the above map $\alpha : h_2(F) \to I^2/I^3$ takes $[a,b] \longmapsto \langle\langle -a, -b \rangle\rangle$.

By analogy with case $n=2$, define

$$\alpha_n : h_n(F) \longrightarrow I^n(F)/I^{n+1}(F)$$
$$[a_1, \dots, a_n] \longmapsto \langle\langle -a_1, \dots, -a_n \rangle\rangle.$$

Is this an iso?

Part of the Milnor Conjecture.

Ans: Yes. Proven by Orlov, Vishik, Voevodsky. (2007)

The other part of the Milnor Conjecture (re β) relates these groups to Galois cohomology.

Recall: Given a group Γ with an action on an abelian group A, we can define group cohomology $H^n(\Gamma, A)$ via cocycles and coboundaries. (For example, $H^2(\Gamma, A) = \{\text{equiv. classes of group extensions of } \Gamma \text{ by } A\}$.)

Namely, first suppose Γ is a finite group, with an action of Γ on A. Call A a Γ-module.

Define the set of n-cochains to be

$$C^n(\Gamma, A) = \{\text{maps } \Gamma^n \to A\}$$

not nec homs

Given $f \in C^n(\Gamma, A)$, define $df \in C^{n+1}(\Gamma, A)$ by

group action

$$\begin{aligned} df(\gamma_1, \ldots, \gamma_{n+1}) &= \gamma_1 \cdot f(\gamma_2, \ldots, \gamma_{n+1}) \\ &+ \sum_{i=1}^{n} (-1)^i f(\gamma_1, \ldots, \gamma_{i-1}, \underbrace{\gamma_i \gamma_{i+1}}_{\text{mult in } \Gamma}, \gamma_{i+2}, \ldots, \gamma_{n+1}) \\ &+ (-1)^{n+1} f(\gamma_1, \ldots, \gamma_n) \end{aligned}$$

So get

coboundary map

$$\cdots \xrightarrow{d} C^{n-1}(\Gamma, A) \xrightarrow{d} C^n(\Gamma, A) \xrightarrow{d} C^{n+1}(\Gamma, A) \xrightarrow{d} \cdots$$

and for every $n \geq 0$,

$$d^2 : C^n(\Gamma, A) \to C^{n+2}(\Gamma, A)$$

is the 0 map.

Let $Z^n(\Gamma,A)=\ker\left(d: C^n\to C^{n+1}\right)$;

group of <u>n-cocycles</u>;

and let $B^n(\Gamma,A) = \operatorname{im}\left(d: C^{n-1}\to C^n\right)$;

group of <u>n-coboundaries</u>.

Let $H^n(\Gamma,A) = Z^n(\Gamma,A)/B^n(\Gamma,A)$,

the <u>n^{th} cohomology group</u>.

Ex. $H^0(\Gamma,A) = A^\Gamma = \{a\in A \mid a \text{ is fixed by } \Gamma\}$.

This construction parallels what is done in topology.

In our applications, we'll want to allow

Γ to be a <u>profinite</u> group

$$\Gamma = \varprojlim \Gamma_i$$ finite groups

Ex. $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n$, p-adics.

Ex. $\Gamma = \mathrm{Gal}(L/K)$ infinite Galois extension

$$\begin{tikzcd} L \arrow[d, dash] \\ L_i \arrow[d, dash, "\Gamma_i \text{ finite}"] \\ K \end{tikzcd} \quad \Gamma$$

In gen'l, such a Γ has a <u>profinite topology</u>

(weakest topology s.t. all $\Gamma\to\Gamma_i$ are continuous).

We require the action of Γ on A discrete topology

to be continuous; and in $C^n(\Gamma,A)$,

we require $f:\Gamma^n\to A$ to be continuous.

Say F is a field, and let $\Gamma = \mathrm{Gal}(F)$ be its absolute Galois group $\mathrm{Gal}(F^{sep}/F)$.

Let A be an abelian group on which Γ acts. (A is then called a Galois module.) Define the Galois cohomology group $H^n(F, A) := H^n(\Gamma, A)$.

Ex. $A = \mathbb{Z}/2$. Then the only action on A is trivial, and for any field we can form $H^n(F, \mathbb{Z}/2)$. (Assume char $\neq 2$)

Have:
$$H^0(F, \mathbb{Z}/2) = \mathbb{Z}/2$$
$$H^1(F, \mathbb{Z}/2) = F^\times / F^{\times 2}$$
$$H^2(F, \mathbb{Z}/2) = \mathrm{Br}(F)[2].$$

These are the same as $W(F)/I(F)$, $I(F)/I^2(F)$, $I^2(F)/I^3(F)$, resp.

The rest of the Milnor Conjecture says:

For all n, get a pattern from 2 to n:

$\mathrm{Br}(F)[2]$ for $n=2$

$$I^n(F)/I^{n+1}(F) \cong K_n^M(F)/2 \cong H^n(F, \mathbb{Z}/2)$$

as above

$h_n(F)$

proven by Voevodsky (2003)

More generally: the Bloch-Kato Conjecture, where we replace mod 2 by mod ℓ (and assume char $F \neq \ell$).

prime

Above, regarding $H^n(F, \mathbb{Z}/2)$, there's only the trivial action of $\Gamma = \mathrm{Gal}(F)$ on $\mathbb{Z}/2$. For $\mathbb{Z}/\ell$, there are non-trivial actions, if $\ell > 2$.

Ex. Let $\mu_\ell \subset F^{sep}$ be the group of the ℓ-th roots of unity. As a group, $\mu_\ell \approx \mathbb{Z}/\ell$. But $\Gamma = \mathrm{Gal}(F)$ acts non-trivially on μ_ℓ (unless $\ell = 2$).

We can take $H^n(F, \mu_\ell)$.

In particular, $H^1(F, \mu_\ell) \cong F^\times/(F^\times)^\ell$, the ℓ-th power classes. $H^2(F, \mu_\ell) = \mathrm{Br}(F)[\ell]$.

Ex. For every $n \geq 0$, we can let Γ act on $\mathbb{Z}/\ell$ by the n-th power of the above action. Write $\mu_\ell^{\otimes n}$ for this Galois module. (Additive notation: $\mathbb{Z}/\ell(n)$.)

Coming back to the Bloch-Kato Conj:

For $i, j \geq 0$, there is a cup product map $H^i(F, A) \otimes H^j(F, B) \to H^{i+j}(F, A \otimes B)$

The map $\partial : F^\times \to F^\times / (F^\times)^\ell \cong H^1(F, \mu_\ell)$

induces a map

$$\partial^n : T^n(F^\times) = \underbrace{F^\times \otimes \cdots \otimes F^\times}_{n \text{ factors}} \to H^1(F, \mu_\ell)^{\otimes n} \xrightarrow{\text{cup product}} H^n(F, \mu_\ell^{\otimes n})$$

$$\begin{tikzcd}
T^n(F^\times) \arrow[r] \arrow[d] & H^1(F, \mu_\ell)^{\otimes n} \arrow[r, "\text{cup product}"] & H^n(F, \mu_\ell^{\otimes n}) \\
K_n^M(F) \arrow[urr, dashed, "\text{(map factors)}"'] \arrow[d] & & \\
K_n^M(F)/\ell \arrow[uurr, dashed, "\text{``Norm residue map''}"'] & &
\end{tikzcd}$$

Bloch-Kato Conj: This map

$$K_n^M(F)/\ell \longrightarrow H^n(F, \mu_\ell^{\otimes n})$$

is an isomorphism.

Note: For $\ell = 2$, this agrees with the Milnor Conj.

Case of $n = 0$: trivial. $(\mathbb{Z}/\ell \xrightarrow{id} \mathbb{Z}/\ell)$

Case of $n = 1$: Follows from Hilbert 90

Case of $n = 2$: Proven by Merkurjev - Suslin (1982)

General Case: proven by Voevodsky (2009)
(with details by Rost, Weibel)
— now often called the

Norm Residue Isomorphism Theorem.

Note: The name "norm residue map" came from the Hilbert symbol in local class field theory, also called the "norm residue symbol." For a local field $F \supset \mu_\ell$ (finite extension of $\mathbb{Q}_p, \mathbb{R}$, or $\mathbb{F}_p((x))$) this is a pairing on $F^\times/(F^\times)^\ell$ into μ_ℓ that factors through $K_2^M(F)/\ell$.

Here $(a,b) = 1 \iff a$ is a norm from $F(\sqrt[\ell]{b})$.

If $\ell = 2$, this is equivalent to: $\left(\frac{a,b}{F}\right)$ splits.
(classical case)

Question: What about a generalization of the other part of Milnor's Conjecture, concerning I^n/I^{n+1}?

Still a big mystery.

Next topic:

Local and global fields, and local-global principles (LGP).

Esp. Hasse-Minkowski:

If q is a q.f. $/\mathbb{Q}$, then

q is isotropic $/\mathbb{Q}$ $\iff$ q isotropic $/\mathbb{R}$ and $/\mathbb{Q}_p$ for all p.

More generally: holds for any global field (a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(x)$).

Recall background on local + global fields.

Global fields:

① Finite extensions of $\mathbb{Q}$: # fields.

the ring of integers of K; the integral closure of $\mathbb{Z}$ in K.

$$\begin{array}{ccc} \mathcal{O}_K & = & K \\ \cup & & \cup \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

the prime ideals that contract to p $\quad$ $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \subset \mathcal{O}_K$

$$\begin{array}{ccc} \mathfrak{P}_1, \ldots, \mathfrak{P}_r & \subset & \mathcal{O}_K \\ \vee & & | \\ (p) & \subset & \mathbb{Z} \end{array}$$

prime in $\mathbb{Z}$

For p prime, have local ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$.

$\mathbb{Z}$ is a Dedekind domain

Noetherian integrally closed domain of Krull dimension 1

i.e. every non-0 prime ideal is max'l

So the localization $\mathbb{Z}_{(p)}$ is a local Ded. dom.

This is equivalent to being a discrete valuation ring

Recall: A discrete valuation on a field F is a map $v: F^\times \to \mathbb{Z}$ st

$v(ab) = v(a) + v(b)$, $\quad v(a+b) \geq \min(v(a), v(b))$.

The valuation ring of v is $\{a \in F^\times \mid v(a) \geq 0\} \cup \{0\}$

A discrete valuation ring. (dvr)

Also write $v(0) = \infty$, for convenience.

Viewed as a local Dedekind domain, the max'l ideal of a dvr R is principal. (π)

uniformizer

$\mathfrak{m} = \{a \in R \mid v(a) > 0\}$. $R - \mathfrak{m} = R^\times$

$= (\pi)$, $v(\pi) = 1$. $\qquad = \{a \in R \mid v(a) = 0\}$

In the case of $\mathbb{Z}_{(p)} \subset \mathbb{Q}$, $\mathfrak{m} = (p)$ $\leftarrow = \pi$

v is the p-adic valuation:

For a rat'l # $\alpha = p^n \frac{a}{b}$, with $p \nmid a, b$,

$v(\alpha) = n$.

The max'l ideal is $p\mathbb{Z}_{(p)}$.

A discrete valuation v $\rightsquigarrow$ an absolute value $|\cdot|_v$.

To define, pick $c > 1$ and define

$$|\alpha|_v = c^{-v(\alpha)}.$$

This satisfies $|\alpha + \beta|_v \leq \max(|\alpha|_v, |\beta|_v)$, $|\alpha\beta|_v = |\alpha|_v |\beta|_v$

Strong Δ inequality "non-archimedean abs. val."

Ex. For the p-adic valuation on $\mathbb{Q}$, take $c = p$;

so $\left|p^n \frac{a}{b}\right|_p = p^{-n}$. $(p \nmid a, b)$

Given a field F with a discrete valuation $v \rightsquigarrow |\cdot|_v$,
we can complete F wrt $|\cdot|_v$, and get a field F_v
(just as we complete $\mathbb{Q}$ wrt $|\cdot|$ to get $\mathbb{R}$)
$\uparrow$ usual abs. val.

Ex. Complete $\mathbb{Q}$ wrt $|\cdot|_p$; get $\mathbb{Q}_p$.

$$\begin{array}{ccc} \mathbb{Q} & & \mathbb{Q}_p \\ \cup & & \cup \\ \mathbb{Z} & & \mathbb{Z}_p \end{array}$$

Also: " $\mathbb{Z}$ " " " $\mathbb{Z}_p$

$v, |\cdot|_v$ on $\mathbb{Q}$ extend to $v, |\cdot|_v$ on $\mathbb{Q}_p$

$$\begin{array}{ccc} \mathbb{Q} & & \mathbb{Q}_p \\ \cup & & \cup \\ \mathbb{Z} & & \mathbb{Z}_p \end{array}$$

Another sense of "completion":

Can complete a local ring R at its maximal ideal $\mathfrak{m}$ as an inverse limit:

$$\hat{R}_{\mathfrak{m}} = \varprojlim R/\mathfrak{m}^n.$$

Do this with a dvr:

Ex. $\underset{\overset{\shortparallel}{R}}{\mathbb{Z}_{(p)}} \supset \underset{\overset{\shortparallel}{\mathfrak{m}}}{(p)}$; $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}^n = \mathbb{Z}/p^n\mathbb{Z}$,

So get $\hat{\mathbb{Z}}_{(p)} = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$.

Get the same result as before. For a dvr R,

$\varprojlim R/\mathfrak{m}^n$ = v-adic metric completion of R.

$=: \hat{R}_{\mathfrak{m}}$; this is a complete d.v.r.

$\operatorname{frac}(\hat{R}_{\mathfrak{m}}) = F_v$, the completion of $F = \operatorname{frac} R$.

Can apply this to $\mathbb{Q}, \mathbb{Z}$, and get

$$\begin{array}{ccccc} \mathbb{Q} & & \subset & \mathbb{Q}_p & \leftarrow \text{Complete discretely valued field.} \\ \cup & \supset & & \cup & \\ \mathbb{Z} & \subset \mathbb{Z}_{(p)} & \subset & \mathbb{Z}_p & \leftarrow \text{Complete d.v.r.} \end{array}$$

Similarly if take $\mathcal{O}_K \subset K$, a # fld, can do this for a prime $\mathfrak{P}$ over a prime $(p) \subset \mathbb{Z}$.

(2) Can also do this with $F = \mathbb{F}_p(x)$ or a finite extension. (global function fields)

Ex. $F = \mathbb{F}_p(x) = \mathrm{frac}(R)$, $R = \mathbb{F}_p[x]$. Dedekind domain

$(x) \subset R$ is a prime ideal.

Localization $R_{(x)} \subset F$ dvr

Completion $\hat{R}_{(x)} \subset F_x$ max'l ideal $x R_{(x)}$

$$\begin{array}{ccc} \hat{R}_{(x)} & \subset & F_x \\ \| & & \| \\ \mathbb{F}_p[[x]] & \subset & \mathbb{F}_p((x)) \\ \text{cdvr} & & \text{cdvf} \end{array}$$

π

Similarly for finite extensions of $\mathbb{F}_p(x)$.

Will study quadratic forms over cdvf's, in particular:

— Witt groups (+ rings)

— local-global principles